Patrones

Recomendaciones de AWS

Recomendaciones de AWS: Patrones

Table of Contents

AWS Patrones de orientación prescriptiva

Los patrones de orientación prescriptiva de Amazon Web Services (AWS) proporcionan step-by-step instrucciones, arquitectura, herramientas y código para implementar escenarios específicos de migración, modernización e implementación a la nube. Estos patrones, que son examinados por expertos en la materia AWS, están pensados para desarrolladores y usuarios prácticos que planean migrar o están en proceso de migrar a ellos. AWS También ayudan a los usuarios que ya están conectados AWS y buscan formas de optimizar o modernizar sus operaciones en la nube.

Puede utilizar estos patrones para trasladar sus cargas de trabajo locales o en la nube de complejidad variable a la nube AWS y acelerar sus esfuerzos de adopción, optimización y modernización de la nube, independientemente de si se encuentra en la fase de prueba de concepto, planificación o implementación de su proyecto. Por ejemplo, para un proyecto de migración a la nube:

- En la fase de planificación, puede evaluar las diferentes opciones disponibles para migrar a AWS. Puede elegir el patrón adecuado que se adapte a sus necesidades, en función de si desea reubicar, realojar, redefinir la plataforma o rediseñar la arquitectura. También puede comprender las diferentes herramientas disponibles para la migración y empezar a planificar la adquisición de licencias o iniciar las primeras conversaciones con los proveedores.
- En las fases de prueba de concepto e implementación, puede seguir las step-by-step instrucciones que se proporcionan en el patrón para migrar su carga de trabajo a una. AWS Cada patrón incluye detalles como los requisitos previos, las arquitecturas de referencia objetivo, las herramientas, las step-by-step tareas, las mejores prácticas, la solución de problemas y el código.
- Si ya lo usa Nube de AWS, puede encontrar patrones que lo ayudarán a modernizar, optimizar, escalar y proteger el uso de los recursos de la nube.

Para ver las listas de patrones por dominio técnico, utilice los siguientes enlaces o las opciones de filtrado y búsqueda de la AWS página de inicio de la guía prescriptiva de.

- Análisis
- Productividad empresarial
- Nativo en la nube
- Contenedores y microservicios
- Entrega de contenido

- Administración de costos
- Lagos de datos
- Bases de datos
- DevOps
- Informática para usuarios finales
- Computación de alto rendimiento
- Nube híbrida
- Infraestructura
- IoT
- Machine learning e IA
- Unidades centrales
- Gestión y gobernanza
- Mensajería y comunicaciones
- Migración
- Modernización
- Redes
- Sistemas operativos
- Operaciones
- Software como servicio (SaaS)
- Seguridad, identidad, conformidad
- Sin servidor
- Desarrollo y pruebas de software
- Almacenamiento y copia de seguridad
- Aplicaciones web y móviles

Para ver todas las publicaciones, incluidas las guías, las estrategias y los patrones, consulte la AWS página de inicio de la guía prescriptiva de.

Análisis

Temas

- Analizar los datos de Amazon Redshift en Microsoft SQL Server Analysis Services
- Analice y visualice datos JSON anidados con Amazon Athena y Amazon QuickSight
- Automatice la aplicación del cifrado en AWS Glue mediante una CloudFormation plantilla de AWS
- Cree una canalización de servicios de ETL para cargar datos de forma incremental desde Amazon S3 a Amazon Redshift mediante AWS Glue
- Calcule el valor en riesgo (VaR) mediante los servicios de AWS
- Convierta la característica temporal NORMALIZE de Teradata en Amazon Redshift SQL
- Convierta la característica RESET WHEN de Teradata en Amazon Redshift SQL
- Imponga el etiquetado de los clústeres de Amazon EMR en el lanzamiento
- Asegúrese de que el registro de Amazon EMR en Amazon S3 esté habilitado en el lanzamiento
- Genere datos de prueba con un trabajo de AWS Glue y Python
- Lanzar un trabajo de Spark en un clúster EMR transitorio mediante una función de Lambda
- Migre las cargas de trabajo de Apache Cassandra a Amazon Keyspaces con AWS Glue
- Migración de Oracle Business Intelligence 12c a la nube de AWS desde servidores en las instalaciones
- Migre un clúster de Apache Kafka local a Amazon MSK mediante MirrorMaker
- Migre ELK Stack a Elastic Cloud en AWS
- Migre datos a la nube de AWS mediante Starburst
- Optimice la incorporación ETL del tamaño del archivo de entrada en AWS
- Orqueste un proceso de ETL con validación, transformación y particionamiento mediante AWS Step Functions
- Realizar análisis avanzados mediante Amazon Redshift ML
- Acceder, consultar y unirse a las tablas de Amazon DynamoDB con Athena
- Configure un espacio de datos mínimo viable para compartir datos entre organizaciones
- Configure la clasificación por idioma para los resultados de las consultas de Amazon Redshift mediante una UDF escalar de Python
- Suscripción de una función de Lambda a las notificaciones de eventos de buckets de S3 en diferentes regiones de AWS

- Tres tipos de trabajos de AWS Glue ETL para convertir datos a Apache Parquet
- Visualice los registros de auditoría de Amazon Redshift con Amazon Athena y Amazon QuickSight
- Visualice los informes de credenciales de IAM para todas las cuentas de AWS que utilizan Amazon QuickSight
- Más patrones

Analizar los datos de Amazon Redshift en Microsoft SQL Server Analysis Services

Documento creado por Sunil Vora (AWS)

Entorno: PoC o piloto	Origen: Amazon Redshift	Destino: Microsoft SQL Server Analysis Services
Tipo R: N/D	Carga de trabajo: Microsoft	Tecnologías: Análisis
Servicios de AWS: Amazon Redshift		

Resumen

Este patrón describe cómo conectar y analizar los datos de Amazon Redshift en Microsoft SQL Server Analysis Services mediante Intellisoft OLE DB Provider o CData ADO.NET Provider para acceder a la base de datos.

Amazon Redshift es un servicio de almacenamiento de datos administrado de varios petabytes en la nube. SQL Server Analysis Services es una herramienta de procesamiento analítico en línea (OLAP) que se puede utilizar para analizar datos de data mart y almacenamiento de datos como Amazon Redshift. Puede usar SQL Server Analysis Services para crear cubos OLAP a partir de sus datos para un análisis de datos rápido y avanzado.

Requisitos previos y limitaciones

Supuestos

- Este patrón describe cómo configurar SQL Server Analysis Services así como Intellisoft OLE DB Provider o CData ADO.NET Provider para Amazon Redshift en una instancia de Amazon Elastic Compute Cloud (Amazon EC2). Como alternativa, puede instalar ambas opciones en un host del centro de datos corporativo.

Requisitos previos

- Una cuenta de AWS activa
- Un clúster de Amazon Redshift con credenciales

Arquitectura

Pila de tecnología de origen

- Un clúster de Amazon Redshift

Pila de tecnología de destino

- Microsoft SQL Server Analysis Services

Arquitectura de origen y destino

Herramientas

- Microsoft Visual Studio 2019 (Community Edition)
- Intellisoft OLE DB Provider for Amazon Redshift (Trial) o bien CData ADO.NET Provider for Amazon Redshift (Trial)

Epics

Analizar tablas

Tarea	Descripción	Habilidades requeridas
Analice las tablas y los datos que se van a importar.	Identifique las tablas de Amazon Redshift que se van a importar y sus tamaños.	Administrador de base de datos

Configurar la instancia de EC2 e instalar herramientas

Tarea	Descripción	Habilidades requeridas
Configure una instancia de EC2.	En su cuenta de AWS, cree una instancia de EC2 en una subred pública o privada.	Administrador de sistemas
Instale herramientas para acceder a la base de datos.	Descargue e instale Intelliso ft OLE DB Provider para Amazon Redshift (o bien CData ADO.NET Provider para Amazon Redshift).	Administrador de sistemas
Instale Visual Studio.	Descargue e instale Visual Studio 2019 (Community Edition).	Administrador de sistemas
Instalar extensiones.	Instale la extensión de Microsoft Analysis Services Projects en Visual Studio.	Administrador de sistemas
Cree un proyecto.	Cree un nuevo proyecto de modelo tabular en Visual Studio para almacenar los datos de Amazon Redshift. En Visual Studio, seleccione la opción Analysis Services Tabular Project (Proyecto tabular de Analysis Services) al crear el proyecto.	Administrador de base de datos

Cree un origen de datos y tablas de importación

Tarea	Descripción	Habilidades requeridas
Cree un origen de datos de Amazon Redshift.	Cree un origen de datos de Amazon Redshift mediante Intellisoft OLE DB Provider para Amazon Redshift (o bien CData ADO.NET Provider para Amazon Redshift) y sus credenciales de Amazon Redshift.	Amazon Redshift, administrador de base de datos
Importar tablas.	Seleccione e importe tablas y vistas de Amazon Redshift a su proyecto de SQL Server Analysis Services.	Amazon Redshift, administrador de base de datos

Limpiar después de la migración

Tarea	Descripción	Habilidades requeridas
Elimine la instancia de EC2.	Elimine la instancia de EC2 que lanzó anteriormente.	Administrador de sistemas

Recursos relacionados

- Amazon Redshift (Documentación de AWS)
- Install SQL Server Analysis Services (Instalar SQL Server Analysis Services) (documentación de Microsoft)
- Tabular Model Designer (Diseñador de modelos tabulares) (documentación de Microsoft)
- Overview of OLAP cubes for advanced analytics (Descripción general de los cubos OLAP para análisis avanzados) (documentación de Microsoft)
- Microsoft Visual Studio 2019 (Community Edition)
- Intellisoft OLE DB Provider for Amazon Redshift (Trial)

- CData ADO.NET Provider for Amazon Redshift (Trial)

Analice y visualice datos JSON anidados con Amazon Athena y Amazon QuickSight

Creado por Anoop Singh (AWS)

Entorno: PoC o piloto	Tecnologías: análisis; bases de datos	Servicios de AWS: Amazon Athena; Amazon QuickSight

Resumen

Este patrón explica cómo convertir una estructura de datos anidada con formato JSON en una vista tabular mediante Amazon Athena y, a continuación, visualizar los datos en Amazon. QuickSight

Puede usar datos con formato JSON para fuentes de datos de sistemas operativos basadas en API para crear productos de datos. Estos datos también pueden ayudarle a comprender mejor a sus clientes y sus interacciones con sus productos, de forma que pueda personalizar las experiencias de los usuarios y predecir los resultados.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Un archivo JSON que representa una estructura de datos anidada (este patrón proporciona un archivo de ejemplo)

Limitaciones:

- Las funciones de JSON se integran bien con las funciones orientadas a SQL existentes en Athena. Sin embargo, no son compatibles con ANSI SQL y se espera que el archivo JSON contenga cada registro en una línea separada. Puede que tengas que usar la `ignore.malformed.json` propiedad de Athena para indicar si los registros JSON con formato incorrecto deben convertirse en caracteres nulos o generar errores. Para obtener más información, consulte Prácticas recomendadas para leer datos JSON en la documentación de Athena.

- Este patrón considera solo cantidades pequeñas y simples de datos con formato JSON. Si desea utilizar estos conceptos a gran escala, considere la posibilidad de aplicar la partición de datos y consolidar los datos en archivos más grandes.

Arquitectura

El siguiente diagrama muestra la arquitectura y el flujo de trabajo de este patrón. Las estructuras de datos anidadas se almacenan en Amazon Simple Storage Service (Amazon S3) en formato JSON. En Athena, los datos JSON se asignan a una estructura de datos de Athena. A continuación, se crea una vista para analizar los datos y visualizar la estructura de datos en ella. QuickSight

Herramientas

Servicios de AWS

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos. Este patrón utiliza Amazon S3 para almacenar el archivo JSON.
- Amazon Athena es un servicio de consultas interactivo que facilita el análisis de datos en Amazon S3 con SQL estándar. Este patrón usa Athena para consultar y transformar los datos JSON. Con unas cuantas acciones en el AWS Management Console, puede dirigir Athena a sus datos en Amazon S3 y utilizar SQL estándar para ejecutar consultas únicas. Athena no tiene servidores, por lo que no es necesario configurar ni administrar ninguna infraestructura, y solo paga por las consultas que ejecuta. Athena escala automáticamente y ejecuta consultas en paralelo, por lo que los resultados son rápidos, incluso con conjuntos de datos grandes y consultas complejas.
- Amazon QuickSight es un servicio de inteligencia empresarial (BI) a escala de nube que te ayuda a visualizar, analizar y elaborar informes sobre tus datos en un único panel. QuickSight le permite crear y publicar fácilmente paneles interactivos que incluyen información sobre el aprendizaje automático (ML). Puede acceder a estos paneles desde cualquier dispositivo e integrarlos en sus aplicaciones, portales y sitios web.

Código de ejemplo

El siguiente archivo JSON proporciona una estructura de datos anidada que puede utilizar en este patrón.

```
{
  "symbol": "AAPL",
  "financials": [
    {
      "reportDate": "2017-03-31",
      "grossProfit": 20591000000,
      "costOfRevenue": 32305000000,
      "operatingRevenue": 52896000000,
      "totalRevenue": 52896000000,
      "operatingIncome": 14097000000,
      "netIncome": 11029000000,
      "researchAndDevelopment": 2776000000,
      "operatingExpense": 6494000000,
      "currentAssets": 101990000000,
      "totalAssets": 334532000000,
      "totalLiabilities": 200450000000,
      "currentCash": 15157000000,
      "currentDebt": 13991000000,
      "totalCash": 67101000000,
      "totalDebt": 98522000000,
      "shareholderEquity": 134082000000,
      "cashChange": -1214000000,
      "cashFlow": 12523000000,
      "operatingGainsLosses": null
    }
  ]
}
```


Epics

Configure un bucket de S3

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3.	Para crear un bucket para almacenar el archivo JSON, inicie sesión en AWS Management Console, abra la consola Amazon S3 y, a continuación, seleccione Create bucket. Para obtener	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	más información, consulte Crear un bucket en la documentación de Amazon S3.	
Añada los datos JSON anidados.	Sube tu archivo JSON al bucket de S3. Para ver un ejemplo de archivo JSON, consulta la sección anterior. Para más instrucciones, consulte Cargar objetos en la documentación de Amazon S3.	Administrador de sistemas

Analice datos en Athena

Tarea	Descripción	Habilidades requeridas
Cree una tabla para mapear los datos de JSON.	1. Abre la consola Athena. 2. Cree una base de datos siguiendo las instrucciones de la documentación de Athena. 3. En el menú Base de datos, elija la base de datos que ha creado. 4. En el editor de consultas , introduzca una `CREATE TABLE` sentencia como la siguiente: `CREATE EXTERNAL TABLE financials_json ( symbol string, financials array<`	Desarrollador

Tarea	Descripción	Habilidades requeridas
	<pre>struct<re portdate: string, grossprof it: bigint, totalreve nue: bigint, totalcash : bigint, totaldebt : bigint, researcha nddevelopment: bigint>>) ROW FORMAT SERDE 'org.openx.data.js onserde.JsonSerDe' LOCATION 's3://s3b ucket-for-athena/'</pre> donde `LOCATION` especific a la ubicación del depósito de S3 que contiene el archivo JSON. 5. Elija Ejecutar para crear la tabla. Para obtener más informaci ón sobre la creación de tablas, consulte la documentación de Athena.	

Tarea	Descripción	Habilidades requeridas
Cree una vista para el análisis de datos.	1. Abre la consola Athena. 2. Cree una base de datos siguiendo las instrucciones de la documentación de Athena. 3. En el menú Base de datos, elija la base de datos que ha creado. 4. En el editor de consultas , introduzca una `CREATE VIEW` sentencia como la siguiente: `CREATE OR REPLACE VIEW financial_json_view AS SELECT symbol, financials[1].reportdate one_report_date, -- indexes start with 1 financials[1].totalrevenue one_total_revenue, financials[1].reportdate another_report_date, financials[1].totalrevenue another_total_revenue FROM financials_json where symbol='AAPL' ORDER BY 1` 5. Elija Ejecutar para crear la vista.	Desarrollador

Tarea	Descripción	Habilidades requeridas
	Para obtener más informaci ón sobre la creación de vistas, consulte la documentación de Athena.	
Analice y valide los datos.	1. Abre la consola Athena. 2. En el editor de consultas, ejecute las consultas con la vista que creó en el paso anterior. 3. Valide los datos con el archivo JSON para confirmar que los nombres de las columnas y los tipos de datos están mapeados correctamente.	Desarrollador

Visualice los datos en QuickSight

Tarea	Descripción	Habilidades requeridas
Configure Athena como fuente de datos en. QuickSight	1. Abra la consola de AWS CloudFormation. 2. Elija Conjuntos de datos, Nuevo conjunto de datos. 3. Elija Athena como fuente de datos. 4. Elija la base de datos que incluye la vista que ha creado. 5. Elija la vista para la que desee crear un conjunto de datos.	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	6. En la página Finalizar la creación del conjunto de datos, selecciona Consultar directamente tus datos. 7. Elija Visualize.	
Visualice los datos en QuickSight.	1. Después de visualizar el conjunto de datos, elija las imágenes del panel izquierdo y elija los campos para el conjunto de datos. Para obtener más informaci ón, consulte el tutorial en la QuickSight documentación. 2. Guarde los cambios en el análisis. 3. Elija Publicar panel para publicar las imágenes que ha creado.	Analista de datos

Recursos relacionados

- Documentación de Amazon Athena
- QuickSight Tutoriales de Amazon
- Trabajando con JSON anidado (entrada de blog)

Automatice la aplicación del cifrado en AWS Glue mediante una CloudFormation plantilla de AWS

Creado por Diogo Guedes (AWS)

Repositorio de código: AWS Glue Encryption Enforcement	Entorno: producción	Tecnologías: análisis; seguridad, identidad, conformidad
Carga de trabajo: todas las demás cargas de trabajo	Servicios de AWS: Amazon EventBridge; AWS Glue; AWS KMS; AWS Lambda; AWS CloudFormation	

Resumen

Este patrón muestra cómo configurar y automatizar la aplicación del cifrado en AWS Glue mediante una CloudFormation plantilla de AWS. La plantilla crea todas las configuraciones y los recursos necesarios para aplicar el cifrado. Estos recursos incluyen una configuración inicial, un control preventivo creado por una EventBridge regla de Amazon y una función de AWS Lambda.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Permisos para implementar la CloudFormation plantilla y sus recursos

Limitaciones

Este control de seguridad es regional. Debe implementar el control de seguridad en cada región de AWS en la que desee configurar la aplicación del cifrado en AWS Glue.

Arquitectura

Pila de tecnología de destino

- Amazon CloudWatch Logs (de AWS Lambda)
- EventBridge Regla de Amazon
- CloudFormation Pila de AWS
- AWS CloudTrail
- Rol y política gestionados de AWS Identity and Access Management (IAM)
- AWS Key Management Service (AWS KMS)
- Alias de AWS KMS
- Función de AWS Lambda
- Almacén de parámetros de AWS Systems Manager

Arquitectura de destino

En el siguiente diagrama, se muestra cómo automatizar la aplicación del cifrado en AWS Glue.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Una CloudFormation plantilla crea todos los recursos, incluida la configuración inicial y el control de detección para la aplicación del cifrado en AWS Glue.
2. Una EventBridge regla detecta un cambio de estado en la configuración de cifrado.
3. Se invoca una función Lambda para la evaluación y el registro a través CloudWatch de los registros. En caso de detección de incumplimiento, se recupera el almacén de parámetros con un nombre de recurso de Amazon (ARN) como clave de AWS KMS. Se corrige el estado de cumplimiento del servicio con el cifrado activado.

Automatizar y escalar

Si utiliza AWS Organizations, puede utilizar AWS CloudFormation StackSets para implementar esta plantilla en varias cuentas en las que desee habilitar la aplicación del cifrado en AWS Glue.

Herramientas

- Amazon le CloudWatch ayuda a monitorizar las métricas de sus recursos de AWS y las aplicaciones que ejecuta en AWS en tiempo real.

- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, funciones de Lambda, puntos de conexión de invocación HTTP que utilizan destinos API o buses de eventos en otras cuentas de AWS.
- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- AWS le CloudTrail ayuda a habilitar la auditoría operativa y de riesgos, la gobernanza y el cumplimiento de su cuenta de AWS.
- AWS Glue es un servicio de extracción, transformación y carga (ETL) completamente administrado. Ayuda a clasificar, limpiar, enriquecer y mover datos de forma fiable entre almacenes de datos y flujos de datos.
- AWS Key Management Service (AWS KMS) facilita poder crear y controlar claves criptográficas para proteger los datos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Systems Manager le permite administrar las aplicaciones y la infraestructura que se ejecutan en la nube de AWS. Simplifica la administración de aplicaciones y recursos, reduce el tiempo requerido para detectar y resolver problemas operativos y ayuda a utilizar y administrar los recursos de AWS a escala de manera segura.

Código

El código de este patrón está disponible en el repositorio GitHub aws-custom-guardrail-event-driven.

Prácticas recomendadas

AWS Glue admite el cifrado de datos en reposo para la creación de trabajos en AWS Glue y el desarrollo de scripts mediante puntos de conexión de desarrollo.

Tenga en cuenta las siguientes prácticas recomendadas:

- Configure trabajos ETL y puntos de conexión de desarrollo para utilizar claves de AWS KMS para escribir datos cifrados en reposo.
- Cifre los metadatos almacenados en el catálogo de datos de AWS Glue mediante claves que administra a través de KMS de AWS.

- Además, puede usar las claves KMS de AWS para cifrar marcadores de trabajo y los registros que generan los rastreadores y los trabajos de ETL.

Epics

Lance la plantilla CloudFormation

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation plantilla.	Descargue la `aws-custom-guardrail-event-driven.yaml` plantilla del GitHub repositorio y, a continuación, impleméntela. El estado `CREATE_COMPLETE` indica que su plantilla se implementó correctamente. Nota: La plantilla no requiere parámetros de entrada.	Arquitecto de la nube

Compruebe la configuración de cifrado en AWS Glue

Tarea	Descripción	Habilidades requeridas
Compruebe las configuraciones clave de AWS KMS.	1. Inicie sesión en la consola de administración de AWS y, a continuación, abra la consola de AWS Glue. 2. En el panel de navegación, en Data Catalog (Catálogo de datos), elija Catalog settings (Configuración de catálogo). 3. Compruebe que los ajustes de cifrado de metadatos y	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	cifrado de contraseñas de conexión estén marcados y configurados para usar `KMSKeyGlue` .	

Pruebe la aplicación del cifrado

Tarea	Descripción	Habilidades requeridas
Identifique la configuración de cifrado en CloudFormation.	1. Inicie sesión en la consola de administración de AWS y, a continuación, abra la CloudFormation consola. 2. En el panel de navegación, elija Stacks (Pilas) y, a continuación, elija la pila que desee. 3. Elija la pestaña Recursos. 4. En la tabla de Resources (Recursos), busque la configuración de cifrado por Logical ID (ID lógico).	Arquitecto de la nube
Cambie la infraestructura aprovisionada a un estado que no cumpla con las normas.	1. Inicie sesión en la consola de administración de AWS y, a continuación, abra la consola de AWS Glue. 2. En el panel de navegación, en Data Catalog (Catálogo de datos), elija Catalog settings (Configuración de catálogo). 3. Desactive la casilla de verificación Metadata	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	encryption (Cifrado de metadatos). 4. Desactive la casilla de verificación Encrypt connection passwords (Cifrar contraseñas de conexión). 5. Seleccione Save (Guardar). 6. Actualice la consola de AWS Glue. La barrera de protección detecta el estado no conforme en AWS Glue después de desactivar las casillas y, a continuación, aplica el cumplimiento corrigiendo automáticamente el error de configuración del cifrado. Como resultado, las casillas de verificación de cifrado deberían volver a seleccion arse después de actualizar la página.	

Recursos relacionados

- Creación de una pila en la CloudFormation consola de AWS (CloudFormation documentación de AWS)
- Creación de una regla de CloudWatch eventos que se active en una llamada a la API de AWS mediante AWS CloudTrail (CloudWatch documentación de Amazon)
- Configuración del cifrado en AWS Glue (documentación de AWS Glue)

Cree una canalización de servicios de ETL para cargar datos de forma incremental desde Amazon S3 a Amazon Redshift mediante AWS Glue

Creado por Rohan Jamadagni (AWS) y Arunabha Datta (AWS)

Entorno: producción	Tecnologías: análisis; lagos de datos; almacenamiento y copia de seguridad	Servicios de AWS: Amazon Redshift; Amazon S3; AWS Glue; AWS Lambda

Resumen

Este patrón proporciona orientación sobre cómo configurar Amazon Simple Storage Service (Amazon S3) para obtener un rendimiento óptimo del lago de datos y, a continuación, cargar los cambios incrementales de datos de Amazon S3 en Amazon Redshift mediante AWS Glue, realizando operaciones de extracción, transformación y carga (ETL).

Los archivos de origen de Amazon S3 pueden tener distintos formatos, incluidos valores separados por comas (CSV), archivos XML y JSON. Este patrón describe cómo puede utilizar AWS Glue para convertir los archivos de origen en un formato optimizado para los costos y el rendimiento, como Apache Parquet. Puede consultar los archivos de Parquet directamente desde Amazon Athena y Amazon Redshift Spectrum. También puede cargar archivos de Parquet en Amazon Redshift, agregarlos y compartir los datos agregados con los consumidores o visualizar los datos mediante Amazon. QuickSight

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Un bucket de origen de S3 que tenga los privilegios adecuados y que contenga archivos CSV, XML o JSON.

Supuestos

- Los archivos de origen CSV, XML o JSON ya están cargados en Amazon S3 y se puede acceder a ellos desde la cuenta en la que están configurados AWS Glue y Amazon Redshift.
- Se siguen las prácticas recomendadas para cargar los archivos, dividirlos, comprimirlos y utilizar un manifiesto, tal como se describe en la documentación de Amazon Redshift.
- La estructura de los archivos de origen permanece inalterada.
- El sistema de origen puede incorporar datos en Amazon S3 siguiendo la estructura de carpetas definida en Amazon S3.
- El clúster de Amazon Redshift abarca una sola zona de disponibilidad. (Esta arquitectura es adecuada porque AWS Lambda, AWS Glue y Amazon Athena están sin servidor). Para una alta disponibilidad, se toman instantáneas de los clústeres con una frecuencia regular.

Limitaciones

- Los formatos de archivo se limitan a los que actualmente admite AWS Glue.
- No se admite la generación de informes posteriores en tiempo real.

Arquitectura

Pila de tecnología de origen

- Bucket de S3 con archivos CSV, XML o JSON

Pila de tecnología de destino

- Lago de datos de S3 (con almacenamiento de archivos Parquet particionado)
- Amazon Redshift

Arquitectura de destino

Flujo de datos

Herramientas

- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos altamente escalable. Amazon S3 puede utilizarse para una amplia gama de soluciones de almacenamiento, incluidos sitios web, aplicaciones móviles, copias de seguridad y lagos de datos.
- AWS Lambda: AWS Lambda le permite ejecutar código sin aprovisionar ni administrar servidores. AWS Lambda es un servicio basado en eventos; puede configurar el código para que se inicie automáticamente desde otros servicios de AWS.
- Amazon Redshift: Amazon Redshift es un servicio de almacenamiento de datos totalmente administrado de varios petabytes. Con Amazon Redshift, puede consultar petabytes de datos estructurados y semiestructurados en su almacenamiento de datos y su lago de datos mediante SQL estándar.
- AWS Glue: AWS Glue es un servicio ETL totalmente gestionado que facilita la preparación y la carga de datos para su análisis. AWS Glue descubre sus datos y almacena los metadatos asociados (por ejemplo, definiciones de tablas y esquemas) en el catálogo de datos de AWS Glue. Sus datos catalogados se pueden buscar, consultar y están disponibles para ETL inmediatamente.
- AWS Secrets Manager: AWS Secrets Manager facilita la protección y la administración centralizada de los secretos necesarios para el acceso a aplicaciones o servicios. El servicio almacena credenciales de bases de datos, claves de API y otros datos confidenciales y elimina la necesidad de codificar de forma rígida la información confidencial en formato de texto sin formato. Secrets Manager también ofrece rotación de claves para satisfacer las necesidades de seguridad y cumplimiento. Incorpora una integración para Amazon Redshift, Amazon Relational Database Service (Amazon RDS) y Amazon DocumentDB. Puede almacenar y gestionar secretos de forma centralizada a través de la consola de Secrets Manager, la interfaz de la línea de comandos (CLI) o la API y los SDK de Secrets Manager.
- Amazon Athena : Amazon Athena es un servicio de consultas interactivo que facilita el análisis de datos que están almacenados en Amazon S3. Athena no tiene servidor y está integrada con AWS Glue, por lo que puede consultar directamente los datos catalogados con AWS Glue. Athena se escala con elasticidad para ofrecer un rendimiento de consultas interactivas.

Epics

Cree los buckets y la estructura de carpetas de S3

Tarea	Descripción	Habilidades requeridas
Analice los sistemas de origen para determinar la estructura y los atributos de los datos.	Realice esta tarea para cada origen de datos que contribuya al lago de datos de Amazon S3.	Ingeniero de datos
Defina la estrategia de partición y acceso.	Esta estrategia debe basarse en la frecuencia de las capturas de datos, el procesamiento delta y las necesidades de consumo. Asegúrese de que los buckets de S3 no estén abiertos al público y de que el acceso esté controlado únicamente por políticas específicas basadas en los roles de servicio. Para obtener más información, consulte la documentación de Amazon S3.	Ingeniero de datos
Cree buckets de S3 independientes para cada tipo de origen de datos y un bucket de S3 independiente por origen para los datos procesados (Parquet).	Cree un bucket independiente para cada origen y, a continuación, cree una estructura de carpetas que se base en la frecuencia de ingesta de datos del sistema de origen; por ejemplo, `s3://source-system-name/date/hour` . Para los archivos procesados (converti	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	dos al formato Parquet), cree una estructura similar; por ejemplo, `s3://source-processed-bucket/date/hour` . Para más información sobre cómo crear buckets de S3, consulte la documentación de Amazon S3.	

Creación de un almacenamiento de datos en Amazon Redshift

Tarea	Descripción	Habilidades requeridas
Lance el clúster de Amazon Redshift con los grupos de parámetros y la estrategia de mantenimiento y copia de seguridad adecuados.	Utilice el secreto de la base de datos de Secrets Manager como credenciales de usuario administrador al crear el clúster de Amazon Redshift. Para obtener informaci ón sobre la creación y el tamaño de un clúster de Amazon Redshift, consulte la documentación de Amazon Redshift y el documento técnico sobre el tamaño del almacenamiento de datos en la nube.	Ingeniero de datos
Cree y asocie un rol de servicio de IAM al clúster de Amazon Redshift.	El rol de servicio AWS Identity and Access Management (IAM) garantiza el acceso a Secrets Manager y a los buckets de S3 de origen. Para obtener más información,	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	consulte la documentación de AWS sobre la autorización y la adición de un rol.	
Crear el esquema de la base de datos.	Siga las prácticas recomendadas de Amazon Redshift para el diseño de tablas. Según el caso de uso, elija las claves de clasificación y distribución adecuadas y la mejor codificación de compresión posible. Para conocer las prácticas recomendadas, consulte la documentación de AWS.	Ingeniero de datos
Configure la administración de cargas de trabajo.	Configure las colas de administración de la carga de trabajo (WLM), la aceleración de consultas cortas (SQA) o el escalado simultáneo, según sus necesidades. Para obtener más información, consulte Implementación de la administración de la carga de trabajo en la documentación de Amazon Redshift.	Ingeniero de datos

Cree un secreto en Secrets Manager

Tarea	Descripción	Habilidades requeridas
Cree un nuevo secreto para almacenar las credenciales de inicio de sesión de Amazon Redshift en Secrets Manager.	Este secreto almacena las credenciales del usuario administrador y de los usuarios individuales del	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	servicio de base de datos. Para obtener instrucciones, consulte la documentación de Secretes Manager. Elija Amazon Redshift Cluster como tipo de secreto. Además, en la página de rotación secreta, active la rotación. Esto creará el usuario adecuado en el clúster de Amazon Redshift y cambiará las claves secretas a intervalos definidos.	
Cree una política de IAM para restringir el acceso a Secrets Manager.	Restrinja el acceso a Secrets Manager solo a los administr adores de Amazon Redshift y a AWS Glue.	Ingeniero de datos

Configuración de AWS Glue

Tarea	Descripción	Habilidades requeridas
En el catálogo de datos de AWS Glue, añada una conexión para Amazon Redshift.	Para obtener instrucciones, consulte la documentación de AWS Glue.	Ingeniero de datos
Cree y asocie un rol de servicio de IAM para que AWS Glue pueda acceder a los buckets de Secrets Manager, Amazon Redshift y S3.	Para obtener más información, consulte la documentación de AWS Glue.	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
Defina el catálogo de datos de AWS Glue para el origen.	Este paso implica crear una base de datos y las tablas necesarias en el catálogo de datos de AWS Glue. Puede utilizar un rastreador para catalogar las tablas de la base de datos de AWS Glue o definirlas como tablas externas de Amazon Athena. También puede acceder a las tablas externas definidas en Athena a través del catálogo de datos de AWS Glue. Consulte la documentación de AWS para obtener más información sobre la definición del catálogo de datos y la creación de una tabla externa en Athena.	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
Cree un trabajo de AWS Glue para procesar los datos de origen.	El trabajo de AWS Glue puede ser un shell de Python o PySpark estandarizar, deduplicar y limpiar los archivos de datos de origen. Para optimizar el rendimiento y evitar tener que consultar todo el bucket de código fuente de S3, particione el bucket de S3 por fecha, desglosado por año, mes, día y hora como predicado desplegable para el trabajo de AWS Glue. Para obtener más información, consulte la documentación de AWS Glue. Cargue los datos procesados y transformados en las particiones del bucket de S3 procesadas en formato Parquet. Puede consultar los archivos de Parquet en Athena.	Ingeniero de datos
Cree un trabajo de AWS Glue para cargar datos en Amazon Redshift.	El trabajo de AWS Glue puede consistir en un shell de Python o PySpark cargar los datos alterándolos y, a continuación, realizar una actualización completa. Para obtener más información, consulte la documentación de AWS Glue y la sección de información adicional.	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
(Opcional) Programe los trabajos de AWS Glue mediante activadores según sea necesario.	La carga de datos incremental se debe principalmente a un evento de Amazon S3 que hace que una función de AWS Lambda llame a la tarea de AWS Glue. Utilice la programación basada en activadores de AWS Glue para cualquier carga de datos que exija una programación basada en el tiempo en lugar de en los eventos.	Ingeniero de datos

Crear una función de Lambda

Tarea	Descripción	Habilidades requeridas
Cree y adjunte un rol vinculado a un servicio de IAM para que AWS Lambda pueda acceder a los buckets de S3 y al trabajo de AWS Glue.	Cree un rol vinculado a un servicio de IAM para AWS Lambda con una política para leer los objetos y buckets de Amazon S3 y una política para acceder a la API de AWS Glue para iniciar un trabajo de AWS Glue. Para obtener más información, consulte el Centro de conocimientos.	Ingeniero de datos
Cree una función de Lambda para ejecutar el trabajo de AWS Glue en función del evento Amazon S3 definido.	La función de Lambda debe iniciarse con la creación del archivo de manifiesto de Amazon S3. La función de Lambda debe pasar la ubicación de la carpeta de	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	Amazon S3 (por ejemplo, source_bucket/year/month/date/hour) al trabajo de AWS Glue como parámetro . El trabajo de AWS Glue utilizará este parámetro como predicado desplegable para optimizar el acceso a los archivos y el rendimiento del procesamiento de los trabajos. Para obtener más información, consulte la documentación de AWS Glue.	
Cree un evento de objeto PUT de Amazon S3 para detectar la creación de objetos y llame a la función de Lambda correspondiente.	El evento de objeto PUT de Amazon S3 debe iniciarse solo con la creación del archivo de manifiesto. El archivo de manifiesto controla la función de Lambda y la simultaneidad de las tareas de AWS Glue, y procesa la carga como un lote en lugar de procesar los archivos individuales que llegan a una partición específica del bucket de origen de S3. Para más información, consulte la documentación de Lambda.	Ingeniero de datos

Recursos relacionados

- Documentación de Amazon RDS
- Documentación de AWS Glue

- Documentación de Amazon Redshift
- AWS Lambda
- Amazon Athena
- AWS Secrets Manager

Información adicional

Enfoque detallado para una actualización automática y completa

Upsert: se trata de conjuntos de datos que requieren un agrupado histórico, según el caso de uso empresarial. Siga uno de los enfoques descritos en Actualización e inserción de datos nuevos (documentación de Amazon Redshift) en función de las necesidades de su empresa.

Actualización completa: se trata de conjuntos de datos pequeños que no necesitan agrupados históricos. Siga uno de estos enfoques:

1. Trunque la tabla de Amazon Redshift.
2. Cargue la partición actual desde el área de montaje

o bien:

1. Cree una tabla temporal con datos de partición actuales.
2. Elimine la tabla de destino de Amazon Redshift.
3. Cambie el nombre de la tabla temporal a tabla de destino.

Calcule el valor en riesgo (VaR) mediante los servicios de AWS

Creado por Sumon Samanta (AWS)

Entorno: PoC o piloto	Tecnologías: Análisis; Sin servidor	Servicios de AWS: Amazon Kinesis Data Streams; AWS Lambda; Amazon SQS; Amazon ElastiCache

Resumen

Este patrón describe cómo implementar un sistema de cálculo del valor en riesgo (VaR) mediante los servicios de AWS. En un entorno en las instalaciones, la mayoría de los sistemas VaR emplean una gran infraestructura dedicada y un software de programación de redes interno o comercial para ejecutar procesos por lotes. Este patrón presenta una arquitectura simple, fiable y escalable para gestionar el procesamiento de VaR en la nube de AWS. Crea una arquitectura sin servidor que utiliza Amazon Kinesis Data Streams como servicio de streaming, Amazon Simple Queue Service (Amazon SQS) como servicio de colas gestionado ElastiCache , Amazon como servicio de almacenamiento en caché y AWS Lambda para procesar los pedidos y calcular el riesgo.

El VaR es una medida estadística que usan los operadores y gestores de riesgos para estimar las posibles pérdidas de su cartera más allá de cierto nivel de confianza. La mayoría de los sistemas VaR implican la ejecución de una gran cantidad de cálculos matemáticos y estadísticos, así como el almacenamiento de los resultados. Estos cálculos requieren importantes recursos de cómputo, por lo que los procesos por lotes del VaR deben dividirse en conjuntos más pequeños de tareas de computación. Es posible dividir un lote grande en tareas más pequeñas, ya que estas tareas son, en su mayoría, independientes (es decir, los cálculos de una tarea no dependen de otras tareas).

Otro requisito importante de una arquitectura de VaR es la escalabilidad de la computación. Este patrón emplea una arquitectura sin servidor que escala vertical u horizontalmente de manera automática en función de la carga de cálculo. Como la demanda de procesamiento por lotes o en línea es difícil de predecir, es necesario contar con un escalado dinámico para completar el proceso dentro del plazo impuesto por un acuerdo de nivel de servicio (SLA). Además, una arquitectura con costos optimizados debería poder reducir verticalmente la escala de cada recurso informático tan pronto como se completen las tareas de ese recurso.

Los servicios de AWS son adecuados para los cálculos de VaR, ya que ofrecen procesamiento y almacenamiento escalables, servicios de análisis para el procesamiento con costos optimizados y diferentes tipos de programadores para ejecutar los flujos de trabajo de administración de riesgos. Además, usted solo paga por los recursos de almacenamiento y computación que usa en AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Archivos de entrada, que dependen de las necesidades de su empresa. Un caso de uso típico incluye los siguientes archivos de entrada:
  - Archivo de datos de mercado (entrada al motor de cálculo del VaR)
  - Archivo de datos comerciales (a menos que los datos comerciales provengan de un flujo).
  - Archivo de datos de configuración (modelo y otros datos de configuración estáticos)
  - Archivos de modelo de motor de cálculo (bibliotecas cuantitativas)
  - Archivo de datos de serie temporal (para datos históricos, como el precio de las acciones de los últimos cinco años)
- Si los datos de mercado u otra entrada provienen de un flujo, permisos de Amazon Kinesis Data Streams y Amazon Identity and Access Management (IAM) configurados para escribir en dicho flujo.

Este patrón crea una arquitectura en la que los datos comerciales se escriben desde un sistema comercial a un flujo de datos de Kinesis. En lugar de usar un servicio de streaming, puede guardar sus datos comerciales en archivos de lotes pequeños, almacenarlos en un bucket de Amazon Simple Storage Service (Amazon S3) e invocar un evento para comenzar a procesar los datos.

Limitaciones

- La secuenciación del flujo de datos de Kinesis está garantizada en cada partición, por lo que no se garantiza que las órdenes comerciales que se escriben en varias particiones se entreguen en el mismo orden que las operaciones de escritura.
- Actualmente, el límite de tiempo de ejecución de AWS Lambda es de 15 minutos. (Para más información, consulte las Preguntas frecuentes sobre Lambda)

Arquitectura

Arquitectura de destino

El siguiente diagrama de arquitectura muestra los servicios y flujos de trabajo de AWS para el sistema de evaluación de riesgos.

En el siguiente diagrama se ilustra lo siguiente:

1. Las operaciones se transmiten desde el sistema de gestión de pedidos.
2. La función de Lambda de compensación de posiciones de tickets procesa los pedidos y escribe los mensajes consolidados de cada ticker en una cola de riesgos de Amazon SQS.
3. La función Lambda del motor de cálculo de riesgos procesa los mensajes de Amazon SQS, realiza cálculos de riesgo y actualiza la información de pérdidas y ganancias (PnL) del VaR en la caché de riesgos de Amazon. ElastiCache
4. La función Lambda de lectura de ElastiCache datos recupera los resultados del riesgo y los almacena en una base de datos ElastiCache y en un bucket de S3.

Para obtener más información sobre estos servicios y pasos, consulte la sección Épica.

Automatizar y escalar

Puede implementar toda la arquitectura mediante el Kit de desarrollo en la nube de AWS (AWS CDK) o las CloudFormation plantillas de AWS. La arquitectura es compatible tanto con procesamiento por lotes como con procesamiento intradiario (en tiempo real).

El escalado está integrado en la arquitectura. A medida que se escriban más operaciones en el flujo de datos de Kinesis y estén pendientes de ser procesadas, es posible invocar funciones de Lambda adicionales para procesar esas operaciones y, a continuación, reducir verticalmente una vez finalizado el procesamiento. El procesamiento mediante varias colas de cálculo de riesgos de Amazon SQS también es una opción. Si es necesario mantener un orden o consolidación estrictos en todas las colas, el procesamiento no se puede paralelizar. Sin embargo, para un end-of-the-day lote o un minilote intradía, las funciones Lambda pueden procesar en paralelo y almacenar los resultados finales en él. ElastiCache

Herramientas

Servicios de AWS

- La edición de Amazon Aurora compatible con PostgreSQL es un motor de base de datos relacional compatible con MySQL y completamente administrado que le permite configurar, administrar y escalar implementaciones de MySQL. Este patrón emplea MySQL como ejemplo, pero puede usar cualquier sistema RDBMS para almacenar datos.
- Amazon le ElastiCache ayuda a configurar, gestionar y escalar entornos de caché en memoria distribuidos en la nube de AWS.
- Amazon Kinesis Data Streams lo ayuda a recopilar y procesar grandes secuencias de registros de datos en tiempo real.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Queue Service (Amazon SQS) ofrece una cola alojada segura, duradera y disponible que le permite integrar y desacoplar sistemas y componentes de software distribuidos.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Código

Este patrón proporciona un ejemplo de arquitectura para un sistema de VaR en la nube de AWS y describe cómo usar las funciones de Lambda para cálculos de VaR. Para crear las funciones de Lambda, consulte los ejemplos de código en la documentación de Lambda. Para obtener ayuda, póngase en contacto con AWS Professional Services.

Prácticas recomendadas

- Intente que cada tarea de cómputo del VaR sea lo más pequeña y ligera posible. Experimente con diferentes números de operaciones en cada tarea de cómputo para optimizar al máximo el tiempo y coste del cómputo.
- Almacena objetos reutilizables en Amazon ElastiCache. Use un marco como Apache Arrow para reducir la serialización y la deserialización.

- Tenga en cuenta la limitación de tiempo de Lambda. Si cree que sus tareas de computación pueden superar los 15 minutos, intente dividirlas en tareas más pequeñas para evitar el tiempo de espera de Lambda. Si no es posible, considere una solución de orquestación de contenedores con AWS Fargate, Amazon Elastic Container Service (Amazon ECS) y Amazon Elastic Kubernetes Service (Amazon EKS).

Epics

Sistema de flujo comercial a riesgo

Tarea	Descripción	Habilidades requeridas
Comience a escribir operaciones.	Las operaciones nuevas, liquidadas o parcialmente liquidadas se escriben desde el sistema de gestión de pedidos a un flujo de riesgo. Este patrón usa Amazon Kinesis como servicio de flujo gestionado. El hash del ticker de la orden comercial se usa para colocar las órdenes comerciales en varias particiones.	Amazon Kinesis

Ejecute funciones de Lambda para el procesamiento de pedidos

Tarea	Descripción	Habilidades requeridas
Inicie el procesamiento de riesgos con Lambda.	Ejecute una función de Lambda de AWS para los nuevos pedidos. En función del número de órdenes comerciales pendientes, Lambda escalará automáticamente. Cada instancia de	Amazon Kinesis, AWS Lambda, Amazon ElastiCache

Tarea	Descripción	Habilidades requeridas
	Lambda tiene uno o más pedidos y recupera la última posición de cada ticker de Amazon. ElastiCache (Puede utilizar un identificador CUSIP, un nombre de curva o un nombre de índice para otros productos derivados financieros como clave para almacenar y recuperar datos). ElasticCache En ElastiCache, la posición total (cantidad) y el par clave-valor < indicador , posición neta >, donde la posición neta es el factor de escala, se actualizan una vez para cada indicador.	

Escriba los mensajes de cada ticker en la cola

Tarea	Descripción	Habilidades requeridas
Escriba mensajes consolida dos en la cola de riesgos.	Escriba el mensaje en una cola. Este patrón emplea Amazon SQS como servicio de colas gestionado. Una sola instancia de Lambda puede recibir un minilote de órdenes comerciales en un momento dado, pero solo escribirá un mensaje para cada ticker en Amazon SQS. Se calcula un factor de escala: (posición	Amazon SQS, AWS Lambda

Tarea	Descripción	Habilidades requeridas
	neta anterior + posición actual) / posición neta anterior.	

Invoque el motor de riesgo

Tarea	Descripción	Habilidades requeridas
Inicie los cálculos de riesgo.	Se invoca la función de Lambda para el motor de riesgo Lambda. Cada posición es procesada por una sola función de Lambda. Sin embargo, con fines de optimización, cada función de Lambda puede procesar varios mensajes de Amazon SQS.	Amazon SQS, AWS Lambda

Recupere los resultados de riesgo de la memoria caché

Tarea	Descripción	Habilidades requeridas
Recupere y actualice la caché de riesgos.	Lambda recupera la posición neta actual de cada ticker de. ElastiCache También recupera una matriz de ganancias y pérdidas (pNL) de VaR para cada ticker de. ElastiCache Si la matriz pNL ya existe, la función de Lambda actualiza la matriz y el VaR con una escala que proviene del	Amazon SQS, AWS Lambda, Amazon ElastiCache

Tarea	Descripción	Habilidades requeridas
	mensaje de Amazon SQS escrito por la función Lambda de compensación. Si la matriz pNL no está incluida ElasticCache, se calculan un pNL y un VaR nuevos utilizando datos simulados de series de precios de cotizadores.	

Actualice los datos en Elastic Cache y almacénelos en la base de datos

Tarea	Descripción	Habilidades requeridas
Almacene los resultados de riesgo.	Una vez actualizados los números VaR y PnL ElastiCache, se invoca una nueva función Lambda cada cinco minutos. Esta función lee todos los datos almacenados ElastiCache y los almacena en una base de datos compatible con Aurora MySQL y en un bucket de S3.	AWS Lambda, Amazon ElastiCache

Recursos relacionados

- Marco VaR de Basel

Convierta la característica temporal NORMALIZE de Teradata en Amazon Redshift SQL

Origen: almacenamiento de datos de Teradata	Destino: Amazon Redshift	Tipo R: renovar arquitectura
Entorno: producción	Tecnologías: análisis; bases de datos; migración	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon Redshift		

Resumen

NORMALIZE es una extensión de Teradata del estándar ANSI SQL. Cuando una tabla SQL incluye una columna que tiene un tipo de datos tipo PERIOD, NORMALIZE combina los valores que coinciden o se superponen en esa columna para formar un período único que consolida varios valores de períodos individuales. Para utilizar NORMALIZE, al menos una columna de la lista SQL SELECT debe ser del tipo de datos PERIOD temporal de Teradata. Para obtener más información sobre NORMALIZE, consulte la documentación de Teradata.

Amazon Redshift no admite NORMALIZE, pero puede implementar esta funcionalidad mediante la sintaxis SQL nativa y la función de ventana LAG en Amazon Redshift. Este patrón se centra en el uso de la extensión NORMALIZE de Teradata con la condición ON MEETS OR OVERLAPS, que es el formato más popular. En él se explica cómo funciona esta función en Teradata y cómo se puede convertir a la sintaxis SQL nativa de Amazon Redshift.

Requisitos previos y limitaciones

Requisitos previos

- Conocimientos y experiencia básicos de Teradata SQL
- Conocimiento y experiencia en Amazon Redshift

Arquitectura

Pila de tecnología de origen

- Almacenamiento de datos de Teradata

Pila de tecnología de destino

- Amazon Redshift

Arquitectura de destino

Para obtener una arquitectura de alto nivel para migrar una base de datos de Teradata a Amazon Redshift, consulte el patrón Migración de una base de datos de Teradata a Amazon Redshift mediante agentes de extracción de datos SCT de AWS. La migración no convierte automáticamente la frase NORMALIZE de Teradata en Amazon Redshift SQL. Puede convertir esta extensión de Teradata siguiendo las pautas de este patrón.

Herramientas

Código

Para ilustrar el concepto y la funcionalidad de NORMALIZE, considere la siguiente definición de tabla en Teradata:

```
CREATE TABLE systest.project
     (    emp_id        INTEGER,
          project_name  VARCHAR(20),
          dept_id       INTEGER,
          duration      PERIOD(DATE)
     );
```

Ejecute el siguiente código SQL para insertar datos de ejemplo en la tabla:

```
BEGIN TRANSACTION;

INSERT INTO systest.project VALUES (10, 'First Phase', 1000,  PERIOD(DATE '2010-01-10',
 DATE '2010-03-20') );
INSERT INTO systest.project VALUES (10, 'First Phase', 2000,  PERIOD(DATE '2010-03-20',
 DATE '2010-07-15') );
```

```
INSERT INTO systest.project VALUES (10, 'Second Phase', 2000,  PERIOD(DATE
 '2010-06-15', DATE '2010-08-18') );
INSERT INTO systest.project VALUES (20, 'First Phase', 2000,  PERIOD(DATE '2010-03-10',
 DATE '2010-07-20') );

INSERT INTO systest.project VALUES (20, 'Second Phase', 1000,  PERIOD(DATE
 '2020-05-10', DATE '2020-09-20') );

END TRANSACTION;
```

Resultados:

```
select * from systest.project order by 1,2,3;

 *** Query completed. 4 rows found. 4 columns returned.
 *** Total elapsed time was 1 second.

     emp_id  project_name              dept_id  duration
-----------  --------------------  -----------  ------------------------
         10  First Phase                  1000  ('10/01/10', '10/03/20')
         10  First Phase                  2000  ('10/03/20', '10/07/15')
         10  Second Phase                 2000  ('10/06/15', '10/08/18')
         20  First Phase                  2000  ('10/03/10', '10/07/20')
         20  Second Phase                 1000  ('20/05/10', '20/09/20')
```

Caso de uso de Teradata NORMALIZE

Ahora añada la cláusula SQL NORMALIZE de Teradata a la sentencia SELECT::

```
SELECT NORMALIZE ON MEETS OR OVERLAPS emp_id, duration
FROM systest.project
ORDER BY 1,2;
```

Esta operación NORMALIZE se realiza en una sola columna (emp_id). Para emp_id=10, los tres valores de período superpuestos en duración se fusionan en un único valor de período, de la siguiente manera:

```
     emp_id  duration
-----------  ------------------------
         10  ('10/01/10', '10/08/18')
         20  ('10/03/10', '10/07/20')
```

```
         20  ('20/05/10', '20/09/20')
```

La siguiente instrucción SELECT realiza una operación NORMALIZE en project_name y dept_id. Tenga en cuenta que la lista SELECT contiene solo una columna PERIOD, la duración.

```
SELECT NORMALIZE project_name, dept_id, duration
FROM systest.project;
```

Salida:

```
project_name              dept_id  duration
--------------------  -----------  ------------------------
First Phase                  1000  ('10/01/10', '10/03/20')
Second Phase                 1000  ('20/05/10', '20/09/20')
First Phase                  2000  ('10/03/10', '10/07/20')
Second Phase                 2000  ('10/06/15', '10/08/18')
```

SQL equivalente a Amazon Redshift

Amazon Redshift actualmente no admite el tipo de datos PERIOD en una tabla. En su lugar, debe dividir un campo de datos PERIOD de Teradata en dos partes: fecha de inicio y fecha de finalización, de la siguiente manera:

```
CREATE TABLE systest.project
     (    emp_id        INTEGER,
          project_name  VARCHAR(20),
          dept_id       INTEGER,
          start_date  DATE,
          end_date    DATE
     );
```

Inserte una fila de datos en la tabla:

```
BEGIN TRANSACTION;

INSERT INTO systest.project VALUES (10, 'First Phase', 1000,  DATE '2010-01-10', DATE
 '2010-03-20' );
INSERT INTO systest.project VALUES (10, 'First Phase', 2000,  DATE '2010-03-20', DATE
 '2010-07-15');
```

```
INSERT INTO systest.project VALUES (10, 'Second Phase', 2000,  DATE '2010-06-15', DATE
 '2010-08-18' );
INSERT INTO systest.project VALUES (20, 'First Phase', 2000,  DATE '2010-03-10', DATE
 '2010-07-20' );

INSERT INTO systest.project VALUES (20, 'Second Phase', 1000,  DATE '2020-05-10', DATE
 '2020-09-20' );

END TRANSACTION;
```

Salida:

```
 emp_id | project_name | dept_id | start_date |  end_date
--------+--------------+---------+------------+------------
     10 | First Phase  |    1000 | 2010-01-10 | 2010-03-20
     10 | First Phase  |    2000 | 2010-03-20 | 2010-07-15
     10 | Second Phase |    2000 | 2010-06-15 | 2010-08-18
     20 | First Phase  |    2000 | 2010-03-10 | 2010-07-20
     20 | Second Phase |    1000 | 2020-05-10 | 2020-09-20
(5 rows)
```

Para reescribir la cláusula NORMALIZE de Teradata, puede utilizar la función de ventana LAG de Amazon Redshift. Esta función devuelve los valores para una fila en un desplazamiento dado arriba (antes) de la fila actual en la partición.

Puede usar la función LAG para identificar cada fila que comienza un nuevo período determinando si un período coincide o se superpone con el período anterior (0 en caso afirmativo y 1 en caso negativo). Cuando este indicador se suma de forma acumulativa, proporciona un identificador de grupo que se puede utilizar en la cláusula externa Group By para obtener el resultado deseado en Amazon Redshift.

A continuación, se muestra un ejemplo de sentencia SQL de Amazon Redshift que utiliza LAG():

```
SELECT emp_id, start_date, end_date,
            (CASE WHEN start_date <= LAG(end_date) OVER (PARTITION BY emp_id ORDER BY
 start_date, end_date) THEN 0 ELSE 1 END) AS GroupStartFlag
FROM systest.project
ORDER BY 1,2;
```

Salida:

```
 emp_id | start_date |  end_date  | groupstartflag
```

```
--------+------------+------------+----------------
     10 | 2010-01-10 | 2010-03-20 |              1
     10 | 2010-03-20 | 2010-07-15 |              0
     10 | 2010-06-15 | 2010-08-18 |              0
     20 | 2010-03-10 | 2010-07-20 |              1
     20 | 2020-05-10 | 2020-09-20 |              1
(5 rows)
```

La siguiente sentencia SQL de Amazon Redshift solo se normaliza en la columna emp_id:

```
SELECT T2.emp_id, MIN(T2.start_date) as new_start_date, MAX(T2.end_date) as
 new_end_date
FROM
( SELECT T1.*, SUM(GroupStartFlag) OVER (PARTITION BY emp_id ORDER BY start_date ROWS
 UNBOUNDED PRECEDING) As GroupID
FROM ( SELECT emp_id, start_date, end_date,
            (CASE WHEN start_date <= LAG(end_date) OVER (PARTITION BY emp_id ORDER BY
 start_date, end_date) THEN 0 ELSE 1 END) AS GroupStartFlag
FROM systest.project ) T1
) T2
GROUP BY T2.emp_id, T2.GroupID
ORDER BY 1,2;
```

Salida:

```
 emp_id | new_start_date | new_end_date
--------+----------------+--------------------------------------
     10 | 2010-01-10     | 2010-08-18
     20 | 2010-03-10     | 2010-07-20
     20 | 2020-05-10     | 2020-09-20
(3 rows)
```

La siguiente sentencia SQL de Amazon Redshift se normaliza en las columnas project_name y dept_id:

```
SELECT T2.project_name, T2.dept_id, MIN(T2.start_date) as new_start_date,
 MAX(T2.end_date) as new_end_date
FROM
( SELECT T1.*, SUM(GroupStartFlag) OVER (PARTITION BY project_name, dept_id ORDER BY
 start_date ROWS UNBOUNDED PRECEDING) As GroupID
```

```
FROM ( SELECT project_name, dept_id, start_date, end_date,
            (CASE WHEN start_date <= LAG(end_date) OVER (PARTITION BY project_name,
 dept_id ORDER BY start_date, end_date) THEN 0 ELSE 1 END) AS GroupStartFlag
FROM systest.project ) T1
) T2
GROUP BY T2.project_name, T2.dept_id, T2.GroupID
ORDER BY 1,2,3;
```

Salida:

```
 project_name | dept_id | new_start_date | new_end_date
--------------+---------+----------------+--------------
 First Phase  |    1000 | 2010-01-10     | 2010-03-20
 First Phase  |    2000 | 2010-03-10     | 2010-07-20
 Second Phase |    1000 | 2020-05-10     | 2020-09-20
 Second Phase |    2000 | 2010-06-15     | 2010-08-18
(4 rows)
```

Epics

Convierta NORMALIZE en Amazon Redshift SQL

Tarea	Descripción	Habilidades requeridas
Cree código SQL en Teradata.	Use la frase NORMALIZE en función de sus necesidades.	Desarrollador SQL
Convierta el código a Amazon Redshift SQL.	Para convertir el código, siga las instrucciones de la sección «Herramientas» de este patrón.	Desarrollador SQL
Ejecute el código en Amazon Redshift.	Cree la tabla, cargue los datos en la tabla y ejecute el código en Amazon Redshift.	Desarrollador SQL

Recursos relacionados

Referencias

- Característica temporal NORMALIZE de Teradata (documentación de Teradata)
- Función de ventana LAG (documentación de Amazon Redshift)
- Migración a Amazon Redshift (sitio web de AWS)
- Migración de una base de datos de Teradata a Amazon Redshift con los agentes de extracción de datos de AWS SCT (Recomendaciones de AWS)
- Convertir la característica RESET WHEN de Teradata a Amazon Redshift SQL (Recomendaciones de AWS)

Herramientas

- Herramienta de conversión de esquemas de AWS (AWS SCT)

Socios

- Socios con competencias en migración de AWS

Convierta la característica RESET WHEN de Teradata en Amazon Redshift SQL

Origen: almacenamiento de datos de Teradata	Destino: Amazon Redshift	Tipo R: renovar arquitectura
Entorno: producción	Tecnologías: análisis; bases de datos; migración	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon Redshift		

Resumen

RESET WHEN es una característica de Teradata que se utiliza en las funciones de la ventana analítica de SQL. Es una extensión del estándar ANSI SQL. RESET WHEN determina la partición sobre la que opera una función de ventana SQL basada en alguna condición específica. Si la condición se evalúa como TRUE, se crea una nueva subpartición dinámica dentro de la partición de ventana existente. Para obtener más información acerca de RESET WHEN, consulte la documentación de Teradat.

Amazon Redshift no admite RESET WHEN en las funciones de ventana de SQL. Para implementar esta funcionalidad, debe convertir RESET WHEN a la sintaxis SQL nativa de Amazon Redshift y utilizar varias funciones anidadas. Este patrón demuestra cómo puede utilizar lacaracterística RESET WHEN de Teradata y cómo puede convertirla a la sintaxis SQL de Amazon Redshift.

Requisitos previos y limitaciones

Requisitos previos

- Conocimientos básicos del almacén de datos de Teradata y su sintaxis SQL
- Buen conocimiento de Amazon Redshift y su sintaxis SQL

Arquitectura

Pila de tecnología de origen

- Almacenamiento de datos de Teradata

Pila de tecnología de destino

- Amazon Redshift

Arquitectura

Para obtener una arquitectura de alto nivel para migrar una base de datos de Teradata a Amazon Redshift, consulte el patrón Migración de una base de datos de Teradata a Amazon Redshift mediante agentes de extracción de datos SCT de AWS. La migración no convierte automáticamente la frase RESET WHEN de Teradata en Amazon Redshift SQL. Puede convertir esta extensión de Teradata siguiendo las pautas de la siguiente sección.

Herramientas

Código

Para ilustrar el concepto de RESET WHEN, considere la siguiente definición de tabla en Teradata:

```
create table systest.f_account_balance
( account_id integer NOT NULL,
  month_id integer,
  balance integer )
unique primary index (account_id, month_id);
```

Ejecute el siguiente código SQL para insertar datos de ejemplo en la tabla:

```
BEGIN TRANSACTION;
Insert Into systest.f_account_balance values (1,1,60);
Insert Into systest.f_account_balance values (1,2,99);
Insert Into systest.f_account_balance values (1,3,94);
Insert Into systest.f_account_balance values (1,4,90);
Insert Into systest.f_account_balance values (1,5,80);
Insert Into systest.f_account_balance values (1,6,88);
Insert Into systest.f_account_balance values (1,7,90);
Insert Into systest.f_account_balance values (1,8,92);
Insert Into systest.f_account_balance values (1,9,10);
Insert Into systest.f_account_balance values (1,10,60);
Insert Into systest.f_account_balance values (1,11,80);
```

```
Insert Into systest.f_account_balance values (1,12,10);
END TRANSACTION;
```

La tabla de muestra tiene los siguientes datos:

account_id	month_id	balance
1	1	60
1	2	99
1	3	94
1	4	90
1	5	80
1	6	88
1	7	90
1	8	92
1	9	10
1	10	60
1	11	80
1	12	10

Para cada cuenta, digamos que desea analizar la secuencia de aumentos de saldo mensuales consecutivos. Cuando el saldo de un mes es inferior o igual al saldo del mes anterior, es necesario restablecer el contador a cero y reiniciarlo.

Teradata se restablece en caso de uso

Para analizar estos datos, Teradata SQL utiliza una función de ventana con un agregado anidado y una frase RESET WHEN, de la siguiente manera:

```
SELECT account_id, month_id, balance,
```

```
 ( ROW_NUMBER() OVER (PARTITION BY account_id ORDER BY month_id
RESET WHEN balance <= SUM(balance) over (PARTITION BY account_id ORDER BY month_id ROWS
 BETWEEN 1 PRECEDING AND 1 PRECEDING) ) -1 ) as balance_increase
FROM systest.f_account_balance
ORDER BY 1,2;
```

Salida:

account_id	month_id	balance	balance_increase
1	1	60	0
1	2	99	1
1	3	94	0
1	4	90	0
1	5	80	0
1	6	88	1
1	7	90	2.
1	8	92	3
1	9	10	0
1	10	60	1
1	11	80	2.
1	12	10	0

La consulta se procesa de la siguiente manera en Teradata:

1. La función de agregado SUM (saldo) calcula la suma de todos los saldos de una cuenta determinada en un mes determinado.
2. Comprobamos si el saldo de un mes determinado (para una cuenta determinada) es superior al saldo del mes anterior.

3. Si el saldo aumentó, registramos un valor de recuento acumulado. Si la condición RESET WHEN se evalúa como false, lo que significa que el saldo ha aumentado durante meses sucesivos, seguiremos aumentando el recuento.
4. La función analítica ordenada ROW_NUMBER () calcula el valor del recuento. Cuando llegamos a un mes cuyo saldo es inferior o igual al saldo del mes anterior, la condición RESET WHEN se evalúa como verdadera. Si es así, iniciamos una nueva partición y ROW_NUMBER () reinicia el conteo desde 1. Usamos FILAS ENTRE 1 ANTERIOR Y 1 ANTERIOR para acceder al valor de la fila anterior.
5. Restamos 1 para asegurarnos de que el valor del recuento comience por 0.

SQL equivalente a Amazon Redshift

Amazon Redshift no admite la frase RESET WHEN en una función de ventana analítica de SQL. Para obtener el mismo resultado, debe reescribir el SQL de Teradata con la sintaxis SQL nativa de Amazon Redshift y las subconsultas anidadas, de la siguiente manera:

```
SELECT account_id, month_id, balance,
   (ROW_NUMBER() OVER(PARTITION BY account_id, new_dynamic_part ORDER BY month_id) -1)
 as balance_increase
FROM
( SELECT account_id, month_id, balance, prev_balance,
SUM(dynamic_part) OVER (PARTITION BY account_id ORDER BY month_id ROWS BETWEEN
 UNBOUNDED PRECEDING AND CURRENT ROW) As new_dynamic_part
FROM ( SELECT account_id, month_id, balance,
SUM(balance) over (PARTITION BY account_id ORDER BY month_id ROWS BETWEEN 1 PRECEDING
 AND 1 PRECEDING) as prev_balance,
(CASE When balance <= prev_balance Then 1 Else 0 END) as dynamic_part
FROM systest.f_account_balance ) A
) B
ORDER BY 1,2;
```

Como Amazon Redshift no admite funciones de ventana anidadas en la cláusula SELECT de una sola sentencia SQL, debe utilizar dos subconsultas anidadas.

- En la subconsulta interna (alias A), se crea y rellena un indicador de partición dinámica (dynamic_part). dynamic_part se establece en 1 si el saldo de un mes es inferior o igual al saldo del mes anterior; de lo contrario, se establece en 0.
- En la siguiente capa (alias B), se genera un atributo new_dynamic_part como resultado de unacaracterística de ventana SUM.

- Por último, añada new_dynamic_part como un nuevo atributo de partición (partición dinámica) al atributo de partición existente (account_id) y aplique la mismacaracterística de ventana ROW_NUMBER () que en Teradata (y menos una).

Tras estos cambios, Amazon Redshift SQL genera el mismo resultado que Teradata.

Epics

Convierta RESET WHEN en Amazon Redshift SQL

Tarea	Descripción	Habilidades requeridas
Cree su función de ventana de Teradata.	Use agregados anidados y la frase RESET WHEN de acuerdo con sus necesidades.	Desarrollador SQL
Convierta el código a Amazon Redshift SQL.	Para convertir el código, siga las instrucciones de la sección «Herramientas» de este patrón.	Desarrollador SQL
Ejecute el código en Amazon Redshift.	Cree la tabla, cargue los datos en la tabla y ejecute el código en Amazon Redshift.	Desarrollador SQL

Recursos relacionados

Referencias

- Frase RESET WHEN (Documentación Teradata)
- Explicación de RESET WHEN (Stack Overflow)
- Migración a Amazon Redshift (sitio web de AWS)
- Migración de una base de datos de Teradata a Amazon Redshift con los agentes de extracción de datos de AWS SCT (Recomendaciones de AWS)
- Convierta la función temporal NORMALIZE de Teradata en Amazon Redshift SQL (AWS Prescriptive Guidance)

Herramientas

- Herramienta de conversión de esquemas de AWS (AWS SCT)

Socios

- Socios con competencias en migración de AWS

Imponga el etiquetado de los clústeres de Amazon EMR en el lanzamiento

Creado por Priyanka Chaudhary (AWS)

Entorno: producción	Tecnologías: análisis; seguridad, identidad y cumplimiento	Servicios de AWS: Amazon EMR; AWS Lambda; Amazon Events CloudWatch

Resumen

Este patrón proporciona un control de seguridad que garantiza que los clústeres de Amazon EMR se etiqueten cuando son creados.

Amazon EMR es un servicio de Amazon Web Services (AWS) para procesar y analizar grandes cantidades de datos. Amazon EMR ofrece un servicio ampliable de baja configuración como alternativa más simple a la ejecución interna de computación en clústeres. Puede usar el etiquetado para clasificar los recursos de AWS de diversas maneras, por ejemplo, según su finalidad, propietario o entorno. Por ejemplo, puede etiquetar sus clústeres de Amazon EMR asignando metadatos personalizados a cada clúster. Una etiqueta consta de una clave y un valor que define el usuario. Le recomendamos que cree un conjunto de etiquetas coherente para satisfacer los requisitos de su organización. Cuando se agrega una etiqueta a un clúster de Amazon EMR, la etiqueta también se propaga a cada una de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) activas que están asociadas al clúster. Del mismo modo, si elimina una etiqueta de un clúster de Amazon EMR, dicha etiqueta se elimina también de cada una de las instancias de EC2 activas asociadas.

El control de detección supervisa las llamadas a las API e inicia un evento de Amazon CloudWatch Events para las CreateTagsAPI RunJobFlowAddTagsRemoveTags,, y. El evento llama a AWS Lambda, que ejecuta un script de Python. La función de Python obtiene el ID del clúster de Amazon EMR de la entrada JSON del evento y realiza las siguientes comprobaciones:

- Comprobar si el clúster de Amazon EMR está configurado con los nombres de etiquetas que especifique.
- Si no lo está, envía una notificación de Amazon Simple Notification Service (Amazon SNS) al usuario con la información pertinente: el nombre del clúster de Amazon EMR, los detalles de la

infracción, la región de AWS, la cuenta de AWS y el nombre de recurso de Amazon (ARN) de Lambda del que proviene la notificación.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Cargue el código Lambda proporcionado en un bucket de Amazon Simple Storage Service (Amazon S3). O bien, puede crear un bucket de S3 para este fin, tal y como se describe en la sección Epics.
- Especifique una dirección de correo electrónico activa en la que desee recibir notificaciones de infracciones.
- Una lista de etiquetas obligatorias que desea comprobar.

Limitaciones

- Este control de seguridad es regional. Debe implementarlo en cada región de AWS que desee supervisar.

Versiones de producto

- Amazon EMR 4.8.0 y versiones posteriores.

Arquitectura

Arquitectura de flujo de trabajo

Automatizar y escalar

- Si utiliza AWS Organizations, puede utilizar AWS Cloudformation StackSets para implementar esta plantilla en varias cuentas que desee supervisar.

Herramientas

Servicios de AWS

- AWS CloudFormation: AWS le CloudFormation ayuda a modelar y configurar sus recursos de AWS, a aprovisionarlos de forma rápida y coherente y a gestionarlos durante todo su ciclo de vida. Facilita poder usar una plantilla para describir los recursos y sus dependencias, y lanzarlos y configurarlos juntos como una pila, en lugar de administrarlos de forma individual. Puede administrar y aprovisionar pilas en varias cuentas y regiones de AWS.
- Amazon CloudWatch Events: Amazon CloudWatch Events ofrece una transmisión casi en tiempo real de los eventos del sistema que describen los cambios en los recursos de AWS.
- Amazon EMR: Amazon EMR es un servicio web que simplifica la ejecución de marcos de macrodatos y el procesamiento eficiente de grandes cantidades de datos.
- AWS Lambda: AWS Lambda es un servicio informático que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objeto. Puede utilizar Amazon S3 para almacenar y recuperar cualquier cantidad de datos en cualquier momento y desde cualquier parte de la web.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) coordina y gestiona la entrega o el envío de mensajes entre publicadores y clientes, incluyendo los servidores web y las direcciones de correo electrónico. Los suscriptores reciben todos los mensajes publicados de los temas a los que están suscritos y todos los suscriptores de un tema reciben los mismos mensajes.

Código

Este patrón incluye los siguientes archivos adjuntos:

- `EMRTagValidation.zip`: el código Lambda para el control de seguridad.
- `EMRTagValidation.yml`— La CloudFormation plantilla que configura el evento y la función Lambda.

Epics

Configure el bucket de S3

Tarea	Descripción	Habilidades requeridas
Elimine el bucket de S3.	En la consola Amazon S3, elija o cree un bucket de S3 para alojar el archivo .zip de código Lambda. El bucket de S3 debe estar en la misma región de AWS que el clúster de Amazon EMR que desea supervisar. Un nombre de bucket de Amazon S3 es globalmente único y todas las cuentas de AWS comparten el espacio de nombres. El nombre de bucket de S3 no puede incluir barras a la izquierda.	Arquitecto de la nube
Cargue el código Lambda.	Cargue el archivo .zip de código Lambda que se proporciona en la sección Adjuntos en el bucket S3.	Arquitecto de la nube

Implemente la CloudFormation plantilla de AWS

Tarea	Descripción	Habilidades requeridas
Lance la CloudFormation plantilla de AWS.	Abra la CloudFormation consola de AWS en la misma región de AWS que su bucket de S3 e implemente la plantilla . Para obtener más informaci	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	ón sobre la implementación de CloudFormation plantillas de AWS, consulte Crear una pila en la CloudFormation consola de AWS en la CloudFormation documentación.	

Tarea	Descripción	Habilidades requeridas
Complete los parámetros de la plantilla.	Al lanzar la plantilla, se le solicitará la siguiente información: • Bucket de S3: especifique el bucket creado o seleccionado en la primera Epic. Aquí es donde cargó el código Lambda adjunto (archivo.zip). • Clave S3: especifique la ubicación del archivo .zip de Lambda en el bucket S3 (por ejemplo, nombre de archivo.zip o controls/nombre de archivo.zip). No incluya barras a la izquierda. • Correo electrónico de notificación: proporcione una dirección de correo electrónico activa en la que desea recibir las notificaciones de Amazon SNS. • Etiquetado de nombres clave: indique las etiquetas que desee comprobar en una lista separada por comas (por ejemplo, `ApplicationID`, `Environment`, `Owner`). El evento CloudWatch Events monitorea el clúster en busca de estas etiquetas y	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	envía una notificación si no las encuentra. • Nivel de registro Lambda: especifique el nivel y la frecuencia de registro de la función de Lambda. Utilice Info para registrar mensajes informativos detallados sobre el progreso, Error para los eventos de error que pudieran continuar con la implementación y Advertencia en caso de situaciones potencialmente dañinas.	

Confirmar la suscripción

Tarea	Descripción	Habilidades requeridas
Confirmar la suscripción.	Cuando la CloudFormation plantilla se implementa correctamente, envía un correo electrónico de suscripción a la dirección de correo electrónico que has proporcionado. Debe confirmar esta suscripción de correo electrónico para recibir las notificaciones de infracciones.	Arquitecto de la nube

Recursos relacionados

- Guía para desarrolladores de AWS Lambda
- Etiquetado de clústeres de Amazon EMR

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Asegúrese de que el registro de Amazon EMR en Amazon S3 esté habilitado en el lanzamiento

Entorno: producción	Tecnologías: seguridad, identidad, conformidad; sin servidor; análisis	Carga de trabajo: código abierto
Servicios de AWS: Amazon EMR; Amazon S3; Amazon SNS; Amazon CloudWatch		

Resumen

Este patrón proporciona un control de seguridad que supervisa la configuración de registro de los clústeres de Amazon EMR ejecutados en Amazon Web Services (AWS).

Amazon EMR es una herramienta de AWS para el procesamiento y el análisis de macrodatos. Amazon EMR ofrece un servicio ampliable de baja configuración como alternativa a la ejecución interna de computación en clústeres. Amazon EMR ofrece dos tipos de clústeres de EMR.

- Clústeres transitorios de Amazon EMR: los clústeres transitorios de Amazon EMR se desactivan automáticamente y dejan de incurrir en costos cuando finaliza el procesamiento.
- Clústeres persistentes de Amazon EMR: los clústeres persistentes de Amazon EMR siguen ejecutándose una vez finalizado el trabajo de procesamiento de datos.

Amazon EMR y Hadoop producen archivos de registro que notifican el estado en el clúster. De forma predeterminada, están escritos en el nodo maestro en el directorio /mnt/var/log/. En función de cómo configure el clúster en el momento de su lanzamiento, también podrá guardar estos registros en Amazon Simple Storage Service (Amazon S3) y consultarlos a través de la herramienta de depuración gráfica. Tenga en cuenta que el registro de Amazon S3 solo se puede especificar cuando se lanza el clúster. Con esta configuración, los registros se envían desde el nodo principal a la ubicación de Amazon S3 cada 5 minutos. En el caso de los clústeres transitorios, el registro en Amazon S3 es muy importante, ya que los clústeres desaparecen cuando se completa el procesamiento y estos archivos de registro pueden usarse para depurar cualquier trabajo fallido.

El patrón utiliza una CloudFormation plantilla de AWS para implementar un control de seguridad que monitorea las llamadas a las API e inicia Amazon CloudWatch Events en «RunJobFlow». El desencadenador invoca AWS Lambda, que ejecuta un script de Python. La función de Lambda recupera la ID del clúster de EMR de la entrada JSON del evento, y también comprueba si hay un URI de registro de Amazon S3. Si no se encuentra un URI de Amazon S3, la función de Lambda envía una notificación de Amazon Simple Notification Service (Amazon SNS) en la que se detalla el nombre del clúster de EMR, los detalles de la infracción, la región de AWS, la cuenta de AWS y el nombre de recurso de Amazon (ARN) de Lambda del que proviene la notificación.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un bucket de S3 para el archivo .zip de código de Lambda
- La dirección de correo electrónico en la que desee recibir la notificación de infracción

Limitaciones

- Este control de detección es regional, por lo que debe implementarse en las regiones de AWS que desee supervisar.

Versiones de producto

- Amazon EMR 4.8.0 y versiones posteriores

Arquitectura

Pila de tecnología de destino

- Evento Amazon CloudWatch Events
- Amazon EMR
- Función de Lambda
- Bucket de S3
- Amazon SNS

Arquitectura de destino

Automatizar y escalar

- Si utiliza AWS Organizations, puede utilizar AWS CloudFormation StackSets para implementar esta plantilla en varias cuentas que desee supervisar.

Herramientas

Herramientas

- AWS CloudFormation: AWS le CloudFormation ayuda a modelar y configurar los recursos de AWS utilizando la infraestructura como código.
- AWS Cloudwatch Events: AWS CloudWatch Events ofrece una transmisión casi en tiempo real de los eventos del sistema que describen los cambios en los recursos de AWS.
- Amazon EMR: Amazon EMR es una plataforma de clúster administrada que simplifica la ejecución de marcos de trabajo de macrodatos.
- AWS Lambda: AWS Lambda permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo.
- Amazon S3: Amazon S3 es una interfaz de servicios web que puede utilizar para almacenar y recuperar cualquier cantidad de datos desde cualquier lugar de la web.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) coordina y gestiona la entrega o el envío de mensajes entre publicadores y clientes, incluyendo los servidores web y las direcciones de correo electrónico.

Código

- El archivo .zip del proyecto está disponible como adjunto.

Epics

Cómo definir el bucket de S3

Tarea	Descripción	Habilidades requeridas
Defina el bucket de S3.	Para alojar el archivo .zip de código de Lambda, seleccione o cree un bucket de S3 con un nombre único que no contenga barras diagonales al inicio. Un nombre de bucket de S3 es globalmente único y todas las cuentas de AWS comparten el espacio de nombres. Su bucket de S3 debe estar en la misma región de AWS que el clúster de Amazon EMR que se evalúa.	Arquitecto de la nube

Cómo cargar el código de Lambda en el bucket de S3

Tarea	Descripción	Habilidades requeridas
Cargue el código de Lambda en el bucket de S3.	Cargue el archivo .zip de código de Lambda que se proporciona en la sección “Adjuntos” del bucket de S3. El bucket de S3 debe encontrarse en la misma región que el clúster de Amazon EMR que se está evaluando.	Arquitecto de la nube

Implemente la CloudFormation plantilla de AWS

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation plantilla de AWS.	En la CloudFormation consola de AWS, en la misma región que su bucket de S3, implemente la CloudForm ation plantilla de AWS que se proporciona como adjunto a este patrón. En la siguiente épica, proporcione los valores de los parámetros. Para obtener más información sobre la implementación de CloudFormation plantillas de AWS, consulte la sección «Recursos relacionados».	Arquitecto de la nube

Complete los parámetros de la CloudFormation plantilla de AWS

Tarea	Descripción	Habilidades requeridas
Ponga nombre al bucket de S3.	Escriba el nombre del bucket de S3 que ha creado en la primera épica.	Arquitecto de la nube
Proporcione la clave de Amazon S3.	Proporcione la ubicación del archivo .zip del código de Lambda en su bucket de S3, sin barras diagonales iniciales (por ejemplo, <directory>/<file-name>.zip).	Arquitecto de la nube
Proporcione una dirección de correo electrónico.	Proporcione una dirección de correo electrónico activa en la	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	que desea recibir las notificac iones de Amazon SNS.	
Defina el nivel de registro.	Defina el nivel y la frecuenci a de registro de la función de Lambda. «Info» designa mensajes informativos detallados sobre el progreso de la aplicación. «Error» designa eventos de error que permiten que la aplicación siga ejecutándose. «Warning» designa situaciones potencial mente peligrosas.	Arquitecto de la nube

Confirmar la suscripción

Tarea	Descripción	Habilidades requeridas
Confirmar la suscripción.	Cuando la plantilla se implementa correctamente, se envía un mensaje de correo electrónico de suscripción a la dirección de correo electróni co proporcionada. Debe confirmar esta suscripción de correo electrónico para recibir las notificaciones de infraccio nes.	Arquitecto de la nube

Recursos relacionados

AWS Lambda

Registro de Amazon EMR

Implementación de CloudFormation plantillas de AWS

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Genere datos de prueba con un trabajo de AWS Glue y Python

Entorno: producción	Tecnologías: análisis; nativa en la nube; lagos de datos; desarrollo y pruebas de software; sin servidor; macrodatos	Servicios de AWS: AWS Glue; Amazon S3

Resumen

Este patrón le muestra cómo generar de forma rápida y sencilla millones de archivos de muestra de forma simultánea mediante la creación de un trabajo de AWS Glue escrito en Python. El archivo de ejemplo se almacena en un bucket de Amazon Simple Storage Service (Amazon S3). La capacidad de generar rápidamente una gran cantidad de archivos de muestra es importante para probar o evaluar los servicios en la nube de AWS. Por ejemplo, puede probar el rendimiento de los DataBrew trabajos de AWS Glue Studio o AWS Glue realizando análisis de datos en millones de archivos pequeños en un prefijo de Amazon S3.

Aunque puede utilizar otros servicios de AWS para generar conjuntos de datos de ejemplo, le recomendamos que utilice AWS Glue. No necesita administrar ninguna infraestructura porque AWS Glue es un servicio de procesamiento de datos sin servidor. Solo tiene que traer su código y ejecutarlo en un clúster de AWS Glue. Además, AWS Glue aprovisiona, configura y escala los recursos necesarios para ejecutar sus trabajos. Solo paga por los recursos que utilizan los trabajos mientras se ejecutan.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada para funcionar con la cuenta AWS.

Versiones de producto

- Python 3.9

- CLI de AWS versión 2

Limitaciones

El número máximo de trabajos de AWS Glue por activador es 50. Para obtener más información, consulte Puntos de conexión y cuotas de AWS Glue.

Arquitectura

El siguiente diagrama muestra un ejemplo de arquitectura centrado en un trabajo de AWS Glue que escribe su salida (es decir, archivos de muestra) en un bucket de S3.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Utilice la AWS CLI, la Consola de administración de AWS o una API para iniciar el trabajo de AWS Glue. La API o la CLI de AWS le permiten automatizar la paralelización del trabajo invocado y reducir el tiempo de ejecución necesario para generar archivos de muestra.
2. El trabajo de AWS Glue genera el contenido del archivo de forma aleatoria, lo convierte en formato CSV y, a continuación, lo almacena como un objeto de Amazon S3 con un prefijo común. Cada archivo ocupa menos de un kilobyte. El trabajo de AWS Glue acepta dos parámetros de trabajo definidos por el usuario: `START_RANGE` y `END_RANGE`. Puede utilizar estos parámetros para establecer los nombres de los archivos y el número de archivos generados en Amazon S3 por cada ejecución de trabajo. Puede ejecutar varias instancias de este trabajo en paralelo (por ejemplo, 100 instancias).

Herramientas

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.
- AWS Glue es un servicio de extracción, transformación y carga (ETL) completamente administrado. Ayuda a clasificar, limpiar, enriquecer y mover datos de forma fiable entre almacenes de datos y flujos de datos.

- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.

Prácticas recomendadas

Tenga en cuenta las siguientes prácticas recomendadas de AWS Glue al implementar este patrón:

- Utilice el tipo de trabajador de AWS Glue adecuado para reducir los costos. Recomendamos que comprenda las diferentes propiedades de los tipos de trabajadores y, a continuación, elija el tipo de trabajador adecuado para su carga de trabajo en función de los requisitos de CPU y memoria. Para este patrón, recomendamos que utilice un trabajo de intérprete de comandos de Python como tipo de trabajo para minimizar la DPU y reducir los costos. Para obtener más información, consulte Cómo agregar trabajos en AWS Glue en la Guía del desarrollador de AWS Glue.
- Use el límite de simultaneidad correcto para escalar su trabajo. Le recomendamos que base la simultaneidad máxima de su trabajo de AWS Glue en sus requisitos de tiempo y en la cantidad de archivos requerida.
- Comience a generar una cantidad pequeña de archivos al principio. Para reducir los costos y ahorrar tiempo a la hora de crear sus trabajos de AWS Glue, comience con un número reducido de archivos (por ejemplo, 1000). Esto puede facilitar la solución de problemas. Si la generación de un número reducido de archivos se realiza correctamente, puede escalar a un número mayor de archivos.
- Ejecute primero de forma local. Para reducir los costos y ahorrar tiempo a la hora de crear sus trabajos de AWS Glue, inicie el desarrollo de forma local y pruebe el código. Para obtener instrucciones sobre cómo configurar un contenedor de Docker que pueda ayudarlo en la escritura de trabajos de AWS Glue de extracción, transformación y carga (ETL), tanto en un intérprete de comandos como en un entorno de desarrollo integrado (IDE), consulte la entrada Desarrollo y prueba de trabajos de ETL de AWS Glue de forma local mediante un contenedor en la el blog de AWS Big Data.

Para obtener más información sobre las prácticas recomendadas de AWS Glue, consulte las Prácticas recomendadas en la documentación de AWS Glue.

Epics

Creación del bucket de Amazon S3 de destino y un rol de IAM

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3; para almacenar los archivos.	Cree un bucket de S3 y un prefijo dentro de él. Nota: Este patrón utiliza la ubicación `s3://{your-s3-bucket-name}/small-files/` con fines de demostración.	Desarrollador de aplicaciones
Creación y configuración de un rol de IAM	Debe crear un rol de IAM que su trabajo de AWS Glue pueda usar para escribir en su bucket de S3. 1. Cree un rol de IAM (por ejemplo, llamado `"AWSGlueServiceRole-smallfiles"`). 2. Elija AWS Glue como entidad de confianza de la política. 3. Asocie la política administrada de AWS llamada `"AWSGlueServiceRole"` a este rol. 4. Cree una política en línea o una Política administrada por el cliente, denominada `"s3-small-file-access"` en base a la siguiente configuración.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	Reemplace `"{bucket}"` con el nombre del bucket. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "s3:GetObject", "s3:PutObject" ], "Resource": [ "arn:aws:s3:::{bucket}/small-files/input/*" ] } ] }` 5. Asocie la política `"s3-small-file-access"` al rol.	

Cree y configure un trabajo de AWS Glue para gestionar ejecuciones simultáneas

Tarea	Descripción	Habilidades requeridas
Crear un trabajo de AWS Glue.	Debe crear un trabajo de AWS Glue que genere su contenido	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	y lo almacene en un bucket de S3. Cree un trabajo de AWS Glue y, a continuación, configure su trabajo siguiendo estos pasos: 1. Inicie sesión en la consola de administración de AWS y abra la consola de AWS Glue. 2. En el panel de navegación, en Integración de datos y ETL, elija Trabajos. 3. En la sección Create job (Crear trabajo), seleccione el Python Shell script editor (editor de intérprete de comandos de Python). 4. En la sección Options (Opciones), seleccione Create a new script with boilerplate code (Crear un nuevo script con código reutilizable) y, a continuación, seleccione Create (Crear). 5. Elija Job details (Detalles del trabajo). 6. En Nombre, introduzca create_small_files. 7. Para IAM role (Rol de IAM), seleccione el rol de IAM que creó previamente.	

Tarea	Descripción	Habilidades requeridas
	8. En la sección This job runs (Este trabajo ejecuta), elija A new script to be authored by you (Un script nuevo para que lo cree usted). 9. Elija Advanced properties (Propiedades avanzadas). 10. En Máxima simultaneidad, introduzca 100 con fines de demostración. Nota: La simultaneidad máxima define el número de instancias del trabajo que se pueden ejecutar en paralelo. 11. Seleccione Guardar.	

Tarea	Descripción	Habilidades requeridas
Actualizar el código del trabajo.	1. Abra la consola de AWS Glue. 2. En el panel de navegación, seleccione Trabajos. 3. En la sección Your jobs (Sus trabajos), elija el trabajo que creó anteriormente. 4. Seleccione la pestaña Script y, a continuación, actualice la secuencia de comandos en función del siguiente código. Actualice las variables `BUCKET_NAME` , `PREFIX` y `text_str` con sus valores. `from awsglue.utils import getResolvedOptions` `import sys` `import boto3` `from random import randrange` `# Two arguments` `args = getResolvedOptions(sys.argv, ['START_RANGE', 'END_RANGE'])` `START_RANGE = int(args['START_RANGE'])` `END_RANGE = int(args['END_RANGE'])`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`` BUCKET_NAME = '{BUCKET_NAME}' PREFIX = 'small-fi les/input/' s3 = boto3.res ource('s3') for x in range(STA RT_RANGE, END_RANGE): # generate file name file_name = f"input_{x}.txt" # generate text text_str = str(randrange(1000 00))+","+str(randr ange(100000))+", " + str(randrange(1000 0000)) + "," + str(randrange(1000 0)) # write in s3 s3.Object(BUCKE T_NAME, PREFIX + file_name).put(Bod y=text_str) ``` 5. Seleccione Guardar.	

Ejecute el trabajo de AWS Glue desde la línea de comandos o la consola

Tarea	Descripción	Habilidades requeridas
Ejecute el trabajo de AWS Glue desde la línea de comandos.	Para ejecutar su trabajo de AWS Glue desde la CLI de AWS, ejecute el siguiente comando con sus valores:	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`cmd:~$ aws glue start-job-run --job-name create_small_files --arguments '{"--START_RANGE":"0","--END_RANGE":"1000000"}'` `cmd:~$ aws glue start-job-run --job-name create_small_files --arguments '{"--START_RANGE":"1000000","--END_RANGE":"2000000"}'` Nota: Para obtener instrucciones sobre cómo ejecutar el trabajo de AWS Glue desde la consola de administración de AWS, consulte el artículo Ejecute el trabajo de AWS Glue en la consola de administración de AWS que sigue este patrón. Consejo: recomendamos que utilice la CLI de AWS para ejecutar trabajos de AWS Glue si quiere ejecutar varias ejecuciones a la vez con distintos parámetros, como se muestra en el ejemplo anterior. Para generar todos los comandos de la CLI de AWS necesarios para generar un número definido de archivos	

Tarea	Descripción	Habilidades requeridas
	con un factor de paraleliz ación determinado, ejecute el siguiente código bash (con sus valores): `# define parameters` `NUMBER_OF_FILES=` `10000000;` `PARALLELIZATION=50;` `# initialize` `_SB=0;` `# generate commands` `for i in $(seq 1` ` $PARALLELIZATION);` `do` `  echo aws glue` ` start-job-run --` `job-name create_sm` `all_files --argumen` `ts "'"'{"--START_RANG` `E":"'$(((NUMBER_OF` `_FILES/PARALLELIZA` `TION) * (i-1) +` ` _SB))'","--END_RAN` `GE":"'$(((NUMBER_O` `F_FILES/PARALLELIZ` `ATION) * (i)))'"}'"'";` `  _SB=1;` `done` Si utiliza el script anterior, tenga en cuenta lo siguiente: • El script simplifica la invocación y la generació n de archivos pequeños a escala.	

Tarea	Descripción	Habilidades requeridas
	• Actualice `NUMBER_OF_FILES` y `PARALLELIZATION` con sus valores. • El script anterior imprime una lista de comandos que debe ejecutar. Copie esos comandos de salida y ejecútelos en su terminal. • Si desea ejecutar los comandos directamente desde el script, elimine la instrucción `echo` de la línea 11. Nota: Para ver un ejemplo del resultado del script anterior, consulte el Resultado del script de intérprete de comandos en la sección de Información adicional de este patrón.	

Tarea	Descripción	Habilidades requeridas
Ejecute el trabajo de AWS Glue en la consola de administración de AWS.	1. Inicie sesión en la consola de administración de AWS y abra la consola de AWS Glue. 2. En el panel de navegación, en Integración de datos y ETL, elija Trabajos. 3. En la sección Your jobs (Sus trabajos), elija su trabajo. 4. En la sección Parameters (optional) (Parámetros (opcional)), actualice sus parámetros. 5. Elija Action (Acción) y, a continuación, seleccione Run job (Ejecutar trabajo). 6. Repita los pasos 3 a 5 tantas veces como sea necesario. Por ejemplo, para crear 10 millones de archivos, repita este proceso 10 veces.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Verifique el estado de su trabajo de AWS Glue.	1. Abra la consola de AWS Glue. 2. En el panel de navegación, seleccione Trabajos. 3. En la sección Your jobs (Sus trabajos), elija el trabajo que creó anteriorm ente (el `create_sm all_files`). 4. Para obtener informaci ón sobre el progreso y la generación de sus archivos, revise las columnas ID de ejecución, Estado de ejecución y otras columnas.	Desarrollador de aplicaciones

Recursos relacionados

Referencias

- Registro de datos abiertos en AWS
- Conjuntos de datos para análisis
- Datos abiertos en AWS
- Cómo añadir trabajos en AWS Glue
- Introducción a AWS Glue

Guías y patrones

- Prácticas recomendadas de AWS Glue
- Aplicaciones de pruebas de carga

Información adicional

Prueba de evaluación comparativa

Este patrón se utilizó para generar 10 millones de archivos utilizando diferentes parámetros de paralelización como parte de una prueba de evaluación comparativa. El resultado de la prueba mostrará lo siguiente:

Paralelización	Número de archivos generados por la ejecución de una tarea	Duración del trabajo	Speed (Velocidad)
10	1 000 000	6 horas, 40 minutos	Muy lento
50	200.000	80 minutos	Moderado
100	100 000	40 minutos	Rápido

Si desea acelerar el proceso, puede configurar más ejecuciones simultáneas en la configuración de su trabajo. Puede ajustar fácilmente la configuración del trabajo en función de sus requisitos, pero tenga en cuenta que existe un límite de cuota de servicio de AWS Glue. Para obtener más información, consulte Puntos de conexión y cuotas de AWS Glue.

Resultado del script de intérprete de comandos

En el siguiente ejemplo, se muestra el resultado del script de intérprete de comandos de la historia Ejecute the AWS Glue desde la línea de comandos siguiendo este patrón.

```
user@MUC-1234567890 MINGW64 ~
  $ # define parameters
  NUMBER_OF_FILES=10000000;
  PARALLELIZATION=50;
  # initialize
  _SB=0;

  # generate commands
  for i in $(seq 1 $PARALLELIZATION);
   do
```

```
        echo aws glue start-job-run --job-name create_small_files --arguments
 "'"'{"--START_RANGE":"'$(((NUMBER_OF_FILES/PARALLELIZATION)  (i-1) + SB))'","--
ENDRANGE":"'$(((NUMBER_OF_FILES/PARALLELIZATION)  (i)))'"}'"'";
        _SB=1;
   done

  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"0","--END_RANGE":"200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"200001","--END_RANGE":"400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"400001","--END_RANGE":"600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"600001","--END_RANGE":"800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"800001","--END_RANGE":"1000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"1000001","--END_RANGE":"1200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"1200001","--END_RANGE":"1400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"1400001","--END_RANGE":"1600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"1600001","--END_RANGE":"1800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"1800001","--END_RANGE":"2000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"2000001","--END_RANGE":"2200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"2200001","--END_RANGE":"2400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"2400001","--END_RANGE":"2600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"2600001","--END_RANGE":"2800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"2800001","--END_RANGE":"3000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"3000001","--END_RANGE":"3200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"3200001","--END_RANGE":"3400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"3400001","--END_RANGE":"3600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"3600001","--END_RANGE":"3800000"}'
```

```
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"3800001","--END_RANGE":"4000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"4000001","--END_RANGE":"4200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"4200001","--END_RANGE":"4400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"4400001","--END_RANGE":"4600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"4600001","--END_RANGE":"4800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"4800001","--END_RANGE":"5000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"5000001","--END_RANGE":"5200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"5200001","--END_RANGE":"5400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"5400001","--END_RANGE":"5600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"5600001","--END_RANGE":"5800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"5800001","--END_RANGE":"6000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"6000001","--END_RANGE":"6200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"6200001","--END_RANGE":"6400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"6400001","--END_RANGE":"6600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"6600001","--END_RANGE":"6800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"6800001","--END_RANGE":"7000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"7000001","--END_RANGE":"7200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"7200001","--END_RANGE":"7400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"7400001","--END_RANGE":"7600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"7600001","--END_RANGE":"7800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"7800001","--END_RANGE":"8000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"8000001","--END_RANGE":"8200000"}'
```

```
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"8200001","--END_RANGE":"8400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"8400001","--END_RANGE":"8600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"8600001","--END_RANGE":"8800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"8800001","--END_RANGE":"9000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"9000001","--END_RANGE":"9200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"9200001","--END_RANGE":"9400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"9400001","--END_RANGE":"9600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"9600001","--END_RANGE":"9800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"9800001","--END_RANGE":"10000000"}'

  user@MUC-1234567890 MINGW64 ~
```

PREGUNTAS FRECUENTES

¿Cuántas ejecuciones simultáneas o trabajos paralelos debo usar?

El número de ejecuciones simultáneas y trabajos paralelos depende del tiempo requerido y del número deseado de archivos de prueba. Le recomendamos que compruebe el tamaño de los archivos que va a crear. En primer lugar, compruebe cuánto tiempo tarda un trabajo de AWS Glue en generar la cantidad de archivos deseada. A continuación, utilice el número correcto de ejecuciones simultáneas para cumplir sus objetivos. Por ejemplo, si supone que 100 000 archivos tardan 40 minutos en completar la ejecución, pero el tiempo objetivo es de 30 minutos, debe aumentar la configuración de simultaneidad para su trabajo de AWS Glue.

¿Qué tipo de contenido puedo crear con este patrón?

Puede crear cualquier tipo de contenido, como archivos de texto con distintos delimitadores (por ejemplo, PIPE, JSON o CSV). Este patrón usa Boto3 para escribir en un archivo y, a continuación, guarda el archivo en un bucket de S3.

¿Qué nivel de permiso de IAM necesito en el bucket de S3?

Debe tener una política basada en identidad que le permita a `Write` acceso a objetos de su bucket de S3. Para obtener más información, consulte Amazon S3: permite el acceso de lectura y escritura a objetos de un bucket de S3 en la documentación de Amazon S3.

Lanzar un trabajo de Spark en un clúster EMR transitorio mediante una función de Lambda

Creado por Dhrubajyoti Mukherjee (AWS)

Entorno: producción	Tecnologías: análisis	Carga de trabajo: código abierto
Servicios de AWS: Amazon EMR; AWS Identity and Access Management; AWS Lambda; Amazon VPC		

Resumen

Este patrón utiliza la acción de la RunJobFlow API Amazon EMR para lanzar un clúster transitorio para ejecutar un trabajo de Spark desde una función Lambda. Un clúster EMR transitorio está diseñado para finalizar tan pronto como se complete el trabajo o si se produce algún error. Un clúster transitorio permite ahorrar costos porque solo se ejecuta durante el tiempo de cálculo y proporciona escalabilidad y flexibilidad en un entorno de nube.

El clúster EMR transitorio se lanza mediante la API Boto3 y el lenguaje de programación Python en una función de Lambda. La función de Lambda, escrita en Python, proporciona la flexibilidad adicional de iniciar el clúster cuando es necesario.

Para demostrar un ejemplo de cálculo y salida por lotes, este patrón lanzará un trabajo de Spark en un clúster de EMR desde una función de Lambda y ejecutará un cálculo por lotes con los datos de ventas de ejemplo de una empresa ficticia. El resultado del trabajo de Spark será un archivo de valores separados por comas (CSV) en Amazon Simple Storage Service (Amazon S3). El archivo de datos de entrada, el archivo.jar de Spark, un fragmento de código y una CloudFormation plantilla de AWS para una nube privada virtual (VPC) y las funciones de AWS Identity and Access Management (IAM) para ejecutar el cálculo se proporcionan como datos adjuntos.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa

Limitaciones

- Solo se puede iniciar un trabajo de Spark a partir del código a la vez.

Versiones de producto

- Probado en Amazon EMR 6.0.0

Arquitectura

Pila de tecnología de destino

- Amazon EMR
- AWS Lambda
- Amazon S3
- Apache Spark

Arquitectura de destino

Automatizar y escalar

Para automatizar el cálculo por lotes de Spark-EMR, puede utilizar cualquiera de las siguientes opciones.

- Implemente una EventBridge regla de Amazon que pueda iniciar la función Lambda en una programación cron. Para obtener más información, consulte el tutorial: Programe funciones de AWS Lambda mediante. EventBridge
- Configure las notificaciones de eventos de Amazon S3 para iniciar la función de Lambda al llegar el archivo.
- Transfiera los parámetros de entrada a la función de AWS Lambda a través del cuerpo del evento y de las variables de entorno de Lambda.

Herramientas

Servicios de AWS

- Amazon EMR es una plataforma de clúster administrada que simplifica la ejecución de marcos de macrodatos en AWS para procesar y analizar grandes cantidades de datos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Otras herramientas

- Apache Spark es un motor de análisis en varios idiomas para el procesamiento de datos a gran escala.

Epics

Cree las funciones de IAM de Amazon EMR y Lambda y la VPC

Tarea	Descripción	Habilidades requeridas
Crear las funciones de IAM y la VPC.	Si ya tiene las funciones de IAM de AWS Lambda y Amazon EMR y una VPC, puede omitir este paso. Para ejecutar el código, tanto el clúster de EMR como la función de Lambda requieren funciones de IAM. El clúster de EMR también requiere una VPC con una subred pública o una subred privada con una gateway NAT. Para	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	crear automáticamente todas las funciones de IAM y una VPC, implemente la plantilla de CloudFormation AWS adjunta tal cual o puede crear las funciones y la VPC manualmente, tal como se especifica en la sección Información adicional.	
Anote las claves de salida CloudFormation de la plantilla de AWS.	Una vez que la CloudForm ation plantilla se haya implementado correctamente, vaya a la pestaña Outputs de la CloudFormation consola de AWS. Tenga en cuenta las cinco claves de salida: • `S3Bucket` • `LambdaExecutionRole` • `ServiceRole` • `JobFlowRole` • `Ec2SubnetId` Utilizará los valores de estas claves cuando cree la función de Lambda.	Arquitecto de la nube

Cargue el archivo .jar de Spark

Tarea	Descripción	Habilidades requeridas
Subir el archivo.jar de Spark.	Cargue el archivo.jar de Spark en el depósito de S3 que creó	AWS general

Tarea	Descripción	Habilidades requeridas
	la CloudFormation pila de AWS. El nombre del bucket es el mismo que el de la clave de salida`S3Bucket`.	

Crear la función de Lambda para lanzar el clúster de EMR

Tarea	Descripción	Habilidades requeridas
Creación de una función de Lambda.	En la consola Lambda, cree una función de Lambda de Python 3.9+ con un rol de ejecución. La política de funciones de ejecución debe permitir a Lambda lanzar un clúster de EMR. (Consulte la CloudFormation plantilla de AWS adjunta).	Ingeniero de datos, ingeniero de nube
Copie y pegue el código.	Sustituya el código del archivo `lambda_function.py` por el código de la sección de Información adicional de este patrón.	Ingeniero de datos, ingeniero de nube
Cambie los parámetros del código.	Siga los comentarios del código para cambiar los valores de los parámetro s para que se ajusten a su cuenta de AWS.	Ingeniero de datos, ingeniero de nube
Inicie la función para iniciar el clúster.	Inicie la función para iniciar la creación de un clúster EMR transitorio con el archivo .jar de Spark proporcionado.	Ingeniero de datos, ingeniero de nube

Tarea	Descripción	Habilidades requeridas
	Ejecutará el trabajo de Spark y finalizará automáticamente cuando se complete el trabajo.	
Compruebe el estado del clúster de EMR.	Una vez iniciado el clúster de EMR, aparece en la consola de Amazon EMR, en la pestaña Clústeres. Se puede comprobar en consecuencia cualquier error que se produzca al lanzar el clúster o al ejecutar el trabajo.	Ingeniero de datos, ingeniero de nube

Crear y ejecutar la ejemplo de ejemplo

Tarea	Descripción	Habilidades requeridas
Subir el archivo.jar de Spark.	Descargar el archivo.jar de Spark de la sección de Adjuntos y cárgalo en el bucket de S3.	Ingeniero de datos, ingeniero de nube
Cargue el conjunto de datos de entrada.	Cargue el archivo `fake_sales_data.csv` en el bucket de S3.	Ingeniero de datos, ingeniero de nube
Pegue el código Lambda y cambie los parámetros.	Copie el código de la sección Herramientas y péguelo en una función de Lambda, sustituyendo el archivo de código `lambda_function.py`. Cambiar los valores de los parámetros para que se ajusten a su cuenta.	Ingeniero de datos, ingeniero de nube

Tarea	Descripción	Habilidades requeridas
Iniciar la función y verificar la salida.	Una vez que la función de Lambda inicia el clúster con el trabajo de Spark proporcionado, genera un archivo.csv en el bucket de S3.	Ingeniero de datos, ingeniero de nube

Recursos relacionados

- Construyendo Spark
- Apache Spark y Amazon EMR
- Documentación sobre run_job_flow de Boto3 Docs
- Información y documentación de Apache Spark

Información adicional

Código

```
"""
Copy paste the following code in your Lambda function. Make sure to change the
 following key parameters for the API as per your account

-Name (Name of Spark cluster)
-LogUri (S3 bucket to store EMR logs)
-Ec2SubnetId (The subnet to launch the cluster into)
-JobFlowRole (Service role for EC2)
-ServiceRole (Service role for Amazon EMR)

The following parameters are additional parameters for the Spark job itself. Change the
 bucket name and prefix for the Spark job (located at the bottom).

-s3://your-bucket-name/prefix/lambda-emr/SparkProfitCalc.jar (Spark jar file)
-s3://your-bucket-name/prefix/fake_sales_data.csv (Input data file in S3)
-s3://your-bucket-name/prefix/outputs/report_1/ (Output location in S3)
"""
import boto3
```

```
client = boto3.client('emr')


def lambda_handler(event, context):
    response = client.run_job_flow(
        Name='spark_job_cluster',
        LogUri='s3://your-bucket-name/prefix/logs',
        ReleaseLabel='emr-6.0.0',
        Instances={
            'MasterInstanceType': 'm5.xlarge',
            'SlaveInstanceType': 'm5.large',
            'InstanceCount': 1,
            'KeepJobFlowAliveWhenNoSteps': False,
            'TerminationProtected': False,
            'Ec2SubnetId': 'subnet-XXXXXXXXXXXXXX'
        },
        Applications=[{'Name': 'Spark'}],
        Configurations=[
            {'Classification': 'spark-hive-site',
             'Properties': {
                 'hive.metastore.client.factory.class':
 'com.amazonaws.glue.catalog.metastore.AWSGlueDataCatalogHiveClientFactory'}
             }
        ],
        VisibleToAllUsers=True,
        JobFlowRole='EMRLambda-EMREC2InstanceProfile-XXXXXXXXX',
        ServiceRole='EMRLambda-EMRRole-XXXXXXXXX',
        Steps=[
            {
                'Name': 'flow-log-analysis',
                'ActionOnFailure': 'TERMINATE_CLUSTER',
                'HadoopJarStep': {
                    'Jar': 'command-runner.jar',
                    'Args': [
                        'spark-submit',
                        '--deploy-mode', 'cluster',
                        '--executor-memory', '6G',
                        '--num-executors', '1',
                        '--executor-cores', '2',
                        '--class', 'com.aws.emr.ProfitCalc',
                        's3://your-bucket-name/prefix/lambda-emr/SparkProfitCalc.jar',
                        's3://your-bucket-name/prefix/fake_sales_data.csv',
                        's3://your-bucket-name/prefix/outputs/report_1/'
                    ]
```

```
                }
            }
        ]
    )
```

Funciones de IAM y creación de VPC

Para lanzar el clúster de EMR en una función de Lambda, se necesitan funciones de VPC e IAM. Puede configurar las funciones de VPC e IAM mediante la CloudFormation plantilla de AWS de la sección de adjuntos de este patrón, o puede crearlas manualmente mediante los siguientes enlaces.

Las siguientes funciones de IAM son necesarias para ejecutar Lambda y Amazon EMR.

Rol de ejecución de Lambda

El rol de ejecución de una función de AWS Lambda concede permiso a la función para que tenga acceso a los servicios y recursos de AWS.

Roles de servicio para Amazon EMR

El rol de Amazon EMR define las acciones permitidas para Amazon EMR al aprovisionar recursos y realizar tareas de nivel de servicio que no se realizan en el contexto de una instancia de Amazon Elastic Compute Cloud (Amazon EC2) que se ejecuta dentro de un clúster. Por ejemplo, el rol de servicio se utiliza para aprovisionar instancias EC2 cuando se lanza un clúster.

Rol de servicio para una instancia de EC2

El rol de servicio para instancias de EC2 de clúster (también conocido como el perfil de instancia de EC2 para Amazon EMR) es un tipo especial de rol de servicio que está asignado a cada instancia de EC2 de un clúster de Amazon EMR cuando se lanza la instancia. Los procesos de aplicación que se ejecutan sobre el ecosistema de Apache asumen este rol para los permisos, e interactuar así con otros servicios de AWS.

Creación de VPC y subredes

Puede crear una VPC desde la consola de VPC.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Migre las cargas de trabajo de Apache Cassandra a Amazon Keyspaces con AWS Glue

Creado por Nikolai Kolesnikov (AWS), Karthiga Priya Chandran (AWS) y Samir Patel (AWS)

Entorno: producción	Origen: Cassandra	Destino: Amazon Keyspaces
Tipo R: N/D	Carga de trabajo: código abierto; todas las demás cargas de trabajo	Tecnologías: análisis; migración; sin servidor; macrodatos
Servicios de AWS: AWS Glue; Amazon Keyspaces; Amazon S3; AWS CloudShell		

Resumen

Este patrón le muestra cómo migrar sus cargas de trabajo actuales de Apache Cassandra a Amazon Keyspaces (para Apache Cassandra) mediante CQLReplicator en AWS Glue. Puede usar CQLReplicator en AWS Glue para minimizar el retraso en la replicación que supone la migración de sus cargas de trabajo en cuestión de minutos. También aprenderá a usar un bucket de Amazon Simple Storage Service (Amazon S3) para almacenar los datos necesarios para la migración, incluidos los archivos de configuración, los scripts y los archivos de Apache Parquet. Este patrón supone que las cargas de trabajo de Cassandra están alojadas en instancias de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) en una nube privada virtual (VPC).

Requisitos previos y limitaciones

Requisitos previos

- Clúster de Cassandra con tabla de origen
- Tabla objetivo en Amazon Keyspaces para replicar la carga de trabajo
- Bucket de S3 para almacenar archivos intermedios de Parquet que contienen cambios de datos graduales
- Bucket de S3 para almacenar archivos de configuración de trabajos y scripts

Limitaciones

- CQLReplicator en AWS Glue requiere algún tiempo para aprovisionar unidades de procesamiento de datos (DPU) para las cargas de trabajo de Cassandra. El retraso de la replicación entre el clúster de Cassandra y el espacio de claves y la tabla de destino en Amazon Keyspaces se reducirá a pocos minutos.

Arquitectura

Pila de tecnología de origen

- Apache Cassandra
- DataStax Servidor
- ScyllaDB

Pila de tecnología de destino

- Amazon Keyspaces

Arquitectura de migración

El siguiente diagrama muestra un ejemplo de arquitectura en el que un clúster de Cassandra se aloja en instancias EC2 y se distribuye en tres zonas de disponibilidad. Los nodos de Cassandra están alojados en subredes privadas.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un rol de servicio personalizado proporciona acceso a Amazon Keyspaces y al bucket de S3.
2. Un trabajo de AWS Glue lee la configuración del trabajo y los scripts del bucket de S3.
3. El trabajo de AWS Glue se conecta a través del puerto 9042 para leer los datos del clúster de Cassandra.
4. El trabajo de AWS Glue se conecta a través del puerto 9142 para escribir los datos en Amazon Keyspaces.

Herramientas

Servicios y herramientas de AWS

- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que permite interactuar con los servicios de AWS mediante comandos en el intérprete de comandos de línea de comandos.
- AWS CloudShell es un shell basado en navegador que puede utilizar para administrar los servicios de AWS mediante la interfaz de línea de comandos de AWS (AWS CLI) y una gama de herramientas de desarrollo preinstaladas.
- AWS Glue es un servicio de ETL totalmente gestionado que le permite clasificar, limpiar, enriquecer y mover datos de forma fiable entre almacenes de datos y flujos de datos.
- Amazon Keyspaces (para Apache Cassandra) es un servicio de base de datos administrada que le permite migrar, ejecutar y escalar sus cargas de trabajo de Cassandra en la nube de AWS.

Código

El código de este patrón está disponible en el repositorio de CQLReplicator. GitHub

Prácticas recomendadas

- Para determinar los recursos de AWS Glue necesarios para la migración, calcule el número de filas de la tabla de Cassandra de origen. Por ejemplo, 250 000 filas por 0,25 DPU (2 vCPU, 4 GB de memoria) con un disco de 84 GB.
- Caliente previamente las tablas de Amazon Keyspaces antes de ejecutar CQLReplicator. Por ejemplo, ocho teselas de CQLReplicator (trabajos de AWS Glue) pueden escribir hasta 22 K de WCU por segundo, por lo que el objetivo debe precalentarse a entre 25 y 30 K de WCU por segundo.
- Para habilitar la comunicación entre los componentes de AWS Glue, utilice una regla de entrada autorreferenciada para todos los puertos TCP de su grupo de seguridad.
- Utilice la estrategia de tráfico incremental para distribuir la carga de trabajo de migración a lo largo del tiempo.

Epics

Implemente CQLReplicator

Tarea	Descripción	Habilidades requeridas
Cree un espacio de claves y una tabla de destino.	1. Cree un espacio de claves y una tabla en Amazon Keyspaces. Para obtener más información sobre la capacidad de escritura, consulte los cálculos de unidades de escritura en la sección de información adicional de este patrón. También puede crear un espacio de claves mediante el Lenguaje de consultas Cassandra (CQL). Para obtener más información, consulte Crear un espacio de claves mediante CQL en la sección de información adicional de este patrón. Nota: después de crear la tabla, considere cambiarla al modo de capacidad bajo demanda para evitar cargos innecesarios. 2. Para actualizar al modo de rendimiento, ejecute el siguiente script:	Propietario de la aplicación, administrador de AWS, administrador de bases de datos, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`ALTER TABLE target_keyspace.target_table WITH CUSTOM_PROPERTIES = { 'capacity_mode': { 'throughput_mode': 'PAY_PER_REQUEST'} }`	

Tarea	Descripción	Habilidades requeridas
Configure el controlador de Cassandra para conectarse a Cassandra.	Utilice el siguiente script dde configuración: `Datastax-java-driver { basic.request.consistency = “LOCAL_QUORUM” basic.contact-points = [“127.0.0.1:9042”] advanced.reconnect-on-init = true basic.load-balancing-policy { local-datacenter = “datacenter1” } advanced.auth-provider = { class = PlainTextAuthProvider username = “user-at-sample” password = “S@MPLE=PASSWORD=” } }` Nota: el anterior script usa el conector Spark Cassandra. Para obtener más información, consulte la configuración de referencia de Cassandra.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Configure el controlador de Cassandra para conectarse a Amazon Keyspaces.	Utilice el siguiente script dde configuración: `datastax-java-driver { basic { load-balancing-pol icy { local-datacenter = us-west-2 } contact-points = ["cassandr a.us-west-2.amazon aws.com:9142"] request { page-size = 2500 timeout = 360 seconds consistency = LOCAL_QUORUM } } advanced { control-connection { timeout = 360 seconds } session-leak.thres hold = 6 connection { connect-timeout = 360 seconds init-query-timeout = 360 seconds warn-on-init-error = false } auth-provider = { class = software. aws.mcs.auth.SigV4 AuthProvider`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	<pre> aws-region = us- west-2 } ssl-engine-factory { class = DefaultSs lEngineFactory } } }</pre> Nota: el anterior script usa el conector Spark Cassandra. Para obtener más información, consulte la configuración de referencia de Cassandra.	

Tarea	Descripción	Habilidades requeridas
Cree un rol de IAM para el trabajo de AWS Glue.	Cree un nuevo rol de servicio de AWS denominado `glue-cassandra-migration` AWS Glue como entidad de confianza. Nota: `glue-cassandra-migration` Debería proporcionar acceso de lectura y escritura al bucket de S3 y a Amazon Keyspaces . El bucket de S3 contiene los archivos.jar, los archivos de configuración de Amazon Keyspaces y Cassandra y los archivos Parquet intermedi os. Por ejemplo, contiene las políticas administradas y `AWSGlueServiceRole` `AmazonS3FullAccess` , y`AmazonKeyspacesFul lAccess` .	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Descargue CQLReplicator en AWS. CloudShell	Descargue el proyecto en su carpeta de inicio ejecutando el siguiente comando: `git clone https://github.com/aws-samples/cql-replicator .git` `cd cql-replicator/glue` `# Only for AWS CloudShell, the bc package includes bc and dc. Bc is an arbitrary precision numeric processing arithmetic language` `sudo yum install bc -y`	
Modifique los archivos de configuración de referencia.	Copie `CassandraConnector.conf` y `KeyspacesConnector.conf` en el `../glue/conf` directorio de la carpeta del proyecto.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Inicie el proceso de migración.	El siguiente comando inicializa el entorno CQLReplicator. La inicialización implica copiar los artefactos.jar y crear un conector de AWS Glue, un bucket de S3, un trabajo de AWS Glue, el `migration` espacio de claves y la tabla: `ledger` `cd cql-replicator/glue/bin` `./cqlreplicator --state init --sg '"sg-1","sg-2"' \ --subnet "subnet-XXXXXXXXXXXX" \ --az us-west-2a --region us-west-2 \ --glue-iam-role glue-cassandra-migration \ --landing-zone s3://cql-replicator-1234567890-us-west-2` Este script incluye los siguientes parámetros: • `--sg`— Los grupos de seguridad que permiten el acceso al clúster de Cassandra desde AWS Glue e incluyen la regla de	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	entrada autorreferenciante para todo el tráfico • `--subnet`— La subred a la que pertenece el clúster de Cassandra • `--az`— La zona de disponibilidad de la subred • `--region`— La región de AWS en la que se implementa el clúster de Cassandra • `--glue-iam-role` — Los permisos de rol de IAM que AWS Glue puede asumir al llamar a Amazon Keyspaces y Amazon S3 en su nombre • `--landing zone`— Un parámetro opcional para reutilizar un bucket de S3 (si no proporciona un valor para el `--landing zone` parámetro, el `init` proceso intentará crear un nuevo bucket para almacenar los archivos de configura ción, los artefactos.jar y los archivos intermedios).	

Tarea	Descripción	Habilidades requeridas
Valide la implementación.	Tras ejecutar el comando anterior, la cuenta de AWS debe contener lo siguiente: • El trabajo de AWS Glue de CQLReplicator y el conector de AWS Glue en AWS Glue • El depósito S3 que almacena los artefactos • El espacio de claves de destino `migration` y la `ledger` tabla en Amazon Keyspaces	AWS DevOps

Ejecute CQLReplicator

Tarea	Descripción	Habilidades requeridas
Inicie el proceso de migración.	Para utilizar CQLReplicator en AWS Glue, debe utilizar el `--state run` comando seguido de una serie de parámetros. La configuración precisa de estos parámetros viene determinada principal mente por sus requisitos de migración únicos. Por ejemplo, esta configuración puede variar si decide replicar los valores y las actualizaciones del tiempo de vida (TTL) o si descarga objetos que superen 1 MB a Amazon S3.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	Para replicar la carga de trabajo del clúster de Cassandra a Amazon Keyspaces, ejecute el siguiente comando: `./cqlreplicator --state run --tiles 8 \ --landing-zone s3://cql-replicator-1234567890-us-west-2 \ --region us-west-2 \ --src-keyspace source_keyspace \ --src-table source_table \ --trg-keyspace taget_keyspace \ --writetime-column column_name \ --trg-table target_table --inc-traffic` El espacio de claves y la tabla de origen se encuentran `source_keyspace.source_table` en el clúster de Cassandra. El espacio de claves y la tabla de destino se encuentran `target_keyspace.target_tabl`	

Tarea	Descripción	Habilidades requeridas
	e en Amazon Keyspaces . El parámetro `--inc-traffic` ayuda a evitar que el tráfico incremental sobrecargue el clúster de Cassandra y Amazon Keyspaces con un número elevado de solicitudes. Para replicar las actualizaciones, agréguelas `--writetime-column regular_column_name` a su línea de comandos. La columna normal se utilizará como fuente de la marca de tiempo de escritura.	

Supervise el proceso de migración

Tarea	Descripción	Habilidades requeridas
Valide las filas de Cassandra migradas durante la fase de migración histórica.	Para obtener el número de filas replicadas durante la fase de relleno, ejecute el siguiente comando: `./cqlreplicator --state stats \ --landing-zone s3://cql-replicator-1234567890-us-west-2 \ --src-keyspace source_keyspace --src-table`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	source_table --region us-west-2	

Detenga el proceso de migración

Tarea	Descripción	Habilidades requeridas
Utilice el `cqlreplicator` comando o la consola AWS Glue.	Para detener el proceso de migración correctamente, ejecute el siguiente comando: `./cqlreplicator --state request-stop --tiles 8 \ --landing-zone s3://cql-replicator-1234567890-us-west-2 \ --region us-west-2 \ --src-keyspace source_keyspace --src-table source_table` Para detener el proceso de migración de forma inmediata, utilice la consola AWS Glue.	AWS DevOps

Limpieza

Tarea	Descripción	Habilidades requeridas
Elimine los recursos desplegados.	El siguiente comando eliminará el trabajo de AWS Glue, el conector, el bucket de S3 y la tabla de Keyspaces: `ledger` `./cqlreplicator --state cleanup --landing-zone s3://cql-replicator-1234567890-us-west-2`	AWS DevOps

Solución de problemas

Problema	Solución
Los trabajos de AWS Glue fallaron y devolvieron un error de memoria insuficiente (OOM).	1. Cambie el tipo de trabajador (amplíe). Por ejemplo, cambie `G0.25X` a `G.1X` o `G.1X` a `G.2X`. Como alternativa, puede aumentar el número de DPUs por trabajo de AWS Glue (escalado horizontal) en CQLReplicator. 2. Inicie el proceso de migración desde el punto en el que se interrumpió. Para reiniciar los trabajos fallidos de CQLReplicator, vuelva a ejecutar el `--state run` comando con los mismos parámetros.

Recursos relacionados

- CQLReplicator con AWS Glue README.MD
- Documentación de AWS Glue

- Documentación de Amazon Keyspaces
- Apache Cassandra

Información adicional

Consideraciones sobre la migración

Puede usar AWS Glue para migrar la carga de trabajo de Cassandra a Amazon Keyspaces y, al mismo tiempo, mantener por completo la funcionalidad de sus bases de datos de origen de Cassandra durante el proceso de migración. Una vez completada la replicación, puede transferir sus aplicaciones a Amazon Keyspaces con un retraso de replicación mínimo (inferior a minutos) entre el clúster de Cassandra y Amazon Keyspaces. Para mantener la coherencia de datos, también puede seguir un proceso similar para replicar los datos de nuevo en el clúster de Cassandra desde Amazon Keyspaces.

Cálculos de unidades de escritura

Pongamos que, por ejemplo, desea escribir 500.000.000 con un tamaño de fila de 1 KiB durante una hora. El número total de unidades de escritura (WCU) de Amazon Keyspaces que necesita se basa en este cálculo:

```
(number of rows/60 mins 60s) 1 WCU per row = (500,000,000/(60*60s) * 1 WCU)
= 69,444 WCUs required
```

La tasa de 1 hora es de 69.444 WCU por segundo, pero puede añadir algo de capacidad adicional. Por ejemplo, `69,444 * 1.10 = 76,388 WCUs` tiene una capacidad adicional del 10 por ciento.

Cree un espacio de claves mediante CQL

Para crear un espacio de claves con CQL, ejecute los siguientes comandos:

```
CREATE KEYSPACE target_keyspace WITH replication = {'class': 'SingleRegionStrategy'}
CREATE TABLE target_keyspace.target_table ( userid uuid, level text, gameid int,
 description text, nickname text, zip text, email text, updatetime text, PRIMARY KEY
 (userid, level, gameid) ) WITH default_time_to_live = 0 AND CUSTOM_PROPERTIES =
 {'capacity_mode':{ 'throughput_mode':'PROVISIONED', 'write_capacity_units':76388,
 'read_capacity_units':3612 }} AND CLUSTERING ORDER BY (level ASC, gameid ASC)
```

Migración de Oracle Business Intelligence 12c a la nube de AWS desde servidores en las instalaciones

Creada por Lanre (Lan-Ray) showunmi (AWS) y Patrick Huang (AWS)

Entorno: producción	Origen: en las instalaciones	Destino: Amazon EC2, Amazon RDS, Amazon ALB, Amazon EFS
Tipo R: redefinir la plataforma	Carga de trabajo: Oracle	Tecnologías: análisis; bases de datos
Servicios de AWS: Amazon EBS; Amazon EC2; Amazon EFS; CloudFormation AWS; Elastic Load Balancing (ELB); AWS Certificate Manager (ACM)		

Resumen

Este patrón muestra cómo migrar Oracle Business Intelligence Enterprise Edition 12c de los servidores locales a la nube de AWS mediante AWS. CloudFormation También describe cómo puede usar otros servicios de AWS para implementar componentes de Oracle BI 12c y obtener alta disponibilidad, seguridad, flexibilidad y capacidad de escalado dinámico.

Para ver una lista de las prácticas recomendadas relacionadas con la migración de Oracle BI 12c a la nube de AWS, consulte la sección de Información adicional de este patrón.

Nota: Se recomienda realizar varias migraciones de prueba antes de transferir los datos existentes de Oracle BI 12c a la nube. Estas pruebas le ayudarán a ajustar su enfoque de migración, identificar y solucionar posibles problemas y estimar los requisitos de tiempo de inactividad con mayor precisión.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Conectividad de red segura entre los servidores en las instalaciones y AWS a través de los servicios de AWS Virtual Private Network (AWS VPN) o AWS Direct Connect
- Licencias de software para su sistema operativo Oracle, Oracle BI 12c, Oracle Database, Oracle WebLogic Server y Oracle HTTP Server

Limitaciones

Para obtener más información sobre límites de almacenamiento, consulte la documentación de Amazon Relational Database Service (Amazon RDS) para Oracle.

Versiones de producto

- Oracle Business Intelligence Enterprise Edition 12c
- WebLogic Servidor Oracle 12c
- Oracle HTTP Server 12c
- Oracle Database 12c (o posterior)
- Oracle Java SE 8

Arquitectura

El siguiente diagrama muestra un ejemplo de arquitectura para ejecutar componentes de Oracle BI 12c en la nube de AWS:

En el siguiente diagrama se muestra la arquitectura:

1. Amazon Route 53 para proporcionar la configuración de sistema de nombres de dominio (DNS).
2. Elastic Load Balancing (ELB) distribuye el tráfico de red para mejorar la escalabilidad y la disponibilidad de los componentes de Oracle BI 12c en múltiples zonas de disponibilidad.
3. Los grupos de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2) alojan los servidores Oracle HTTP, el servidor Weblogic Admin y los servidores de BI administrados en varias zonas de disponibilidad.
4. Amazon Relational Database Service (Amazon RDS) para bases de datos de Oracle almacena metadatos de BI Server en varias zonas de disponibilidad.

5. Amazon Elastic File System (Amazon EFS) está montado en todos los componentes de Oracle BI 12c para el almacenamiento de archivos compartidos.

Pila de tecnología

- Amazon Elastic Block Store (Amazon EBS)
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Elastic File System (Amazon EFS)
- Amazon RDS para Oracle
- AWS Certificate Manager (ACM)
- Elastic Load Balancing (ELB)
- Oracle BI 12c
- WebLogic Servidor Oracle 12c
- Oracle HTTP Server (OHS)

Herramientas

- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- AWS Certificate Manager (ACM) le ayuda a crear, almacenar y renovar certificados y claves SSL/TLS X.509 públicos y privados que protegen sus sitios web y aplicaciones de AWS.
- AWS Database Migration Service (AWS DMS) le permite migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones.
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon EC2 Auto Scaling le ayuda a mantener disponible la aplicación y le permite añadir o quitar automáticamente instancias de Amazon EC2 según las condiciones que defina.
- Amazon Elastic File System (Amazon EFS) le ayuda a crear y configurar sistemas de archivos compartidos en la nube de AWS.
- Elastic Load Balancing permite distribuir el tráfico entrante de las aplicaciones entre distintos destinos. Así, por ejemplo, puede distribuir el tráfico a través de instancias de Amazon Elastic

Compute Cloud (Amazon EC2), contenedores y direcciones IP de una o varias zonas de disponibilidad.

- Amazon Relational Database Service (Amazon RDS) le ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esta red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.
- Oracle Data Pump le ayuda a trasladar datos y metadatos de una base de datos a otra a altas velocidades.
- Oracle Fusion Middleware es un conjunto de herramientas de desarrollo de aplicaciones y soluciones de integración para la gestión de identidades, la colaboración y la generación de informes de inteligencia empresarial.
- Oracle le GoldenGate ayuda a diseñar, ejecutar, organizar y monitorizar sus soluciones de replicación y procesamiento de datos en streaming en la infraestructura de nube de Oracle.
- La herramienta Oracle WebLogic Scripting Tool (WLST) proporciona una interfaz de línea de comandos que le ayuda a escalar horizontalmente sus clústeres. WebLogic

Epics

Evalúe el entorno de origen

Tarea	Descripción	Habilidades requeridas
Recopile información sobre el inventario de software.	Identifique las versiones y los niveles de parches de cada uno de los component es de software de su pila de tecnología de origen, incluidos los siguientes: • El sistema operativo de Oracle • Oracle Database	Arquitecto de migración, arquitecto de soluciones, propietario de la aplicación, administrador de Oracle BI

Tarea	Descripción	Habilidades requeridas
	• Oracle BI 12c • Servidor Oracle WebLogic • Servidor de Oracle HTTP • Java	
Recopile información sobre el inventario de cómputo y almacenamiento.	En su entorno de origen, revise las métricas de uso actuales e históricas para comprobar lo siguiente: • Uso de la CPU • Uso de memoria • Uso del almacenamiento Importante: asegúrese de tener en cuenta los picos históricos de uso.	Arquitecto de migración, arquitecto de soluciones, propietario de la aplicación, administrador de Oracle BI, administrador de sistema
Recopile información sobre la arquitectura del entorno de origen y sus requisitos.	Comprenda por completo la arquitectura de su entorno de origen y sus requisito s, incluidos los siguientes aspectos: • Configuración WebLogic del dominio de Oracle Server • Agrupamiento en clústeres • Equilibrio de carga • Conectividad • Disponibilidad • Requisitos de recuperación de desastres	Arquitecto de migración, arquitecto de soluciones, propietario de la aplicación, administrador de Oracle BI

Tarea	Descripción	Habilidades requeridas
Identifique orígenes de datos de Java Database Connectivity (JDBC).	Recopile información sobre los orígenes de datos JDBC y los controladores de su entorno de origen para cada motor de base de datos que utilice.	Arquitecto de migración, propietario de la aplicación, administrador de Oracle BI, ingeniero o administrador de bases de datos
Recopile información sobre la configuración específica del entorno.	Recopile información sobre los ajustes y configuraciones específicos de su entorno de origen, incluidos los siguientes: • Scripts de inicio y cierre personalizados • Java y otras variables de entorno • Certificados	Arquitecto de migración, arquitecto de soluciones, propietario de la aplicación, administrador de Oracle BI
Identifique cualquier dependencia de otras aplicaciones.	Recopile información sobre las integraciones de su entorno de origen que crean dependencias con otras aplicaciones. Importante: asegúrese de identificar las integraciones de Lightweight Directory Access Protocol (LDAP) y otros requisitos de red.	Arquitecto de migración, arquitecto de soluciones, propietario de la aplicación, administrador de Oracle BI

Diseñe su entorno de destino

Tarea	Descripción	Habilidades requeridas
Cree un documento de diseño de alto nivel.	Cree un documento de diseño de arquitectura de destino. Asegúrese de usar la información que recopiló al evaluar su entorno de origen para elaborar el documento de diseño.	Arquitecto de soluciones, arquitecto de aplicaciones, ingeniero de bases de datos, arquitecto de migraciones
Obtenga la aprobación del documento de diseño.	Revise el documento de diseño con las partes interesadas y obtenga las aprobaciones necesarias.	Propietario de la aplicación o servicio, arquitecto de soluciones, arquitecto de aplicaciones

Implementación de la infraestructura

Tarea	Descripción	Habilidades requeridas
Prepare el código de infraestructura en CloudFormation.	Cree CloudFormation plantillas para aprovisionar su infraestructura de Oracle BI 12c en la nube de AWS. Para obtener más información, consulte Trabajar con CloudFormation plantillas de AWS en la Guía del CloudFormation usuario de AWS. Nota: Se recomienda crear CloudFormation plantillas modulares para cada nivel de Oracle BI 12c, en lugar	Arquitecto de infraestructura de nube, arquitecto de soluciones y arquitecto de aplicaciones

Tarea	Descripción	Habilidades requeridas
	de crear una plantilla grande para todos los recursos. Para obtener más información sobre las prácticas CloudFormation recomendadas, consulte 8 prácticas recomendadas para automatizar las implementaciones con AWS CloudFormation en el blog de AWS.	
Descargue el software necesario.	Descargue el siguiente software junto con las versiones y los parches necesarios del sitio web de Oracle: • Java JDK8 • Servidor Oracle 12c WebLogic • Oracle BI 12c	Arquitecto de migraciones, ingeniero de bases de datos, arquitecto de aplicaciones

Tarea	Descripción	Habilidades requeridas
Prepare los scripts de instalación.	Cree scripts de instalación de software que ejecuten una instalación silenciosa. Estos scripts simplifican la automatización de la implementación. Para obtener más información, consulte OBIEE 12c: ¿Cómo realizar una instalación silenciosa? en el sitio de Oracle Support. Necesitará una cuenta de Oracle Support para acceder a estos documentos.	Arquitecto de migraciones, ingeniero de bases de datos, arquitecto de aplicaciones

Tarea	Descripción	Habilidades requeridas
Cree una AMI de Linux con respaldo Amazon EBS para los niveles de web y aplicaciones.	1. Implemente y configure instancias de Amazon EC2 para sus niveles web y de aplicaciones. Asegúrese de que las instancias cumplan los requisitos previos para ejecutar lo siguiente: • Entorno de sistema operativo Oracle configurado • Cuenta de usuario de sistema operativo Oracle configurada • Instalación de software Java 2. Cree imágenes de máquina de Amazon (AMI) de las instancias y guarde copias para usarlas en el futuro. Para más información, consulte Creación de una AMI de Linux con respaldo en Amazon EBS en la Guía de usuario de Amazon EC2 para instancias de Linux.	Arquitecto de migraciones, ingeniero de bases de datos, arquitecto de aplicaciones

Tarea	Descripción	Habilidades requeridas
Lance su infraestructura de AWS mediante CloudFormation.	Implemente sus niveles web y de aplicaciones de Oracle BI 12c en módulos mediante las CloudFormation plantillas que ha creado. Para obtener instrucciones, consulte Introducción a AWS CloudFormation en la Guía del CloudFormation usuario de AWS.	Arquitecto de infraestructura de nube, arquitecto de soluciones y arquitecto de aplicaciones

Migración de Oracle BI 12c a AWS mediante una instalación nueva

Tarea	Descripción	Habilidades requeridas
Prepare el software necesario.	Instale el software necesario en una ubicación a la que puedan acceder las instancias de Amazon EC2. Por ejemplo, puede instalar el software en Amazon S3 o en otra instancia de Amazon EC2 a la que puedan acceder sus servidores web y de aplicaciones.	Arquitecto de migración, arquitecto de Oracle BI, arquitecto de infraestructura en la nube, arquitecto de soluciones y arquitecto de aplicaciones
Prepare la base de datos del repositorio para la instalación de Oracle BI 12c.	Cree esquemas de Oracle BI 12c ejecutando la utilidad de creación de repositorios de Oracle (RCU) en una nueva instancia de base de datos Amazon RDS para Oracle.	Arquitecto de infraestructura en la nube, arquitecto de soluciones, arquitecto de aplicaciones, arquitecto de migración, arquitecto de Oracle BI

Tarea	Descripción	Habilidades requeridas
Instale Oracle Fusion Middleware 12c y Oracle BI 12c.	1. A partir de una instancia de Amazon EC2, instale la infraestructura Oracle Fusion Middleware 12c y OBIEE 12c. Para obtener más información, consulte las siguientes secciones de la Guía de implement ación empresarial de Oracle Fusion Middleware para Oracle Business Intellige nce: • Inicie el instalador de infraestructura en BIHOST1 • Instalación de Oracle Business Intelligence como preparación para una implementación empresarial Nota: Use Amazon EFS para alojar los directorios que se compartirán entre los nodos del clúster de Oracle BI 12c. 2. Aplique los parches necesarios a la instalación. 3. Cree imágenes de máquina de Amazon (AMI) de las instancias y guarde copias para usarlas en el futuro.	Arquitecto de migración, arquitecto de Oracle BI

Tarea	Descripción	Habilidades requeridas
Configure su dominio WebLogic de Oracle Server para Oracle BI 12c.	Configure su dominio de Oracle BI 12c como implementación no agrupada en clúster. Para obtener más información, consulte Configurar el dominio BI en la Guía de implementación empresarial de Oracle Fusion Middleware para Oracle Business Intelligence.	Arquitecto de migración, arquitecto de Oracle BI
Realice un escalado horizontal a partir de Oracle BI 12c.	Escale horizontalmente el nodo único hasta el número deseado de nodos. Para obtener más información, consulte Escalado horizontal de Oracle Business Intelligence en la Guía de implementación empresarial de Oracle Fusion Middleware para Oracle Business Intelligence.	Arquitecto de migración, arquitecto de Oracle BI

Tarea	Descripción	Habilidades requeridas
Instale el servidor HTTP 12c de Oracle.	1. Instale el servidor HTTP 12c de Oracle en las instancias de Amazon EC2 de nivel web de Oracle. Para obtener más instrucciones, consulte Instalación del servidor HTTP 12c de Oracle en Instalación y configuración del servidor HTTP de Oracle para Oracle Access Management 12c. 2. Aplique los parches necesarios a la instalación. 3. Cree imágenes de máquina de Amazon (AMI) de las instancias y guarde copias para usarlas en el futuro.	Arquitecto de migración, arquitecto de Oracle BI
Configure los equilibradores de carga para la finalización de SSL.	1. Solicite o importe un certificado en ACM. 2. Asocie los certificados SSL con ELB.	Arquitecto de infraestructura de nube, arquitecto de migraciones

Tarea	Descripción	Habilidades requeridas
Migre los artefactos de metadatos de inteligencia empresarial a AWS.	1. Exporte los archivos de Oracle Business Intelligence Application Archive (BAR) desde la instalación de Oracle BI 12c en las instalaciones. Para exportar los archivos BAR, utilice la herramienta de secuencias de WebLogic comandos (WLST) para ejecutar el comando. exportServiceInstance 2. Importe los archivos BAR en las instalaciones a la instalación de AWS Oracle BI 12c. Para importar los archivos BAR, ejecute el comando importServiceInstanceWLST.	Arquitecto de migración, arquitecto de Oracle BI

Tarea	Descripción	Habilidades requeridas
Realice las tareas posteriores a la migración.	Después de importar los archivos BAR, haga lo siguiente: • Configure cualquier origen de datos JDBC adicional. • Instale controladores para otros orígenes de datos, como PostgreSQL o Amazon Redshift. • Configure LDAP, SSL, el inicio de sesión único (SSO) y el almacén de seguridad de Oracle. WebLogic • Configuración de políticas de AWS Identity and Access Management (IAM). • Active el seguimiento del uso. • Configure integraciones con otros sistemas. • Migre cualquier script personalizado.	Arquitecto de migración, arquitecto de Oracle BI

Pruebe el nuevo entorno

Tarea	Descripción	Habilidades requeridas
Pruebe el nuevo entorno de Oracle BI 12c.	Realice end-to-end pruebas en el nuevo entorno Oracle BI 12c. Utilice la automatización en la medida de lo posible.	Arquitecto de migración, arquitecto de soluciones, propietario de la aplicación, administrador de Oracle BI

Tarea	Descripción	Habilidades requeridas
	A continuación se muestran ejemplos de actividades de prueba: • Validación de paneles, informes y URL • Pruebas de aceptación de usuarios (UAT) • Pruebas de aceptación operativa (OAT) Nota: Realice pruebas y validaciones adicionales según sea necesario.	

Realizar la transición al nuevo entorno

Tarea	Descripción	Habilidades requeridas
Desconecte el tráfico al entorno Oracle BI 12c en las instalaciones.	En la ventana de transición designada, detenga todo el tráfico al entorno Oracle BI 12c en las instalaciones.	Arquitecto de migración, arquitecto de soluciones, propietario de la aplicación, administrador de Oracle BI
Vuelva a sincronizar la nueva base de datos del repositorio Oracle BI 12c con la base de datos de origen.	Vuelva a sincronizar la base de datos del repositorio Oracle Oracle BI 12c de Amazon RDS con la base de datos en las instalaciones. Para sincronizar las bases de datos, puede realizar una actualización de Oracle Data Pump o una captura de datos	Administrador de BI, ingeniero /administrador de bases de datos de Oracle

Tarea	Descripción	Habilidades requeridas
	de cambios (CDC) de AWS DMS.	
Cambie las URL de Oracle BI 12c para que apunten al nuevo entorno de AWS.	Actualice las URL de Oracle BI 12c en sus servidores DNS internos para que apunten a la nueva instalación de AWS.	Arquitecto de migración, arquitecto de soluciones, propietario de la aplicación, administrador de Oracle BI
Supervise el nuevo entorno.	Supervise el nuevo entorno de Oracle BI 12c con cualquier a de las siguientes herramien tas: • Amazon CloudWatch • Amazon RDS Performance Insights • Oracle Enterprise Manager	Administrador de Oracle BI, ingeniero/administrador de bases de datos, administrador de aplicaciones
Obtenga la aprobación del proyecto.	Revise los resultados de las pruebas con las partes interesadas y obtenga las aprobaciones necesarias para finalizar la migración.	Propietario de la aplicació n, propietario del servicio, arquitecto de infraestructura de nube, arquitecto de migración, arquitecto de BI de Oracle

Recursos relacionados

- Uso de Oracle Repository Creation Utility en Amazon RDS para Oracle (Guía de usuario de Amazon RDS)
- Amazon RDS en Oracle (Guía de usuario de Amazon RDS)
- Oracle WebLogic Server 12c en AWS (documento técnico de AWS)
- Implementación de Oracle Business Intelligence para una alta disponibilidad (Centro de ayuda de Oracle)
- Archivos Oracle Business Intelligence Application (BAR) (Centro de ayuda de Oracle)

- Cómo migrar OBI 12c entre entornos (Soporte de Oracle)

Información adicional

La siguiente es una lista de prácticas recomendadas relacionadas con la migración de Oracle BI 12c a la nube de AWS.

Bases de datos de repositorio

Se recomienda alojar los esquemas de bases de datos de Oracle BI 12c en una instancia de Amazon RDS para Oracle. Este tipo de instancia proporciona una capacidad rentable y redimensionable, a la vez que automatiza tareas de administración como el aprovisionamiento de hardware, la configuración de bases de datos, la aplicación de parches y las copias de seguridad.

Para obtener más información, consulte Uso de la utilidad de creación de repositorios de Oracle en RDS para Oracle en la Guía del usuario de Amazon RDS.

Niveles web y de aplicaciones

Las instancias de Amazon EC2 con memoria optimizada suelen ser adecuadas para los servidores Oracle BI 12c. Sea cual sea el tipo de instancia que elija, asegúrese de que las instancias que aprovisione cumplan con los requisitos de uso de memoria del sistema. Además, asegúrese de configurar un tamaño de pila de máquina virtual WebLogic Java (JVM) suficiente en función de la memoria disponible de la instancia Amazon EC2.

Almacenamiento local

La E/S desempeña un papel importante en el rendimiento general de su aplicación Oracle BI 12c. Amazon Elastic Block Store (Amazon EBS) ofrece diferentes clases de almacenamiento optimizadas para distintos patrones de carga de trabajo. Asegúrese de elegir un tipo de volumen de Amazon EBS que se adapte a su caso de uso.

Para obtener más información acerca de tipo de volúmenes de EBS, consulte Características de Amazon EBS en la documentación de Amazon EBS.

Almacenamiento compartido

Un dominio Oracle BI 12c agrupado en clúster requiere almacenamiento compartido para los siguientes recursos:

- Archivos de configuración
- Directorio de datos singleton (SDD) de Oracle BI 12c
- Caché global de Oracle
- Scripts de Oracle BI Scheduler
- Binarios de Oracle Server WebLogic

Puede satisfacer este requisito de almacenamiento compartido con Amazon EFS, que proporciona un sistema de archivos Network File System (NFS) elástico, escalable y totalmente administrado.

Optimizar el rendimiento del almacenamiento compartido

Amazon EFS tiene dos modos de rendimiento: aprovisionado y en ráfaga. El servicio también tiene dos modos de rendimiento: de uso general y de E/S máxima.

Para ajustar el rendimiento, comience por probar sus cargas de trabajo en el modo de rendimiento de uso general y en el modo de rendimiento aprovisionado. Realizar estas pruebas le ayudará a determinar si dichos modos de referencia son suficientes para cumplir con los niveles de servicio deseados.

Para obtener más información, consulte Rendimiento de Amazon EFS en la Guía del usuario de Amazon EFS.

Disponibilidad y recuperación de desastres

Se recomienda implementar los componentes de Oracle BI 12c en varias zonas de disponibilidad para proteger los recursos en caso de que se produzca un fallo en una zona de disponibilidad. La siguiente lista incluye las prácticas recomendadas de disponibilidad y recuperación de desastres para recursos específicos de Oracle BI 12c alojados en la nube de AWS:

- Bases de datos de repositorios Oracle BI 12c: implemente una instancia de base de datos de Amazon RDS con múltiples zonas de disponibilidad en su base de datos de repositorios Oracle BI 12c. En un despliegue Multi-AZ, Amazon RDS aprovisiona y mantiene automáticamente una réplica en espera sincrónica en una AZ diferente. Ejecutar una instancia de base de datos de repositorio de Oracle BI 12c entre regiones de alta disponibilidad puede mejorar la disponibilidad durante el mantenimiento de sistema planificado y ayuda a proteger sus bases de datos contra los errores de las instancias de base de datos y las interrupciones de las zonas de disponibilidad.
- Servidores gestionados Oracle BI 12c: para lograr la tolerancia a errores, se recomienda implementar los componentes del sistema Oracle BI 12c en servidores gestionados de un grupo

de Amazon EC2 Auto Scaling configurado para abarcar varias zonas de disponibilidad. Auto Scaling reemplaza las instancias defectuosas según las comprobaciones de estado de Amazon EC2. En caso de que se produzca un error en la zona de disponibilidad, los servidores HTTP de Oracle seguirán dirigiendo el tráfico a los servidores gestionados de la zona de disponibilidad en funcionamiento. Después, Auto Scaling lanzará instancias para cumplir con sus requisitos de recuento de hosts. Se recomienda activar la replicación del estado de la sesión HTTP para garantizar que las sesiones existentes se conmuten por error a los servidores gestionados en funcionamiento.

- Servidores de administración Oracle BI 12c: para asegurarse de que su servidor de administración tiene alta disponibilidad, alójelo en un grupo de Amazon EC2 Auto Scaling configurado para abarcar varias zonas de disponibilidad. A continuación, defina el tamaño mínimo y máximo del grupo en 1. Si se produce un error en una zona de disponibilidad, Amazon EC2 Auto Scaling iniciará un servidor de administración de reemplazo en una zona de disponibilidad alternativa. Para recuperar cualquier host subyacente que haya fallado dentro de la misma zona de disponibilidad, puede activar la Recuperación automática de Amazon EC2.
- Servidores Oracle Web Tier: se recomienda asociar su servidor HTTP de Oracle con su dominio de Oracle WebLogic Server. Para obtener una alta disponibilidad, implemente su servidor HTTP de Oracle en un grupo de Amazon EC2 Auto Scaling configurado para asentar varias zonas de disponibilidad. A continuación, instale el servidor detrás de un equilibrador de carga elástico ELB. Para ofrecer protección adicional contra errores en el host, puede activar la Recuperación automática de Amazon EC2.

Escalabilidad

La elasticidad de la nube de AWS le ayuda a escalar las aplicaciones horizontal o verticalmente en respuesta a las necesidades de su carga de trabajo.

Escalado vertical

Para escalar verticalmente la aplicación, puede cambiar el tamaño y tipo de las instancias de Amazon EC2 en las que se ejecutan los componentes de Oracle BI 12c. No necesita aprovisionar en exceso las instancias al inicio de la implementación, ni incurrir en costos innecesarios.

Escalado horizontal

Amazon EC2 Auto Scaling le ayuda a escalar horizontalmente su aplicación añadiendo o eliminando automáticamente servidores gestionados en función de las necesidades de su carga de trabajo.

Nota: El escalado horizontal con Amazon EC2 Auto Scaling requiere conocimientos de creación de scripts y pruebas exhaustivas para su implementación.

Copia de seguridad y recuperación

La siguiente lista incluye las prácticas recomendadas de disponibilidad y recuperación de desastres para recursos específicos de Oracle BI 12c alojados en la nube de AWS:

- Repositorios de metadatos de Oracle Business Intelligence: Amazon RDS crea y guarda automáticamente copias de seguridad de las instancias de sus bases de datos. Estas copias de seguridad se retienen durante el período que usted especifique. Asegúrese de configurar la duración y retención de las copias de seguridad de Amazon RDS en función de sus requisitos de protección de datos. Para obtener información adicional, consulte Copia de seguridad y restauración de Amazon RDS.
- Servidores gestionados, servidores de administración y servidores de nivel web: asegúrese de configurar las instantáneas de Amazon EBS en función de sus requisitos de protección y retención de datos.
- Almacenamiento compartido: puede gestionar las copias de seguridad y la recuperación de los archivos almacenados en Amazon EFS mediante AWS Backup. El servicio AWS Backup también se puede implementar para gestionar de forma centralizada las copias de seguridad y la recuperación de otros servicios, como Amazon EC2, Amazon EBS y Amazon RDS. Para obtener más información, consulte ¿Qué es AWS Backup? En la guía para desarrolladores de AWS Lambda.

Seguridad y conformidad

La siguiente lista de prácticas recomendadas de seguridad y servicios de AWS puede ayudarle a proteger sus aplicaciones de Oracle BI 12c en la nube de AWS:

- Cifrado en reposo: Amazon RDS, Amazon EFS y Amazon EBS son compatibles con los algoritmos de cifrado estándar del sector. Puede utilizar AWS Key Management Service (AWS KMS) para crear y administrar claves criptográficas, así como a controlar su uso en una amplia gama de servicios de AWS y en sus aplicaciones. También puede configurar Oracle Transparent Data Encryption (TDE) en la instancia de base de datos Amazon RDS para Oracle que aloja la base de datos del repositorio Oracle BI 12c.
- Cifrado en tránsito: se recomienda activar los protocolos SSL o TLS para proteger los datos en tránsito entre las distintas capas de la instalación de Oracle BI 12c. Puede usar AWS Certificate

Manager (ACM) para aprovisionar, administrar e implementar certificados SSL y TLS públicos y privados para los recursos de Oracle BI 12c.

- Seguridad de la red: asegúrese de implementar los recursos de Oracle BI 12c en una VPC de Amazon con los controles de acceso adecuados configurados para su caso de uso. Configure sus grupos de seguridad para filtrar el tráfico entrante y saliente de las instancias de Amazon EC2 en las que se ejecuta la instalación. Asegúrese también de configurar listas de control de acceso a la red (NACL) que permitan o denieguen el tráfico en función de las reglas definidas.
- Supervisión y registro: puede utilizar AWS CloudTrail para realizar un seguimiento de las llamadas a las API a su infraestructura de AWS, incluidos los recursos de Oracle BI 12c. Esta funcionalidad resulta útil para supervisar los cambios en la infraestructura o para realizar análisis de seguridad. También puede utilizar Amazon CloudWatch para ver datos operativos que le proporcionarán información útil sobre el rendimiento y el estado de su aplicación Oracle BI 12c. Puede configurar alarmas y tomar medidas automatizadas en función de esas alarmas. Amazon RDS proporciona herramientas de supervisión adicionales, incluidas Enhanced Monitoring y Performance Insights.

Migre un clúster de Apache Kafka local a Amazon MSK mediante MirrorMaker

Creado por Han Zhang (AWS) y Tanner Pratt (AWS)

Entorno: PoC o piloto	Origen: clúster de Apache Kafka autogestionado o en las instalaciones	Destino: Amazon Managed Streaming para Apache Kafka (Amazon MSK)
Tipo R: redefinir la plataforma	Carga de trabajo: código abierto; todas las demás cargas de trabajo	Tecnologías: análisis; macrodatos; migración
Servicios de AWS: Amazon MSK		

Resumen

Este patrón proporciona instrucciones para migrar un clúster de Apache Kafka en las instalaciones, autogestionado o alojado a Amazon Managed Streaming para Apache Kafka (Amazon MSK). También puede usar este patrón para migrar de un clúster de Amazon MSK a otro.

Apache Kafka incluye la MirrorMaker función, que replica los datos entre dos clústeres de Kafka. MirrorMaker consiste en un conjunto de consumidores que forman parte de un grupo de consumidores. Los consumidores leen los datos de los temas del clúster de origen y, a continuación, los pasan a los productores, que los escriben en el clúster de destino.

La documentación de Amazon MSK contiene una descripción general de alto nivel del proceso de uso de la MirrorMaker versión 1.0 para migrar clústeres de Kafka locales a Amazon MSK. Este patrón complementa esta información al ofrecer step-by-step instrucciones completas para usar la versión 2.0. MirrorMaker

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa

- Un clúster de origen de Kafka que sea uno de los siguientes tipos:
  - En un centro de datos en las instalaciones
  - Autoadministrado en la nube
  - Alojado a través de un socio

Limitaciones

- Para usar la MirrorMaker versión 2.0, el clúster de origen debe utilizar la versión 2.4.0 o posterior de Apache Kafka. Para versiones anteriores, consulte las instrucciones de la documentación de Amazon MSK para utilizar la MirrorMaker versión 1.0.

Versiones de producto

- MirrorMaker versión 2.0
- Apache Maven versión 2.4.0 o posterior. Para obtener más información sobre las versiones de Apache Kafka compatibles con Amazon MSK, consulte Versiones de Apache Kafka compatibles.

Arquitectura

Pila de tecnología de origen

- Clúster de Kafka autogestionado o en las instalaciones

Pila de tecnología de destino

- Clúster de Amazon RDS

Arquitectura de destino

En el diagrama se muestra los siguientes procesos:

1. MirrorMaker lee los datos de los temas y grupos de consumidores del clúster de Kafka de origen.
2. MirrorMaker replica los datos y la información del consumidor en el clúster de Amazon MSK de destino.

Herramientas

Servicios de AWS

- Amazon Elastic Compute Cloud (Amazon EC2) brinda capacidad de computación escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon Managed Streaming para Apache Kafka (Amazon MSK) es un servicio completamente administrado que le permite crear y ejecutar aplicaciones que utilizan Apache Kafka para procesar datos de streaming.
- Amazon Virtual Private Cloud (Amazon VPC) permite lanzar recursos de AWS en una red virtual que se haya definido. Esa red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Otras herramientas

- Apache Kafka es una plataforma de transmisión de eventos de código abierto. En este patrón, se utiliza la MirrorMakerfunción de Kafka para realizar la migración entre clústeres.

Prácticas recomendadas

Puede ejecutarlo MirrorMaker en el entorno de origen o en el de destino, pero se recomienda ejecutarlo lo más cerca posible del clúster de destino. Para obtener más información, consulte las Prácticas recomendadas: consumir desde remoto, producir a local en la documentación de Apache Kafka.

Epics

Cree la VPC y el clúster de Amazon MSK de destino

Tarea	Descripción	Habilidades requeridas
Cree una VPC.	1. Cree una VPC en la cuenta de destino de AWS. Para obtener instrucciones, consulte la sección Crear una VPC.	Administrador de sistemas, DevOps ingeniero y administrador de la nube de AWS

Tarea	Descripción	Habilidades requeridas
	2. Cree tres subredes privadas en diferentes zonas de disponibilidad de la nueva VPC. Para obtener instrucciones, consulte la sección Crear una subred. El uso de diferentes zonas de disponibilidad proporcio na alta disponibilidad y tolerancia a errores. Nota: si usa una conexión pública a Internet para migrar el clúster de Kafka, cree subredes públicas y habilite el acceso público al clúster de Amazon MSK.	
Cree el clúster de Amazon MSK.	Cree un clúster de Amazon MSK. Para obtener más instrucciones, consulte Crear un clúster mediante la consola de administración de AWS o Crear un clúster mediante la CLI de AWS. Configure el clúster para que use la VPC y las subredes que creó anteriormente.	Administrador de sistemas, DevOps ingeniero y administr ador de la nube de AWS

Configurar MirrorMaker

Tarea	Descripción	Habilidades requeridas
Instalar MirrorMaker.	1. Lance una instancia EC2. 2. Conéctese a su instancia EC2. 3. En la instancia de EC2, descargue y extraiga la última versión de Kafka. Para obtener instrucciones, consulte Inicio rápido (documentación de Kafka). Nota: En este patrón, se instala MirrorMaker 2.0 como un MirrorMaker clúster dedicado en una instancia de Amazon EC2. Esta opción es aceptable en entornos de desarrollo, y es el enfoque que se emplea en este patrón. Para obtener más información sobre otras opciones de implementación de la MirrorMaker versión 2.0, consulte la sección de información adicional de este patrón.	Administrador de sistemas de AWS, administrador de la nube, DevOps ingeniero
Especifique la información del clúster de Kafka.	En la carpeta de instalación `bin` del cliente de Kafka, cree un archivo mm2.properties y configúrelo para el clúster de Kafka de origen. Para obtener instrucciones, consulte	Administrador de sistemas de AWS, administrador de la nube, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Ejecutar un MirrorMaker clúster dedicado (document ación de Kafka).	
Comience MirrorMaker.	Introduzca el siguiente comando para iniciar MirrorMaker y pasar el archivo mm2.properties. `$ ./bin/connect-mirr or-maker.sh mm2.prope rties`	Administrador de sistemas de AWS, administrador de la nube, DevOps ingeniero
Monitorear el progreso.	Compruebe el progreso inspeccionando el desfase entre el último desfase de cada tema y el desfase actual que MirrorMaker está consumiendo el tema. Para obtener más instrucci ones, consulte Supervisa r la georeplicación en la documentación de Kafka.	Administrador de sistemas de AWS, administrador de la nube, DevOps ingeniero

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Detenga las aplicaciones de consumidor.	Detenga todas las aplicacio nes de consumidor que consuman datos del clúster de origen.	Desarrollador de aplicaciones
Inicie las aplicaciones de consumidor.	Modifique la configuración de arranque de las aplicacio	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	nes para que apunte al clúster de destino. A continuación, comience a consumir en el clúster de destino.	
Detenga los productores en el clúster de origen.	Cuando las aplicaciones de consumidor se estén consumiendo correctam ente en el clúster de destino, detenga los productores del clúster de origen.	Desarrollador de aplicaciones
Inicie los productores en el clúster de destino.	Modifique la configuración de los servidores de arranque del productor y apunte al clúster de destino. Espere MirrorMak er a que termine de duplicar todos los datos del clúster de origen antes de iniciar los productores.	Desarrollador de aplicaciones
Pare. MirrorMaker	Una vez que los productores se hayan mudado al grupo objetivo, deténgase MirrorMak er.	Administrador de sistemas de AWS, administrador de la nube, DevOps ingeniero

Recursos relacionados

Recursos de AWS

- Migración de clústeres mediante MirrorMaker (documentación de Amazon MSK)
- Laboratorios de migración de Amazon MSK (AWS Workshop Studio)

Otros recursos

- MirrorMaker 2.0 (Propuestas de mejora de Apache Kafka)
- Georreplicación: duplicación de datos entre clústeres (documentación de Apache Kafka)

Información adicional

Este patrón ejecuta la MirrorMaker versión 2.0 como un MirrorMaker clúster dedicado en Amazon EC2. Esta opción es aceptable en entornos de desarrollo. Aunque no se describe en este patrón, también puede ejecutar MirrorMaker 2.0 en un clúster de Kafka Connect. Esta opción de implementación emplea un marco dentro del ecosistema de Kafka que mejora la escalabilidad y el mantenimiento. El conector se implementa en un clúster de Kafka Connect con la configuración asociada para ejecutar la aplicación. El conector se puede ejecutar en modo independiente para el desarrollo o las pruebas, o bien en modo distribuido para producción. Para obtener más información, consulte Ejecución MirrorMaker en un clúster de Connect (documentación de Apache Kafka). Para obtener más información sobre otras opciones de implementación de la MirrorMaker versión 2.0, consulte Tutorial: Ejecutar MirrorMaker 2.0 (documentación de Kafka).

Migre ELK Stack a Elastic Cloud en AWS

Creado por Battulga Purevragchaa (AWS), uday Reddy y Antony Prasad Thevaraj (AWS)

Entorno: producción	Origen: Elasticsearch	Destino: Elastic Cloud
Tipo R: redefinir la plataforma	Carga de trabajo: todas las demás cargas de trabajo	Tecnologías: análisis; seguridad, identidad y conformidad
Servicios de AWS: Amazon EC2 Auto Scaling; Amazon EFS; Elastic Load Balancing (ELB); Amazon S3; Amazon Route 53		

Resumen

Elastic ha prestado servicios durante muchos años y, por lo general, sus usuarios y clientes administran Elastic ellos mismos en las instalaciones. Elastic Cloud, el servicio gestionado de Elasticsearch, proporciona una forma de consumir Elastic Stack (ELK Stack) y soluciones de búsqueda empresarial, observabilidad y seguridad. Puede acceder a las soluciones de Elastic con aplicaciones de registro, métricas, APM (supervisión del rendimiento de las aplicaciones) y SIEM (administración de eventos e información de seguridad). También puede usar características integradas como machine learning, gestión de ciclo de vida de índices y Kibana Lens (para visualizaciones de arrastrar y soltar).

Cuando transiciona de Elasticsearch autogestionado a Elastic Cloud, el servicio de Elasticsearch se ocupa de lo siguiente:

- Aprovisionamiento y administración de la infraestructura subyacente
- Creación y administración de clústeres de Elasticsearch
- Escalado vertical y horizontal de los clústeres
- Actualizaciones, parches y toma de instantáneas

Todo esto le brinda más tiempo para resolver otros desafíos.

Este patrón define cómo migrar de Elasticsearch 7.13 en las instalaciones a Elasticsearch en Elastic Cloud en Amazon Web Services (AWS). Es posible que otras versiones requieran pequeñas modificaciones de los procesos descritos en este patrón. Para obtener más información, contacte con su representante de Elastic.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa con acceso a Amazon Simple Storage Service (Amazon S3) para las instantáneas
- Un enlace privado seguro y con un ancho de banda suficientemente alto para copiar archivos de datos de instantáneas a Amazon S3
- Amazon S3 Transfer Acceleration
- Políticas de Elastic Snapshot para garantizar que la ingesta de datos se archive con regularidad, ya sea en un almacén de datos local lo suficientemente grande o en un almacenamiento remoto (Amazon S3)

Debe conocer el tamaño de sus instantáneas y las políticas de ciclo de vida de los índices correspondientes en las instalaciones antes de iniciar la migración. Para obtener más información, póngase en contacto con Elastic.

Roles y habilidades

El proceso de migración también requiere los roles y la experiencia que se describen en la siguiente tabla.

Rol	Experiencia	Responsabilidades
Compatibilidad con aplicaciones	Familiaridad con Elastic Cloud y Elastic en las instalaciones	Todas las tareas relacionadas con Elastic
Administrador de sistemas o administrador de base de datos	Conocimiento profundo del entorno de Elastic en las instalaciones y su configuración	Capacidad de aprovisionar almacenamiento, instalar y usar la Interfaz de la línea de comandos de AWS (AWS CLI) e identificar todos los orígenes

		de datos que alimentan Elastic en las instalaciones
Administrador de red	Conocimiento de la conectividad, la seguridad y el rendimiento de la red en las instalaciones a AWS	Creación de enlaces de red desde las instalaciones a Amazon S3 y conocimiento del ancho de banda de conectividad

Limitaciones

- Elasticsearch en Elastic Cloud solo está disponible en regiones de AWS compatibles (septiembre de 2021).

Versiones de producto

- Elasticsearch 7.13

Arquitectura

Pila de tecnología de origen

Elasticsearch 7.13 o posterior en las instalaciones:

- Instantáneas del clúster
- Instantáneas de índice
- Configuración de Beats

Arquitectura de la tecnología de origen

El siguiente diagrama muestra una arquitectura típica en las instalaciones con diferentes métodos de ingesta, tipos de nodos y Kibana. Los distintos tipos de nodos reflejan las funciones de clúster, autenticación y visualización de Elasticsearch.

1. Ingestión de Beats a Logstash

2. Ingestión de Beats a cola de mensajes de Apache Kafka
3. Ingestión de Filebeat a Logstash
4. Ingestión de cola de mensajes de Apache Kafka a Logstash
5. Ingestión de Logstash a clúster de Elasticsearch
6. Clúster de destino de Elasticsearch
7. Nodo de autenticación y notificación
8. Nodos de Kibana y blob

Pila de tecnología de destino

Elastic Cloud se implementa en su cuenta de software como servicio (SaaS) en varias regiones de AWS con replicación entre clústeres.

- Instantáneas del clúster
- Instantáneas de índice
- Configuraciones de Beats
- Elastic Cloud
- Equilibrador de carga de red
- Amazon Route 53
- Amazon S3

Arquitectura de destino

La infraestructura gestionada de Elastic Cloud es:

- De alta disponibilidad, ya que está presente en varias zonas de disponibilidad y varias regiones de AWS.
- Tolerante a fallos en la región, ya que los datos (índices e instantáneas) se replican mediante la replicación entre clústeres (CCR) de Elastic Cloud
- De archivo, porque las instantáneas se archivan en Amazon S3
- Tolerante a particiones de red mediante una combinación de equilibradores de carga de red y Route 53
- La ingesta de datos se origina, entre otros, en Elastic APM, Beats y Logstash

Pasos de migración de alto nivel

Elastic ha desarrollado su propia metodología prescriptiva para migrar de Elastic Cluster en las instalaciones a Elastic Cloud. La metodología de Elastic está directamente alineada y complementa la guía y las prácticas recomendadas de migración de AWS, incluidos el marco Well-Architected y el Programa de aceleración de la migración (MAP). Por lo general, las tres fases de migración a AWS son las siguientes:

- Evaluación
- Movilización
- Migrar y modernizar

Elastic sigue fases de migración similares con terminología complementaria:

- Iniciar
- Planificar
- Implementar
- Entregar
- Cerrar

Elastic usa la metodología de implementación de Elastic para facilitar la entrega de los resultados del proyecto. Su diseño es inclusivo para garantizar que Elastic, los equipos de consultoría y los equipos de cliente trabajen juntos con claridad para lograr, de forma conjunta, los resultados esperados.

La metodología de Elastic combina fases tradicionales en cascada con Scrum en la fase de implementación. Las configuraciones de los requisitos técnicos se proporcionan de forma iterativa y colaborativa, minimizando el riesgo.

Herramientas

Servicios de AWS

- Amazon Route 53: Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad. Puede utilizar Route 53 para realizar tres funciones principales en cualquier combinación: registro de dominio, direccionamiento DNS y comprobación de estado.

- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos. Puede utilizar Amazon S3 para almacenar y recuperar cualquier cantidad de datos en cualquier momento y desde cualquier parte de la web. Este patrón emplea un bucket de S3 y Amazon S3 Transfer Acceleration.
- Elastic Load Balancing: Elastic Load Balancing distribuye automáticamente el tráfico entrante entre varios destinos, por ejemplo, instancias EC2, contenedores y direcciones IP en una o varias zonas de disponibilidad.

Otras herramientas

- Beats: Beats envía datos desde Logstash o Elasticsearch
- Elastic Cloud: Elastic Cloud es un servicio gestionado para alojar Elasticsearch.
- Elasticsearch: Elasticsearch es un motor de búsqueda y análisis que usa Elastic Stack para almacenar de forma centralizada los datos con el fin de realizar búsquedas y análisis escalables. Este patrón también emplea creación de instantáneas y replicación entre clústeres.
- Logstash: Logstash es un sistema de procesamiento de datos en el lado del servidor que ingiere datos de varias fuentes, los transforma y, a continuación, los envía al almacenamiento de datos.

Epics

Preparativos para la migración

Tarea	Descripción	Habilidades requeridas
Identifique los servidores que ejecutan la solución Elastic en las instalaciones.	Confirme que se puede realizar la migración a Elastic.	Propietario de la aplicación
Comprenda la configuración del servidor en las instalaciones.	Para comprender la configuración del servidor necesaria para gestionar correctamente las cargas de trabajo en las instalaciones, averigüe el tamaño del hardware del servidor, la configuración de	Compatibilidad con aplicaciones

Tarea	Descripción	Habilidades requeridas
	la red y las características del almacenamiento actual	
Recopile la información del usuario y de la cuenta de la aplicación.	Identifique los nombres de usuario y los nombres de las aplicaciones que emplea el entorno de Elastic en las instalaciones.	Administrador de sistemas, soporte de aplicaciones
Documente la configuración de Beats y del remitente de datos.	Para documentar las configuraciones, consulte los orígenes de datos y los receptores de datos existentes. Para obtener más información, consulte la documentación de Elastic.	Compatibilidad con aplicaciones
Determine la velocidad y el volumen de los datos.	Establezca una línea base para la cantidad de datos que gestiona el clúster.	Administrador de sistemas, soporte de aplicaciones
Documente los escenarios de RPO y RTO.	Documente los escenarios de objetivo de punto de recuperación (RPO) y objetivo de tiempo de recuperación (RTO) en términos de interrupciones y acuerdos de nivel de servicio (SLA).	Propietario de aplicaciones, administrador de sistemas, soporte de aplicaciones
Determine la configuración óptima del ciclo de vida de las instantáneas.	Defina la frecuencia con la que se deben proteger los datos mediante el uso de instantáneas de Elastic durante y después de la migración.	Propietario de aplicaciones, administrador de sistemas, soporte de aplicaciones

Tarea	Descripción	Habilidades requeridas
Defina las expectativas de rendimiento tras la migración.	Genere métricas sobre las actualizaciones de pantalla actuales y esperadas, los tiempos de ejecución de las consultas y el comportamiento de la interfaz de usuario.	Administrador de sistemas, soporte de aplicaciones
Documente los requisitos de acceso a Internet, ancho de banda y disponibilidad.	Compruebe la velocidad, la latencia y la resistencia de las conexiones a Internet para copiar instantáneas en Amazon S3.	Administrador de red
Documente los costos actuales del tiempo de ejecución de Elastic en las instalaciones.	Asegúrese de que el tamaño del entorno de destino de AWS esté diseñado para ser rentable y de alto rendimiento.	Administrador de base de datos, administrador de sistemas, soporte de aplicaciones
Identifique las necesidades de autenticación y autorización.	Las características de seguridad de Elastic Stack proporcionan dominios integrados, como Protocolo ligero de acceso a directorios (LDAP), lenguaje de marcado de aserciones de seguridad (SAML) y OpenID Connect (OIDC).	Administrador de base de datos, administrador de sistemas, soporte de aplicaciones
Conozca los requisitos regulatorios específicos en función de la ubicación geográfica.	Asegúrese de que los datos se exportan y cifran según sus necesidades y los requisitos regulatorios pertinentes.	Administrador de base de datos, administrador de sistemas, soporte de aplicaciones

Implemente la migración

Tarea	Descripción	Habilidades requeridas
Prepare el área de almacenamiento en Amazon S3.	Para recibir instantáneas en Amazon S3, cree un bucket de S3 y un rol temporal de AWS Identity and Access Management (IAM) con acceso total al bucket recién creado. Para obtener más información, consulte Creación de un rol para delegar permisos a un usuario de IAM. También puede utilizar AWS Security Token Service para solicitar credenciales de seguridad temporales. Proteja la ID de clave de acceso, la clave de acceso secreta y el token de sesión. Activar Amazon S3 Transfer Acceleration en el bucket.	Administrador de AWS
Instale AWS CLI y el complemento Amazon S3 en las instalaciones.	En cada nodo de Elasticse arch, ejecute el siguiente comando. `sudo bin/elasticsearch-plugin install repository-s3` A continuación, reinicie el nodo.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Configure el acceso de cliente de Amazon S3.	Añada las claves creadas anteriormente ejecutando los siguientes comandos. `elasticsearch-keystore add s3.client.default.access_key` `elasticsearch-keystore add s3.client.default.secret_key` `elasticsearch-keystore add s3.client.default.session_token`	Administrador de AWS
Registre un repositorio de instantáneas para los datos de Elastic	Use Kibana Dev Tools para indicar al clúster local en las instalaciones en qué bucket remoto de S3 debe escribir.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Configure la política de instantáneas.	Para configurar la administración del ciclo de vida de las instantáneas, en la pestaña Políticas de Kibana, seleccione Política de SLM y defina qué horas, flujos de datos o índices deben incluirse y qué nombres usar. Configure una política que tome instantáneas frecuentes. Las instantáneas son graduales, y hacen un uso eficiente del almacenamiento. Adecue esta configuración a la evaluación realizada. La política también puede especificar una política de retención y eliminar automáticamente las instantáneas cuando ya no las necesite.	Compatibilidad con aplicaciones
Compruebe que las instantáneas funcionan.	En Kibana Dev Tools, ejecute el siguiente comando. `GET _snapshot/<your_repo_name>/_all`	Administrador de sistemas, soporte de aplicaciones
Implemente un nuevo clúster en Elastic Cloud.	Inicie sesión en Elastic y elija un clúster de “observabilidad, búsqueda o seguridad” según el resultado de la evaluación empresarial realizada.	Administrador de sistemas, soporte de aplicaciones

Tarea	Descripción	Habilidades requeridas
Configure el acceso al almacén de claves del clúster.	El nuevo clúster debe tener acceso al bucket de S3 que almacenará las instantáneas. En la consola de servicio de Elasticsearch, seleccione Seguridad e introduzca las claves de acceso y de IAM secretas que creó anteriorm ente.	Administrador de AWS
Configure el clúster alojado de Elastic Cloud para acceder a Amazon S3.	Configure un nuevo acceso de clúster al repositorio de instantáneas creado anteriorm ente en Amazon S3. También puede hacer lo siguiente de Kibana: 1. Elija Stack Managemen t, Snapshot Settings, RegisterRepo. 2. En el campo Alias, introduzca el nombre del repositorio. 3. En Nombre del cliente de S3, seleccione secundario. 4. Agregue al repositorio el bucket de S3 que creó anteriormente. 5. Seleccione Comprimir instantánea. 6. En la sección de Cifrado, mantenga la configuración predeterminada.	Administrador de sistemas, soporte de aplicaciones

Tarea	Descripción	Habilidades requeridas
Verifique el nuevo repositorio de Amazon S3.	Asegúrese de poder acceder a su nuevo repositorio alojado en el clúster de Elastic Cloud.	Administrador de AWS
Inicialice el clúster de servicios de Elasticsearch.	En la consola de servicio de Elasticsearch, inicialic e el clúster de servicios de Elasticsearch a partir de la instantánea de S3. Ejecute los siguientes comandos como POST. `*/_close?expand_wi ldcards=all` `/_snapshot/<your-r epo-name>/ <your-sna pshot-name>/_restore` `*/_open?expand_wil dcards=all`	Soporte de aplicaciones

Complete la migración

Tarea	Descripción	Habilidades requeridas
Compruebe que la restaurac ión de la instantánea se ha realizado correctamente.	En Kibana Dev Tools, ejecute el siguiente comando. `GET _cat/indices`	Compatibilidad con aplicacio nes
Vuelva a implementar los servicios de ingestión.	Conecte los puntos de conexión de Beats y Logstash	Compatibilidad con aplicacio nes

Tarea	Descripción	Habilidades requeridas
	al nuevo punto de conexión del servicio Elasticsearch.	

Pruebe el entorno del clúster y límpielo

Tarea	Descripción	Habilidades requeridas
Valide el entorno del clúster.	Tras migrar el entorno de clúster de Elastic en las instalaciones a AWS, puede conectarse a él y usar sus propias herramientas de pruebas de aceptación de usuarios (UAT) para validar el nuevo entorno.	Compatibilidad con aplicaciones
Limpie los recursos.	Tras validar la correcta migración del clúster, elimine el bucket de S3 y el rol de IAM usado para la migración.	Administrador de AWS

Recursos relacionados

Referencias de Elastic

- Elastic Cloud
- Elasticsearch gestionado y Kibana en AWS
- Búsqueda empresarial de Elastic
- Integraciones de Elastic
- Observabilidad de Elastic
- Seguridad de Elastic
- Beats
- Elastic APM

- Migrar a gestión de ciclo de vida de índice
- Suscripciones de Elastic
- Contacte con Elastic

Publicaciones de blog de Elastic

- Cómo migrar de Elasticsearch autogestionado a Elastic Cloud en AWS (publicación de blog)
- Migrar a Elastic Cloud (publicación de blog)

Documentación de Elastic

- Tutorial: Automatice las copias de seguridad con SLM
- ILM: gestión del ciclo de vida del índice
- Logstash
- Replicación entre clústeres (CCR)
- Procesos de ingesta
- Ejecute solicitudes de API de Elasticsearch
- Retención de instantáneas

Vídeo y seminario web de Elastic

- Migración a Elastic Cloud
- Elastic Cloud: ¿Por qué migran los clientes? (seminario web)

Referencias de AWS

- Elastic Cloud en AWS Marketplace
- Interfaz de línea de comandos de AWS
- AWS Direct Connect
- Programa de aceleración de la migración AWS
- Equilibrador de carga de red
- Regiones y zonas de disponibilidad
- Amazon Route 53

- Amazon Simple Storage Service
- Amazon S3 Transfer Acceleration
- Conexiones de VPN
- Marco de buena arquitectura

Información adicional

Si desea migrar cargas de trabajo complejas, contrate los servicios de consultoría de Elastic. Si tiene dudas básicas sobre las configuraciones y los servicios, contacte con el equipo de soporte de Elastic.

Migre datos a la nube de AWS mediante Starburst

Creado por Antony Prasad Thevaraj (AWS), Shaun Van Staden (Starburst) y Suresh Veeragoni (AWS)

Entorno: Producción	Tecnologías: análisis; lagos de datos; bases de datos	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon EKS		

Resumen

Starburst ayuda a acelerar su migración de datos a Amazon Web Services (AWS) con un motor de consultas empresarial que reúne los orígenes de datos existentes en un único punto de acceso. Puede realizar análisis en varios orígenes de datos para obtener información valiosa antes de finalizar cualquier plan de migración. Sin interrumpir el business-as-usual análisis, puede migrar los datos mediante el motor Starburst o una aplicación dedicada a extraer, transformar y cargar (ETL).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una nube privada virtual (VPC).
- Un clúster de Amazon Elastic Kubernetes Service (Amazon EKS)
- Un grupo de escalado automático de Amazon Elastic Compute Cloud (Amazon EC2)
- Lista de las cargas de trabajo actuales del sistema que deben migrarse
- Conectividad de red desde AWS a su entorno en las instalaciones

Arquitectura

Arquitectura de referencia

El siguiente diagrama de arquitectura de alto nivel muestra una implementación típica de Starburst Enterprise en la nube de AWS:

1. El clúster de Starburst Enterprise se ejecuta en su cuenta de AWS.
2. El usuario se autentica mediante Lightweight Directory Access Protocol (LDAP) u Open Authorization (OAuth) e interactúa directamente con el clúster de Starburst.
3. Starburst se puede conectar a varios orígenes de datos de AWS, como AWS Glue, Amazon Simple Storage Service (Amazon S3), Amazon Relational Database Service (Amazon RDS) y Amazon Redshift. Starburst proporciona capacidades de consulta federada en todos los orígenes de datos en la nube de AWS, en las instalaciones o en otros entornos de nube.
4. Para lanzar Starburst Enterprise en un clúster de Amazon EKS, use gráficos de Helm.
5. Starburst Enterprise emplea grupos de Amazon EC2 Auto Scaling e instancias de spot de Amazon EC2 para optimizar la infraestructura.
6. Starburst Enterprise se conecta directamente a sus orígenes de datos existentes en las instalaciones para leer los datos en tiempo real. Si ya cuenta con una implementación de Starburst Enterprise en este entorno, puede conectar directamente su nuevo clúster de Starburst en la nube de AWS al clúster ya existente.

Tenga en cuenta lo siguiente:

- Starburst no es una plataforma de virtualización de datos. Es un motor de consultas de procesamiento paralelo masivo (MPP) basado en SQL que conforma la base de una estrategia global de malla de datos para el análisis.
- Cuando Starburst se implementa como parte de una migración, tiene conectividad directa con la infraestructura existente en las instalaciones.
- Starburst proporciona varios conectores empresariales y de código abierto integrados que facilitan la conectividad con diferentes sistemas heredados. Para obtener una lista completa de los conectores y sus capacidades, consulte Conectores en la Guía del usuario de Starburst Enterprise.
- Starburst puede consultar datos en tiempo real desde orígenes de datos en las instalaciones. Esto permite migrar los datos sin interrumpir las operaciones empresariales habituales.
- Si va a migrar desde una implementación de Starburst Enterprise existente en las instalaciones, puede usar el conector especial Starburst Stargate para conectar su clúster de Starburst Enterprise en AWS directamente con su clúster en las instalaciones. Esto proporciona ventajas de rendimiento adicionales cuando los usuarios empresariales y los analistas de datos federan las consultas de la nube de AWS a su entorno en las instalaciones.

Descripción general del proceso

Puede acelerar los proyectos de migración de datos con Starburst, ya que Starburst le permite obtener información de todos sus datos antes de migrarlos. La siguiente imagen muestra el proceso típico de migración de datos mediante Starburst.

Roles

Por lo general, son necesarios los siguientes roles para completar una migración con Starburst:

- Administrador de la nube: responsable de que los recursos de la nube estén disponibles para ejecutar la aplicación Starburst Enterprise
- Administrador de Starburst: responsable de instalar, configurar, administrar y dar soporte a la aplicación Starburst
- Ingeniero de datos: responsable de:
  - Migración de los datos antiguos a la nube
  - Crear vistas semánticas para respaldar la analítica
- Propietario de la solución o del sistema: responsable de la implementación general de la solución

Herramientas

Servicios de AWS

- Amazon EC2: Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de AWS.
- Amazon EKS: Amazon Elastic Kubernetes Service (Amazon EKS) es un servicio administrado para ejecutar Kubernetes en AWS sin necesidad de montar o mantener su propio plano de control de Kubernetes. Kubernetes es un sistema de código abierto para automatizar la implementación, escalado y administración de las aplicaciones en contenedores.

Otras herramientas

- Helm: Helm es un administrador de paquetes para Kubernetes que le ayuda a instalar y administrar aplicaciones en el clúster de Kubernetes.

- Starburst Enterprise: Starburst Enterprise es un motor de consulta de procesamiento paralelo masivo (MPP) basado en SQL que constituye la base de una estrategia global de malla de datos para análisis.
- Starburst Stargate: Starburst Stargate vincula los catálogos y los orígenes de datos de un entorno Starburst Enterprise, como un clúster de un centro de datos en las instalaciones, con los catálogos y orígenes de datos de otro entorno Starburst Enterprise, como un clúster en la nube de AWS.

Epics

Evalúe los datos

Tarea	Descripción	Habilidades requeridas
Identifique y priorice sus datos.	Identifique los datos que desea transferir. Los grandes sistemas heredados en las instalaciones pueden incluir datos cruciales que desee migrar y, además, datos que no quiera o pueda mover por motivos de cumplimie nto. Comenzar inventari ando sus datos le ayudará a priorizar cuáles deben migrarse primero. Para obtener más información, consulte Introducción a la detección automática de cartera.	Ingeniero de datos, Administr ador de base de datos
Explore, realice un inventario y haga copias de seguridad de sus datos.	Valide la calidad, cantidad y relevancia de los datos según su caso de uso. Realice copias de seguridad o cree una instantánea de los datos según sea necesario, y finalice	Ingeniero de datos, Administr ador de base de datos

Tarea	Descripción	Habilidades requeridas
	el entorno de destino para los datos.	

Configure el entorno Starburst Enterprise

Tarea	Descripción	Habilidades requeridas
Configure Starburst Enterprise en la nube de AWS.	Mientras se catalogan los datos, configure Starburst Enterprise en un clúster gestionado de Amazon EKS. Para obtener más información, consulte Implementación con Kubernetes en la Documenta ción de referencia de Starburst Enterprise. Esto permite realizar business-as-usual análisis mientras la migración de datos está en proceso.	Administrador de AWS, desarrollador de aplicaciones
Connect Starburst a los orígenes de datos.	Una vez que haya identific ado los datos y configurado Starburst Enterprise, conecte Starburst a los orígenes de datos. Starburst lee los datos directamente del origen de datos como una consulta SQL. Para más información, consulte la documentación de referencia de Starburst Enterprise.	Administrador de AWS, desarrollador de aplicaciones

Migrar datos

Tarea	Descripción	Habilidades requeridas
Cree y ejecute los procesos de ETL.	Comience el proceso de migración de datos. Esta actividad se puede realizar al mismo tiempo que la business-as-usual analítica. Puede realizar la migración con Starburst o con un producto de terceros. Starburst puede leer y escribir datos en diferentes fuentes. Para más información, consulte la documentación de referencia de Starburst Enterprise.	Ingeniero de datos
Valide los datos.	Una vez migrados los datos, valídelos para asegurarse de que todos los datos necesarios se hayan trasladado y estén intactos.	Ingeniero de datos, DevOps ingeniero

Transición e implementación

Tarea	Descripción	Habilidades requeridas
Transicione los datos.	Una vez finalizada la migración y validación de los datos, puede realizar la transición. Deberá cambiar los enlaces de conexión de datos en Starburst. En lugar de apuntar a las fuentes en	Ingeniero de datos, responsable de transición

Tarea	Descripción	Habilidades requeridas
	las instalaciones, apunte a las nuevas fuentes en la nube y actualice las vistas semántica s. Para más información, consulte Conectores en la documentación de referencia de Starburst Enterprise.	
Implemente para los usuarios.	Los consumidores de datos comienzan a trabajar con los orígenes de datos migrados. Este proceso es invisible para los usuarios finales de análisis.	Responsable de transición; Ingeniero de datos

Recursos relacionados

AWS Marketplace

- Starburst Galaxy
- Starburst Enterprise
- Datos de Starburst JumpStart
- Starburst Enterprise con Graviton

Documentación de Starburst

- Guía del usuario de Starburst Enterprise
- Documentación de referencia de Starburst Enterprise

Otra documentación de AWS

- Introducción a la detección automática de cartera (Recomendaciones de AWS)
- Optimizar el coste y el rendimiento de la infraestructura de nube con Starburst en AWS (publicación del blog)

Optimice la incorporación ETL del tamaño del archivo de entrada en AWS

Entorno: PoC o piloto	Tecnologías: análisis; lagos de datos	Carga de trabajo: código abierto
Servicios de AWS: AWS Glue; Amazon S3		

Resumen

Este patrón muestra cómo optimizar el paso de incorporación del proceso de extracción, transformación y carga (ETL) para macrodatos y cargas de trabajo de Apache Spark en AWS Glue optimizando el tamaño de los archivos antes de procesarlos. Puede usar este patrón para evitar o resolver el problema de los archivos pequeños. Es decir, cuando un gran número de archivos pequeños ralentiza el procesamiento de datos debido al tamaño agregado de los archivos. Por ejemplo, cientos de archivos de solo unos pocos cientos de kilobytes cada uno pueden reducir considerablemente la velocidad de procesamiento de datos de sus trabajos de AWS Glue. Esto se debe a que AWS Glue realiza funciones de lista internas en Amazon Simple Storage Service (Amazon S3), y YARN (Yet Another Resource Negotiator) debe almacenar una gran cantidad de metadatos. Para mejorar la velocidad del procesamiento de datos, puede usar la agrupación de modo que sus tareas de ETL lean un grupo de archivos de entrada en una sola partición en memoria. La partición agrupa automáticamente los archivos más pequeños. Como alternativa, puede usar un código personalizado para añadir lógica de lotes a los archivos existentes.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Uno o más trabajos de AWS Glue
- Una o más cargas de trabajo de macrodatos o Apache Spark
- Un bucket de S3

Arquitectura

El siguiente patrón muestra cómo un trabajo de AWS Glue procesa los datos en distintos formatos y, a continuación, los almacena en un bucket de S3 para obtener visibilidad del rendimiento.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un trabajo de AWS Glue convierte archivos pequeños en formato CSV, JSON y Parquet en marcos dinámicos. Nota: El tamaño del archivo de entrada es lo que más influye en el rendimiento del trabajo de AWS Glue.
2. El trabajo de AWS Glue realiza funciones de lista internas en un bucket de S3.

Herramientas

- AWS Glue es un servicio ETL completamente administrado. Ayuda a clasificar, limpiar, enriquecer y mover datos de forma fiable entre almacenes de datos y flujos de datos.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Epics

Utilice la agrupación para optimizar la ingesta de ETL durante la lectura

Tarea	Descripción	Habilidades requeridas
Especifique el tamaño del grupo.	Si tiene más de 50 000 archivos, la agrupación se habilita de forma predeterminada. Sin embargo, también puede agrupar menos de 50 000 archivos especificando el tamaño del grupo en el parámetro `connectionOptions` . El parámetro `connectionOptions` está	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	en el método `create_dynamic_frame.from_options` .	

Tarea	Descripción	Habilidades requeridas
Escriba el código de agrupamiento.	Use el método `create_dynamic_frame` para crear un marco dinámico. Por ejemplo: `S3bucket_node1 = glueContext.create_dynamic_frame.from_options(format_options={"multiline": False}, connection_type="s3", format="json", connection_options={ "paths": ["s3://bucket/prefix/file.json"], "recurse": True, "groupFiles": 'inPartition', "groupSize": 1048576 }, transformation_ctx="S3bucket_node1",)`  Nota: Se usa `groupFiles` para agrupar archivos en un grupo de particiones de Amazon S3. Se usa `groupSize` para establecer el tamaño objetivo del grupo que se va a leer en la memoria. Especifique	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	`groupSize` en bytes (1048576 = 1 MB).	
Añada el código al flujo de trabajo.	Añada el código de agrupación a su flujo de trabajo en AWS Glue.	Ingeniero de datos

Use lógica personalizada para optimizar la incorporación de ETL

Tarea	Descripción	Habilidades requeridas
Elija el lenguaje y la plataforma de procesamiento.	Elija el lenguaje de scripting y la plataforma de procesamiento adecuados a su caso de uso.	Arquitecto de la nube
Escribir el código.	Escriba la lógica personalizada para agrupar sus archivos.	Arquitecto de la nube
Añada el código al flujo de trabajo.	Añada el código a su flujo de trabajo en AWS Glue. Esto permite que su lógica personalizada se aplique cada vez que se ejecute el trabajo.	Ingeniero de datos

Reparticione al escribir datos después de la transformación

Tarea	Descripción	Habilidades requeridas
Analice los patrones de consumo.	Descubra cómo las aplicaciones posteriores utilizarán los datos que escriba. Por ejemplo, si consultan datos todos los días y solo particion	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	as los datos por región o tienes archivos de salida muy pequeños, como 2,5 KB por archivo, esto no es óptimo para el consumo.	
Reparticione los datos antes de escribirlos.	Repartición basada en uniones o consultas durante el procesamiento (según la lógica de procesamiento) y después del procesami ento (según el consumo). Por ejemplo, la repartición en función del tamaño de los bytes, por ejemplo `.repartit ion(100000)` , o la repartición en función de las columnas, por ejemplo. `.repartition("colu mn_name")`	Ingeniero de datos

Recursos relacionados

- Lectura de archivos de entrada en grupos más grandes
- Supervisión de AWS Glue
- Supervisión de AWS Glue mediante CloudWatch métricas de Amazon
- Monitorización y depuración de trabajo
- Introducción a ETL sin servidor en AWS Glue

Información adicional

Determinar el tamaño del archivo

No existe una forma sencilla de determinar si el tamaño de un archivo es demasiado grande o demasiado pequeño. El impacto del tamaño del archivo en el rendimiento del procesamiento dependerá de la configuración del clúster. En Hadoop básico, se recomienda usar archivos de 128 MB o 256 MB para aprovechar al máximo el tamaño del bloque.

Para la mayoría de las cargas de trabajo de archivos de texto en AWS Glue, recomendamos un tamaño de archivo de entre 100 MB y 1 GB para un clúster de 5 a 10 DPU. Para determinar el tamaño óptimo de los archivos de entrada, supervise la sección de preprocesamiento de su trabajo de AWS Glue y, a continuación, compruebe el uso de CPU y memoria del trabajo.

Consideraciones adicionales

Si el rendimiento en las primeras etapas de la ETL supone un obstáculo, considere agrupar o fusionar los archivos de datos antes de procesarlos. Si controla por completo el proceso de generación de archivos, puede resultar aún más eficiente agregar puntos de datos en el propio sistema de origen antes de enviar los datos sin procesar a AWS.

Orqueste un proceso de ETL con validación, transformación y particionamiento mediante AWS Step Functions

Creado por Sandip Gangapadhyay (AWS)

Repositorio de código: - pipeline-pattern aws-step-functions-etl	Entorno: producción	Tecnologías: análisis; macrodatos; lagos de datos; sin servidor DevOps
Servicios de AWS: Amazon Athena; AWS Glue; AWS Lambda; AWS Step Functions		

Resumen

Este patrón describe cómo crear un proceso de extracción, transformación y carga (ETL) sin servidor para validar, transformar, comprimir y particionar un conjunto de datos CSV de gran tamaño con el fin de optimizar el rendimiento y los costos. El proceso, orquestado por AWS Step Functions, incluye características de gestión de errores, de reintento automático, y notificación a los usuarios.

Cuando se carga un archivo CSV a una carpeta de origen en un bucket de Amazon Simple Storage Service (Amazon S3), el proceso de ETL comienza a ejecutarse. El proceso valida el contenido y el esquema del archivo CSV de origen, transforma el archivo CSV a un formato comprimido de Apache Parquet, particiona el conjunto de datos por año, mes y día y lo almacena en una carpeta independiente para que las herramientas de análisis lo procesen.

El código que automatiza este patrón está disponible en el GitHub repositorio ETL Pipeline with AWS Step Functions.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- La interfaz de línea de comandos de AWS (AWS CLI) se instaló y configuró con su cuenta de AWS para que pueda crear recursos de AWS mediante la implementación de una pila de CloudFormation AWS. Se recomienda la versión 2 de AWS CLI. Para instrucciones sobre la

instalación, consulte instalación, actualización y desinstalación de la CLI de AWS versión 2 en la documentación de la CLI de AWS. Para obtener instrucciones de configuración de AWS CLI, consulte Ajustes de configuración y archivos de credenciales en la documentación de la CLI de AWS.

- Un bucket de Amazon S3.
- Un conjunto de datos CSV con el esquema correcto. (El repositorio de código incluido en este patrón proporciona un archivo CSV de muestra con el esquema y tipo de datos correctos para su uso).
- Un navegador web compatible para su uso con la consola de administración de AWS. (Consulte la lista de los navegadores compatibles).
- Acceso a la consola de AWS Glue.
- Acceso a la consola de AWS Step Functions.

Limitaciones

- En AWS Step Functions, el límite máximo para conservar los registros del historial es de 90 días. Para obtener más información, consulte Cuotas y Cuotas para flujos de trabajo estándar en la documentación de AWS Step Functions.

Versiones de producto

- Python 3.11 para AWS Lambda
- AWS Glue versión 2.0

Arquitectura

El flujo de trabajo que se muestra en el diagrama consta de los siguientes pasos de alto nivel:

1. El usuario carga un archivo CSV en la carpeta de origen de Amazon S3.
2. Un evento de notificación de Amazon S3 inicia una función de AWS Lambda que inicia la máquina de estado de Step Functions.
3. La función de Lambda valida el esquema y el tipo de datos del archivo CSV sin procesar.
4. En función de los resultados de la validación:

   a. Si la validación del archivo de origen se realiza correctamente, el archivo se mueve a la carpeta transitoria para su posterior procesamiento.
   b. Si el archivo no se valida, se mueve a la carpeta de errores y se envía una notificación de error a través de Amazon Simple Notification Service (Amazon SNS).
5. Un rastreador de AWS Glue crea el esquema del archivo sin procesar a partir de la carpeta transitoria en Amazon S3.
6. Un trabajo de AWS Glue transforma, comprime y particiona el archivo sin procesar en formato Parquet.
7. El trabajo de AWS Glue también mueve el archivo a la carpeta de transformación de Amazon S3.
8. El rastreador de AWS Glue crea el esquema a partir del archivo transformado. El esquema resultante se puede utilizar en cualquier trabajo de análisis. Puede utilizar Amazon Athena para ejecutar consultas ad-hoc.
9. Si el proceso se completa sin errores, el archivo de esquema se mueve a la carpeta de almacenamiento. Si se encuentra algún error, el archivo se mueve a la carpeta de errores.
10. Amazon SNS envía una notificación en la que se indica el éxito o el error en función del estado de finalización del proceso.

Este patrón solo emplea recursos de AWS sin servidor. No es necesario administrar servidores.

Herramientas

Servicios de AWS

- AWS Glue: AWS Glue es un servicio ETL totalmente gestionado que facilita la preparación y la carga de datos para su análisis.
- AWS Step Functions: AWS Step Functions es un servicio de orquestación sin servidor que le permite combinar funciones de Lambda AWS y otros servicios de AWS para crear aplicaciones esenciales para las empresas. A través de la consola gráfica AWS Step Functions, puede ver el flujo de trabajo de su aplicación como una serie de pasos basados en eventos.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos que ofrece escalabilidad, disponibilidad de datos, seguridad y rendimiento líderes del sector.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) es un servicio de mensajería pub/sub de alta disponibilidad, duradero, seguro y totalmente gestionado que le permite desvincular microservicios, sistemas distribuidos y aplicaciones sin servidor.

- AWS Lambda: AWS Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. AWS Lambda ejecuta el código solo cuando es necesario y amplia la capacidad de manera automática, pasando de pocas solicitudes al día a miles por segundo.

Código

El código de este patrón está disponible en el GitHub repositorio ETL Pipeline with AWS Step Functions. El repositorio de código contiene los siguientes archivos y carpetas:

- `template.yml`— CloudFormation Plantilla de AWS para crear la canalización de ETL con AWS Step Functions.
- `parameter.json` – Contiene todos los parámetros y valores de los parámetros. Actualice este archivo para cambiar los valores de los parámetros, tal y como se describe en la sección Épica.
- Carpeta `myLayer/python` – Contiene los paquetes de Python necesarios para crear la capa de AWS Lambda necesaria para este proyecto.
- Carpeta `lambda` – Contiene las siguientes funciones de Lambda:
  - `move_file.py` – Mueve el conjunto de datos de origen a la carpeta de almacenamiento, transformación o errores.
  - `check_crawler.py` – Comprueba el estado del rastreador de AWS Glue tantas veces como se haya configurado en la variable de entorno `RETRYLIMIT` antes de enviar un mensaje de error.
  - `start_crawler.py` – Inicia el rastreador de AWS Glue.
  - `start_step_function.py` – Inicia AWS Step Functions.
  - `start_codebuild.py`— Inicia el CodeBuild proyecto de AWS.
  - `validation.py` – Valida el conjunto de datos sin procesar de entrada.
  - `s3object.py` – Crea la estructura de directorios requerida dentro del bucket de S3.
  - `notification.py` – Envía notificaciones de éxito o error al final del proceso.

Para usar el código de muestra, siga las instrucciones en la sección Epics .

Epics

Preparación del archivo de origen

Tarea	Descripción	Habilidades requeridas
Clone el repositorio de código de muestra.	1. Abra el repositorio Proceso de ETL con AWS Step Functions. 2. Elija Código en la página principal del repositorio, sobre la lista de archivos, y copie la URL que aparece en Clonar con HTTPS. 3. Cambie el directorio de trabajo a la ubicación en la que desee almacenar los archivos de muestra. 4. Ejecute el siguiente comando en un terminal o en la línea de comandos: `git clone <repoURL>` `<repoURL>` es la URL que copió en el paso 2.	Desarrollador
Actualice los valores de los parámetros.	En la copia local del repositorio, edite el archivo `parameter.json` y actualice los valores de los parámetros predeterminados de la siguiente manera: • `pS3BucketName` : El nombre del bucket de S3 para almacenar los	Desarrollador

Tarea	Descripción	Habilidades requeridas
	conjuntos de datos. La plantilla creará este bucket automáticamente. El nombre del bucket tiene que ser único de forma global. • `pSourceFolder` : El nombre de la carpeta en el bucket de S3 que se usará para cargar el archivo CSV de origen. • `pStageFolder` : El nombre de la carpeta en el bucket de S3 que se usará como área transitoria durante el proceso. • `pTransformFolder` : El nombre de la carpeta en el bucket de S3 que se usará para almacenar conjuntos de datos transformados y particionados. • `pErrorFolder` : La carpeta en el bucket de S3 a la que se moverá el archivo CSV de origen si no se puede validar. • `pArchiveFolder` : el nombre de la carpeta en el bucket de S3 que se usará para cargar el archivo CSV de origen. • `pEmailforNotification` : una dirección de correo electrónico válida	

Tarea	Descripción	Habilidades requeridas
	para recibir notificaciones de éxito o error. • `pPrefix`— Una cadena de prefijo que se utilizará en el nombre del rastreador AWS Glue. • `pDatasetSchema` : el esquema del conjunto de datos con el que se validará el archivo de origen. Para la validación del conjunto de datos de origen se usa el paquete Python Cerberus. Para obtener más informaci ón, consulte el sitio web de Cerberus.	

Tarea	Descripción	Habilidades requeridas
Cargue el código fuente en el bucket de S3.	Antes de implementar la CloudFormation plantilla que automatiza la canalización de ETL, debe empaqueta r los archivos fuente de la CloudFormation plantilla y subirlos a un bucket de S3. Para ello, ejecute el siguiente comando de AWS CLI con el perfil preconfigurado: `aws cloudformation package --template-file template.yml --s3-bucket <bucket_name> --output-template-file packaged.template --profile <profile_name>` donde: • `<bucket_name>` es el nombre de un bucket de S3 existente en la región de AWS en la que desea implementar la pila. Este depósito se utiliza para almacenar el paquete de código fuente de la CloudFormation plantilla. • `<profile_name>` es un perfil de AWS CLI válido que preconfiguró al configurar AWS CLI.	Desarrollador

Creación de la pila

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation plantilla.	Para implementar la CloudFormation plantilla, ejecute el siguiente comando de la AWS CLI: `aws cloudformation deploy --stack-name <stack_name> --template-file packaged.template --parameter-overrides file://parameter.json --capabilities CAPABILITY_IAM --profile <profile_name>` donde: • `<stack_name>` es un identificador único de la CloudFormation pila. • `<profile-name>` es su perfil de AWS CLI preconfigurado.	Desarrollador
Compruebe el progreso.	En la CloudFormation consola de AWS, compruebe el progreso del desarrollo de la pila. Cuando el estado sea `CREATE_COMPLETE`, la pila se habrá implementado correctamente.	Desarrollador
Anote el nombre de la base de datos de AWS Glue.	La pestaña Resultados de la pila muestra el nombre de	Desarrollador

Tarea	Descripción	Habilidades requeridas
	la base de datos de AWS Glue. El nombre de la clave es `GlueDBOutput` .	

Prueba la canalización

Tarea	Descripción	Habilidades requeridas
Inicie el proceso de ETL.	1. Navegue hasta la carpeta de origen (`source`, o el nombre de carpeta que haya establecido en el archivo `parameter.json`) en el bucket de S3. 2. Cargue un archivo CSV de muestra en esta carpeta. (El repositorio de código proporciona un archivo de muestra llamado `Sample_Bank_Transaction_Raw_Dataset.csv` para su uso). Al cargar el archivo, se iniciará el proceso de ETL a través de Step Functions. 3. En la consola de Step Functions, compruebe el estado del proceso de ETL.	Desarrollador
Compruebe el conjunto de datos particionado.	Cuando se complete el proceso de ETL, compruebe que el conjunto de datos particionado esté disponibl	Desarrollador

Tarea	Descripción	Habilidades requeridas
	e en la carpeta de transform ación de Amazon S3 (`transform` , o el nombre de carpeta que haya estableci do en el archivo `parameter .json`).	
Compruebe la base de datos de AWS Glue particionada.	1. En la consola de AWS Glue, seleccione la base de datos de AWS Glue creada por la pila (es la base de datos que anotó en la épica anterior). 2. Compruebe que la tabla particionada esté disponible en el catálogo de datos de AWS Glue.	Desarrollador
Ejecutar consultas.	(Opcional) Use Amazon Athena para ejecutar consultas ad hoc en la base de datos particionada y transformada. Para obtener más instrucciones, consulte Ejecutar consultas SQL con Amazon Athena en la documentación de AWS.	Análisis de la base de datos

Resolución de problemas

Problema	Solución
Permisos de AWS Identity and Access Management (IAM) para el trabajo y el rastreador de AWS Glue	Si sigue personalizando la tarea de AWS Glue o el rastreador, asegúrese de conceder los permisos de IAM adecuados en la función de IAM utilizada por la tarea de AWS Glue o de proporcionar permisos de datos a AWS Lake Formation. Para obtener más información, consulte la documentación de AWS.

Recursos relacionados

Documentación de servicio de AWS

- AWS Step Functions
- AWS Glue
- AWS Lambda
- Amazon S3
- Amazon SNS

Información adicional

El siguiente diagrama muestra el flujo de trabajo de AWS Step Functions en un proceso de ETL exitoso desde el panel Inspector de Step Functions.

El siguiente diagrama muestra el flujo de trabajo de AWS Step Functions en un proceso de ETL fallido debido a un error de validación de entrada desde el panel Inspector de Step Functions.

Realizar análisis avanzados mediante Amazon Redshift ML

Entorno: PoC o piloto	Tecnologías: análisis, machine learning e inteligencia artificial	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon Redshift; Amazon SageMaker		

Resumen

En la nube de Amazon Web Services (AWS), puede utilizar el machine learning de Amazon Redshift (Amazon Redshift ML) para realizar análisis de ML de los datos almacenados en un clúster de Amazon Redshift o en Amazon Simple Storage Service (Amazon S3). Amazon Redshift ML admite el aprendizaje supervisado, que se suele utilizar para análisis avanzados. Los casos de uso de Amazon Redshift ML incluyen la previsión de ingresos, la detección de fraudes con tarjetas de crédito y las predicciones del valor de por vida del cliente (CLV) o la pérdida de clientes.

Amazon Redshift ML facilita a los usuarios de bases de datos crear, entrenar e implementar modelos de machine learning mediante comandos SQL estándar. Amazon Redshift ML utiliza Amazon SageMaker Autopilot para entrenar y ajustar automáticamente los mejores modelos de aprendizaje automático para su clasificación o regresión en función de sus datos, sin perder el control y la visibilidad.

Todas las interacciones entre Amazon Redshift, Amazon S3 y Amazon SageMaker se resumen y automatizan. Una vez entrenado e implementado el modelo de ML, pasa a estar disponible como función definida por el usuario (UDF) en Amazon Redshift y se puede usar en consultas de SQL.

Este patrón complementa el tutorial Crear, entrenar e implementar modelos de aprendizaje automático en Amazon Redshift mediante SQL con Amazon Redshift ML del blog de AWS, y el tutorial Crear, entrenar e implementar un modelo de aprendizaje automático con SageMaker Amazon del Centro de recursos de introducción.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa

- Datos existentes en una tabla de Amazon Redshift

Habilidades

- Familiaridad con los términos y conceptos que utiliza Amazon Redshift ML, incluidos machine learning, entrenamiento y predicción.. Para obtener más información, consulte Training ML models (Entrenar modelos de machine learning) en la documentación de Amazon Machine Learning (Amazon ML).
- Experiencia en la configuración de usuarios, la administración de acceso y la sintaxis SQL estándar de Amazon Redshift. Para obtener más información, consulte Introducción a Amazon Redshift en la documentación de Amazon Redshift.
- Conocimiento y experiencia en Amazon S3 y AWS Identity and Access Management (IAM).
- La experiencia en ejecución de comandos de la interfaz de la línea de comandos de AWS (AWS CLI) también es beneficiosa, pero no obligatoria.

Limitaciones

- El clúster de Amazon Redshift y el bucket de Amazon S3 deben estar en la misma región de AWS.
- El enfoque de este patrón solo admite modelos de aprendizaje supervisado, como la regresión, la clasificación binaria y la clasificación multiclase.

Arquitectura

En los siguientes pasos se explica cómo funciona Amazon Redshift ML SageMaker para crear, entrenar e implementar un modelo de aprendizaje automático:

1. Amazon Redshift exporta los datos de entrenamiento a un bucket de S3.
2. SageMaker El piloto automático preprocesa automáticamente los datos de entrenamiento.
3. Una vez invocada la `CREATE MODEL` declaración, Amazon Redshift ML la utiliza SageMaker para la formación.
4. SageMaker Autopilot busca y recomienda el algoritmo de aprendizaje automático y los hiperparámetros óptimos que optimizan las métricas de evaluación.

5. Amazon Redshift ML registra el modelo de ML de salida como una función SQL en el clúster de Amazon Redshift.
6. La función del modelo ML se puede utilizar en una instrucción SQL.

Pila de tecnología

- Amazon Redshift
- SageMaker
- Amazon S3

Herramientas

- Amazon Redshift: Amazon Redshift es un servicio de almacenamiento de datos completamente administrado, de nivel empresarial y de escala de petabytes.
- Amazon Redshift ML: Amazon Redshift machine learning (Amazon Redshift ML) es un servicio robusto basado en la nube que facilita el uso de la tecnología de machine learning a los analistas y científicos de datos con cualquier nivel de habilidades.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet.
- Amazon SageMaker: SageMaker es un servicio de aprendizaje automático totalmente gestionado.
- Amazon SageMaker Autopilot: el SageMaker piloto automático es un conjunto de funciones que automatiza las tareas clave de un proceso de aprendizaje automático (AutoML).

Código

Puede crear un modelo de ML supervisado en Amazon Redshift mediante el siguiente código:

```
“CREATE MODEL customer_churn_auto_model
FROM (SELECT state,
             account_length,
             area_code,
             total_charge/account_length AS average_daily_spend,
             cust_serv_calls/account_length AS average_daily_cases,
             churn
      FROM customer_activity
      WHERE  record_date < '2020-01-01'
```

```
    )
TARGET churn
FUNCTION ml_fn_customer_churn_auto
IAM_ROLE 'arn:aws:iam::XXXXXXXXXXXX:role/Redshift-ML'
SETTINGS (
  S3_BUCKET 'your-bucket'
);”)
```

Nota: El estado `SELECT` puede hacer referencia a las tablas normales de Amazon Redshift, a las tablas externas de Amazon Redshift Spectrum o a ambas.

Epics

Preparación de un conjunto de datos para entrenamiento y prueba

Tarea	Descripción	Habilidades requeridas
Prepare un conjunto de datos para entrenamiento y prueba.	Inicie sesión en la consola de administración de AWS y abra la SageMaker consola de Amazon. Siga las instrucciones del tutorial Build, train, and deploy a machine learning model (Crear, entrenar e implementar un modelo de machine learning) para crear un archivo.csv o Apache Parquet con una columna de etiquetas (entrenamiento supervisado) y sin encabezado. Nota: Se recomienda mezclar el conjunto de datos sin procesar y dividirlo en un conjunto de entrenamiento para entrenar el modelo (70 %) y un conjunto de prueba para evaluar el	Científico de datos

Tarea	Descripción	Habilidades requeridas
	rendimiento del modelo (30 %).	

Preparación y configuración de la pila de tecnología

Tarea	Descripción	Habilidades requeridas
Cree y configure un clúster de Amazon Redshift.	En la consola de Amazon Redshift, cree un clúster de acuerdo con sus requisitos. Para obtener más informaci ón, consulte Create a cluster (Crear un clúster) en la documentación de Amazon Redshift. Importante: los nuevos clústeres de Amazon Redshift deben crearse con la pista de mantenimiento `SQL_PREVI EW` . Para obtener más información acerca de las pistas de de previsualización, consulte Choosing cluster maintenance tracks (Seleccio nar pistas de mantenimiento del clúster) en la documenta ción de Amazon Redshift.	Administrador de base de datos, arquitecto de la nube
Cree un bucket de S3 para almacenar los datos de entrenamiento y los artefactos del modelo.	En la consola de Amazon S3, cree un bucket de S3 para los datos de entrenami ento y prueba. Para obtener más información acerca de la creación de un bucket de	Administrador de base de datos, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	S3, consulte Creación de un bucket de S3 en Inicios rápidos de AWS. Importante: asegúrese de que el clúster de Amazon Redshift y el bucket de Amazon S3 se encuentren en la misma región.	
Cree y asocie una política de IAM al clúster de Amazon Redshift.	Cree una política de IAM para permitir que el clúster de Amazon Redshift SageMaker acceda a Amazon S3. Para las instrucciones y los pasos a seguir, consulte Cluster setup for using Amazon Redshift ML (Configuración del clúster para usar Amazon Redshift ML) en la documentación de Amazon Redshift.	Administrador de base de datos, arquitecto de la nube
Permita que los usuarios y grupos de Amazon Redshift accedan a esquemas y tablas.	Otorgue permisos para permitir que los usuarios y grupos de Amazon Redshift accedan a tablas y esquemas internos y externos. Para ver los pasos e instrucciones, consulte Managing permissions and ownership (Administrar los permisos y la propiedad) en la documentación de Amazon Redshift.	Administrador de base de datos

Creación y entrenamiento del modelo de ML en Amazon Redshift

Tarea	Descripción	Habilidades requeridas
Cree y entrene el modelo de ML en Amazon Redshift.	Cree y entrene el modelo de ML en Amazon Redshift ML. Para obtener más información, consulte la instrucción `CREATE MODEL` en la documentación de Amazon Redshift.	Desarrollador, científico de datos

Cómo realizar inferencias y predicciones por lotes en Amazon Redshift

Tarea	Descripción	Habilidades requeridas
Realice una inferencia mediante la función del modelo de ML generado.	Para obtener más información sobre cómo realizar inferencias mediante la función del modelo de ML generado, consulte Prediction (Predicción) en la documentación de Amazon Redshift.	Científico de datos, usuario de inteligencia empresarial

Recursos relacionados

Preparación de un conjunto de datos para entrenamiento y prueba

- Creación, formación e implementación de un modelo de aprendizaje automático con Amazon SageMaker

Preparación y configuración de la pila de tecnología

- Creación de un clúster de Amazon Redshift

- Choosing Amazon Redshift cluster maintenance tracks (Seleccionar las pistas de mantenimiento de clústeres de Amazon Redshift)
- Creating an S3 bucket (Crear un bucket de S3)
- Setting up an Amazon Redshift cluster for using Amazon Redshift ML (Configurar un clúster de Amazon Redshift para utilizar Amazon Redshift ML)
- Managing permissions and ownership in Amazon Redshift (Administrar permisos y propiedad en Amazon Redshift)

Creación y entrenamiento del modelo de ML en Amazon Redshift

- CREATE MODEL statement in Amazon Redshift (La instrucción CREATE MODEL en Amazon Redshift)

Cómo realizar inferencias y predicciones por lotes en Amazon Redshift)

- Prediction in Amazon Redshift (Predicción en Amazon Redshift)

Otros recursos

- Getting started with Amazon Redshift ML (Introducción a Amazon Redshift ML)
- Creating, training, and deploying ML models in Amazon Redshift using SQL with Amazon Redshift ML (Crear, entrenar e implementar modelos de ML en Amazon Redshift mediante SQL con Amazon Redshift ML)
- Amazon Redshift partners (Socios de Amazon Redshift.)
- AWS machine learning competency partners (Socios con competencias en machine learning de AWS)

Acceder, consultar y unirse a las tablas de Amazon DynamoDB con Athena

Creado por Moinul Al-Mamun (AWS)

Entorno: producción	Tecnologías: Análisis; bases de datos; sin servidor; macrodatos	Servicios de AWS: Amazon Athena; Amazon DynamoDB; AWS Lambda; Amazon S3

Resumen

Este patrón muestra cómo configurar una conexión entre Amazon Athena y Amazon DynamoDB mediante el conector DynamoDB de Amazon Athena. El conector utiliza una función de Lambda de AWS para consultar los datos en DynamoDB. No es necesario escribir ningún código para configurar la conexión. Una vez establecida la conexión, puede acceder y analizar rápidamente las tablas de DynamoDB mediante la Consulta federada de Athena para ejecutar comandos SQL desde Athena. También puede unir una o más tablas de DynamoDB entre sí o con otros orígenes de datos, como Amazon Redshift o Amazon Aurora.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa con permisos para gestionar tablas de DynamoDB, los orígenes de datos de Athena, Lambda y roles de (IAM) de AWS Identity and Access Management
- Un bucket de Amazon Simple Storage Service (Amazon S3) en el que Athena puede almacenar resultados de consultas
- Un bucket de S3 en el que el conector DynamoDB de Athena puede guardar los datos a corto plazo
- Una región de AWS compatible con la versión 2 del motor Athena
- Permisos de IAM para acceder a Athena y a los buckets de S3 necesarios
- Conector Amazon Athena DynamoDB, instalado

Limitaciones

La consulta de las tablas de DynamoDB conlleva un costo. Los tamaños de tabla que superen unos pocos gigabytes (GB) pueden suponer un costo elevado. Le recomendamos que considere el costo antes de realizar cualquier operación de escaneo de una tabla completa. Para obtener más información, consulte los precios de Amazon DynamoDB. Para reducir los costos y lograr un alto rendimiento, le recomendamos que utilice siempre LIMIT en la consulta (por ejemplo, `SELECT * FROM table1 LIMIT 10`). Además, antes de realizar una consulta JOIN (unirse a) o GROUP BY (agrupar por) en un entorno de producción, tenga en cuenta el tamaño de sus tablas. Si sus tablas son demasiado grandes, considere opciones alternativas, como migrar la tabla a Amazon S3.

Arquitectura

En el siguiente diagrama se muestra la forma en que un usuario puede ejecutar una consulta SQL en una tabla de DynamoDB desde Athena.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Para consultar una tabla de DynamoDB, el usuario ejecuta una consulta SQL desde Athena.
2. Athena inicia una función de Lambda.
3. La función de Lambda consulta los datos solicitados en la tabla de DynamoDB.
4. DynamoDB regresa los datos solicitados a la función de Lambda. A continuación, la función transfiere los resultados de la consulta al usuario a través de Athena.
5. La función de Lambda almacena los datos en el bucket de S3.

Pila de tecnología

- Amazon Athena
- Amazon DynamoDB
- Amazon S3
- AWS Lambda

Herramientas

- Amazon Athena es un servicio de consultas interactivo que facilita el análisis de datos en Amazon S3 con SQL estándar.

- El Conector de DynamoDB de Amazon Athena es una herramienta de AWS que permite a Athena conectarse con DynamoDB y acceder a sus tablas mediante consultas SQL.
- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.

Epics

Crear tablas de DynamoDB de muestra

Tarea	Descripción	Habilidades requeridas
Cree la primera tabla de muestra.	1. Inicie sesión en la consola de administración de AWS y abra la consola de DynamoDB. 2. Elija Crear tabla. 3. En Nombre de tabla, introduzca dydbtable1. 4. En Clave de partición, introduzca PK1. 5. En Clave de clasificación, introduzca SK1. 6. En la sección Configuración de la tabla, elija Personali zar configuración. 7. En la sección Clase de tabla, seleccione DynamoDB Standard. 8. En la sección de Configura ción de capacidad de lectura/escritura, en el	Desarrollador

Tarea	Descripción	Habilidades requeridas
	Modo capacidad, seleccione Bajo demanda. 9. En la sección Cifrado en reposo, seleccione Propiedad de Amazon DynamoDB. 10 Elija Crear tabla.	

Tarea	Descripción	Habilidades requeridas
Inserte datos de muestra en la primera tabla.	1. Abra la consola de DynamoDB. 2. En el panel de navegación, seleccione Tabla y, a continuación, seleccione su tabla en la columna Nombre. 3. Elija Acciones y, a continuación, seleccione Crear elemento. 4. Seleccione Vista JSON. 5. En la barra de título del editor de Atributos, desactive Ver DynamoDB JSON. 6. En el editor de Atributos, introduzca los siguientes datos de muestra uno por uno: `{ "PK1": "1234", "SK1": "info", "Salary": "5000" }` `{ "PK1": "1235", "SK1": "info", "Salary": "5200" }`	Desarrollador

Tarea	Descripción	Habilidades requeridas
Cree la segunda tabla de muestra.	1. Abra la consola de DynamoDB. 2. Elija Crear tabla. 3. En Nombre de tabla, introduzca dydbtable2. 4. En Clave de partición, introduzca PK2. 5. En Clave de clasificación, introduzca SK2. 6. En la sección Configuración de la tabla, elija Personalizar configuración. 7. En la sección Clase de tabla, seleccione DynamoDB Standard. 8. En la sección de Configuración de capacidad de lectura/escritura, en el Modo capacidad, seleccione Bajo demanda. 9. En la sección Cifrado en reposo, seleccione Propiedad de Amazon DynamoDB. 10. Elija Crear tabla.	Desarrollador

Tarea	Descripción	Habilidades requeridas
Inserte datos de muestra en la segunda tabla.	1. Abra la consola de DynamoDB. 2. En el panel de navegación, seleccione Tabla y, a continuación, seleccione su tabla en la columna Nombre. 3. Elija Acciones y, a continuación, seleccione Crear elemento. 4. En la barra de título del editor de Atributos, desactive Ver DynamoDB JSON. 5. En el editor de Atributos, introduzca los siguientes datos de muestra uno por uno: `{ "PK2": "1234", "SK2": "bonus", "Bonus": "500" }` `{ "PK2": "1235", "SK2": "bonus", "Bonus": "1000" }`	Desarrollador

Crear un origen de datos en Athena para DynamoDB

Tarea	Descripción	Habilidades requeridas
Configure el conector del origen de datos.	Cree un origen de datos para DynamoDB y, a continuación, cree una función de Lambda para conectarse a ese origen de datos. 1. Inicie sesión en la consola de administración de AWS y abra la consola de Athena. 2. En el panel de navegación, seleccione Origen de datos y, a continuación, seleccione Crear origen de datos. 3. Seleccione el origen de datos de Amazon DynamoDB y, a continuación, seleccione Siguiente. 4. En la sección de Detalles del origen de datos, en Nombre del origen de datos, introduzca TestDynamoDB. 5. En la sección Detalles de conexión, seleccione una función de Lambda que ya esté implementada o seleccione Crear función de Lambda si no tiene una función de Lambda para usar en este patrón. Nota: Para obtener más informaci	Desarrollador

Tarea	Descripción	Habilidades requeridas
	ón acerca de cómo crear una función de Lambda, consulte Introducción a AWS Lambda en la Guía para desarrolladores de Lambda. 6. (Opcional) Si elige Crear función Lambda, debe configurar la CloudForm ation plantilla de AWS que incluye la aplicación Java antes de implement ar esa pila. La plantilla incluye ApplicationName SpillBucket AthenaCat alogName, y otros ajustes de la aplicación. Nota: Tras implementar esta aplicación basada en Java, la pila crea una función de Lambda que permite a Athena comunicarse con DynamoDB. Esto hace que sus tablas sean accesible s mediante comandos de SQL. 7. Implementación de la función de Lambda. 8. Elija Siguiente.	

Tarea	Descripción	Habilidades requeridas
Compruebe que la función de Lambda pueda acceder al bucket para derrames de S3.	1. Abra la consola de Lambda. 2. En el panel de navegación, seleccione Funciones y, a continuación, elija la función que creó anteriormente. 3. Elija la pestaña Configura ción. 4. En el panel izquierdo, seleccione Variables de entorno y, a continuación, confirme que el valor de la clave es `spill_bucket` . 5. En el panel izquierdo, seleccione Permisos y, a continuación, en la sección Función de ejecución, seleccione el rol de IAM asociado. Nota: Se le redirige al rol de IAM asociado a su función de Lambda en la consola de IAM. 6. Confirme que tiene permiso de escritura en el bucket `spill_bucket` . Si se producen errores, consulte la sección de Información adicional de este patrón como guía.	Desarrollador

Acceso a las tablas de DynamoDB desde Athena

Tarea	Descripción	Habilidades requeridas
Consultar las tablas de DynamoDB.	1. Inicie sesión en la consola de administración de AWS y abra la consola de Athena. 2. En el panel de navegación, seleccione Origen de datos y, a continuación, seleccione Crear origen de datos. 3. En el panel de navegación, seleccione Query Editor (Editor de consultas). 4. En la pestaña Editor, en la sección Datos, en Origen de datos, seleccione su origen de datos como Origen de datos. 5. En Database (Base de datos), elija la base de datos. 6. Para la consulta 1, introduzca la siguiente consulta: `SELECT * FROM dydbtable1 t1;` 7. Seleccione Ejecutar y, a continuación, verifique el resultado de la tabla. 8. Para la consulta 2, introduzca la siguiente consulta: `SELECT * FROM dydbtable2 t2;`	Desarrollador

Tarea	Descripción	Habilidades requeridas
	9. Seleccione Ejecutar y, a continuación, verifique el resultado de la tabla.	
Unir las dos tablas de DynamoDB.	DynamoDB es un almacén de datos NoSQL y no admite la operación de unión de SQL. En consecuencia, debe realizar una operación de unión en dos tablas de DynamoDB: 1. Elija el icono de signo más para crear otra consulta. 2. Para la consulta 3, introduzca la siguiente consulta: `SELECT pk1, salary, bonus FROM dydbtable1 t1 JOIN dydbtable2 t2 ON t1.pk1 = t2.pk2;`	Desarrollador

Recursos relacionados

- Conector para DynamoDB de Amazon Athena (Laboratorios de AWS)
- Consulte cualquier origen de datos con la nueva consulta federada de Amazon Athena (blog sobre macrodatos de AWS)
- Referencia de la versión del motor Athena (Guía del usuario de Athena)
- Simplifique la extracción y el análisis de datos de Amazon DynamoDB con AWS Glue y Amazon Athena (blog sobre bases de datos de AWS)

Información adicional

Si ejecuta una consulta en Athena con `spill_bucket` en formato `{bucket_name}/folder_name/`, puede recibir el siguiente mensaje de error:

```
"GENERIC_USER_ERROR: Encountered an exception[java.lang.RuntimeException] from your
 LambdaFunction[arn:aws:lambda:us-east-1:xxxxxx:function:testdynamodb] executed in
 context[retrieving meta-data] with message[You do NOT own the spill bucket with the
 name: s3://test-bucket-dynamodbconnector/athena_dynamodb_spill_data/]
This query ran against the "default" database, unless qualified by the query. Please
 post the error message on our forum  or contact customer support with Query Id:
 [query-id]"
```

Para resolver este error, actualice la variable de entorno de la función de Lambda de `spill_bucket` a `{bucket_name_only}` y, a continuación, actualice la siguiente política de IAM de Lambda para el acceso de escritura al bucket:

```
{
            "Action": [
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketLocation",
                "s3:GetObjectVersion",
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::spill_bucket",
                "arn:aws:s3:::spill_bucket/*"
            ],
            "Effect": "Allow"
        }
```

Como alternativa, puede quitar el conector de origen de datos de Athena que creó anteriormente y volver a crearlo utilizando solo `{bucket_name}` para `spill_bucket`.

Configure un espacio de datos mínimo viable para compartir datos entre organizaciones

Creada por Ramy Hcini (Think-it), Ismail Abdellaoui (Think-it), Malte Gasseling (Think-it), Jorge Hernandez Suarez (AWS) y Michael Miller (AWS)

Entorno: PoC o piloto	Tecnologías: análisis; contenedores y microserv icios; lagos de datos; bases de datos; infraestructura	Carga de trabajo: código abierto
Servicios de AWS: Amazon Aurora; AWS Certificate Manager (ACM); AWS CloudFormation; Amazon EC2; Amazon EFS; Amazon EKS; Elastic Load Balancing (ELB); Amazon RDS; Amazon S3; AWS Systems Manager		

Resumen

Los espacios de datos son redes federadas para el intercambio de datos en las que la confianza y el control sobre los propios datos son principios fundamentales. Permiten a las organizaciones compartir, intercambiar y colaborar en datos a escala al ofrecer una solución rentable e independiente de la tecnología.

Los espacios de datos tienen el potencial de impulsar significativamente los esfuerzos para un futuro sostenible mediante el uso de la resolución de problemas basada en datos con un end-to-end enfoque que involucre a todas las partes interesadas relevantes.

Este patrón lo guía a través del ejemplo de cómo dos empresas pueden utilizar la tecnología de espacio de datos en Amazon Web Services (AWS) para impulsar su estrategia de reducción de emisiones de carbono. En este escenario, la empresa X proporciona datos sobre las emisiones de carbono, que la empresa Y consume. Consulte la sección de información adicional para obtener los siguientes detalles de las especificaciones del espacio de datos:

- Participantes
- Caso de negocio
- Autoridad del espacio de datos
- Componentes del espacio de datos
- Servicios de espacio de datos
- Datos que se van a intercambiar
- Modelo de datos
- Conector Tractus-X EDC

El patrón incluye los pasos siguientes:

- Implementar la infraestructura necesaria para un espacio de datos básico con dos participantes en ejecución AWS.
- Intercambiar datos sobre la intensidad de las emisiones de carbono mediante los conectores de forma segura.

Este patrón implementa un clúster de Kubernetes que alojará los conectores de espacios de datos y sus servicios a través de Amazon Elastic Kubernetes Service (Amazon EKS).

Tanto el plano de control como el plano de datos de Eclipse Dataspace Components (EDC) se implementan en Amazon EKS. El gráfico oficial de Tractus-X Helm despliega los servicios de PostgreSQL y Vault como dependencias. HashiCorp

Además, el servicio de identidad se implementa en Amazon Elastic Compute Cloud (Amazon EC2) para replicar un escenario real de un espacio de datos mínimo viable (MVDS).

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS para implementar la infraestructura que elijas Región de AWS
- Un usuario AWS Identity and Access Management (IAM) con acceso a Amazon S3 que se utilizará temporalmente como usuario técnico (el conector EDC actualmente no admite el uso de funciones). Le recomendamos que cree un usuario de IAM específico para esta demostración y que este usuario tenga permisos limitados asociados a él).

- AWS Command Line Interface (AWS CLI) instalado y configurado según su elección Región de AWS
- AWS credenciales de seguridad
- eksctl en su estación de trabajo
- Git en tu estación de trabajo
- kubectl
- Helm
- Cartero
- Un certificado AWS Certificate Manager SSL/TLS (ACM)
- Un nombre DNS que apuntará a un Application Load Balancer (el nombre DNS debe estar cubierto por el certificado ACM)
- HashiCorp Vault (para obtener información sobre AWS Secrets Manager cómo administrar secretos, consulte la sección Información adicional).

Versiones de producto

- AWS CLI versión 2+
- Colección Postman v2.1

Limitaciones

- Selección de conectores: esta implementación utiliza un conector basado en EDC. Sin embargo, asegúrese de tener en cuenta los puntos fuertes y las funcionalidades de los conectores EDC y FIWARE True para tomar una decisión informada que se ajuste a las necesidades específicas de la implementación.
- Construcción del conector EDC: la solución de despliegue elegida se basa en el diagrama Tractus-X EDC Connector Helm, una opción de despliegue bien establecida y ampliamente probada. La decisión de utilizar este gráfico se debe a su uso habitual y a la inclusión de las extensiones esenciales en la versión proporcionada. Si bien PostgreSQL HashiCorp y Vault son componentes predeterminados, tiene la flexibilidad de personalizar su propia compilación de conectores si es necesario.
- Acceso al clúster privado: el acceso al clúster de EKS implementado está restringido a los canales privados. La interacción con el clúster se realiza exclusivamente mediante el uso de

`kubectl` un IAM. El acceso público a los recursos del clúster se puede habilitar mediante el uso de balanceadores de carga y nombres de dominio, que deben implementarse de forma selectiva para exponer servicios específicos a una red más amplia. Sin embargo, no recomendamos proporcionar acceso público.

- Centrado en la seguridad: se hace hincapié en resumir las configuraciones de seguridad según las especificaciones predeterminadas, de modo que pueda concentrarse en los pasos necesarios para el intercambio de datos de los conectores EDC. Si bien se mantiene la configuración de seguridad predeterminada, es imprescindible habilitar las comunicaciones seguras antes de exponer el clúster a la red pública. Esta precaución garantiza una base sólida para el manejo seguro de los datos.
- Costo de infraestructura: se puede obtener una estimación del costo de la infraestructura utilizando el AWS Pricing Calculator. Un cálculo sencillo muestra que los costes pueden ascender a 162,92 USD al mes para la infraestructura implementada.

Arquitectura

La arquitectura MVDS consta de dos nubes privadas virtuales (VPC), una para el servicio de identidad del Sistema de aprovisionamiento dinámico de atributos (DAPS) y otra para Amazon EKS.

Arquitectura DAPS

El siguiente diagrama muestra la ejecución de DAPS en instancias EC2 controladas por un grupo de Auto Scaling. Un Application Load Balancer y una tabla de enrutamiento muestran los servidores DAPS. Amazon Elastic File System (Amazon EFS) sincroniza los datos entre las instancias de DAPS.

Arquitectura Amazon EKS

Los espacios de datos están diseñados para ser soluciones independientes de la tecnología y existen varias implementaciones. Este patrón utiliza un clúster de Amazon EKS para implementar los componentes técnicos del espacio de datos. El siguiente diagrama muestra la implementación del clúster EKS. Los nodos de trabajo se instalan en subredes privadas. Los pods de Kubernetes acceden a la instancia de Amazon Relational Database Service (Amazon RDS) para PostgreSQL que también se encuentra en las subredes privadas. Los pods de Kubernetes almacenan datos compartidos en Amazon S3.

Herramientas

AWS servicios

- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y administrarlos a lo largo de su ciclo de vida en todas Cuentas de AWS las regiones.
- Amazon Elastic Compute Cloud (Amazon EC2) brinda capacidad de computación escalable en la Nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon Elastic File System (Amazon EFS) lo ayuda a crear y configurar sistemas de archivos compartidos en la Nube de AWS.
- Amazon Elastic Kubernetes Service (Amazon EKS) le ayuda a ejecutar AWS Kubernetes sin necesidad de instalar o mantener su propio plano de control o nodos de Kubernetes.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Elastic Load Balancing (ELB) distribuye el tráfico entrante de aplicaciones o redes entre varios destinos. Así, por ejemplo, puede distribuir el tráfico entre instancias de EC2, contenedores y direcciones IP de una o varias zonas de disponibilidad.

Otras herramientas

- eksctl: es una utilidad sencilla de línea de comandos para crear y administrar clústeres de Kubernetes en Amazon EKS.
- Git es un sistema de control de versiones distribuido de código abierto.
- HashiCorp Vault proporciona un almacenamiento seguro con acceso controlado para las credenciales y otra información confidencial.
- Helm es un administrador de paquetes de código abierto para Kubernetes que le ayuda a instalar y administrar aplicaciones en su clúster de Kubernetes.
- kubectl: una interfaz de la línea de comandos que le ayuda en la ejecución de comandos en clústeres de Kubernetes.
- Postman es una plataforma de API.

Repositorio de código

Los archivos YAML de configuración de Kubernetes y los scripts de Python para este patrón están disponibles en el repositorio aws-patterns-edc. GitHub El patrón también usa el repositorio EDC de Tractus-X.

Prácticas recomendadas

Amazon EKS y el aislamiento de las infraestructuras de los participantes

Siguiendo este patrón, los espacios de nombres de Kubernetes separarán la infraestructura del proveedor X de la empresa de la infraestructura del consumidor de la empresa Y. Para obtener más información, consulte las guías de mejores prácticas de EKS.

En una situación más realista, cada participante tendría un clúster de Kubernetes independiente que se ejecutaría dentro del suyo. Cuenta de AWS Los participantes del espacio de datos podrían acceder a la infraestructura compartida (DAPS según este patrón) y, al mismo tiempo, estaría completamente separada de las infraestructuras de los participantes.

Epics

Configure el entorno y aprovisione un clúster EKS e instancias EC2

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Para clonar el repositorio en su estación de trabajo, ejecute el siguiente comando: `git clone https://github.com/Think-iT-Labs/aws-patterns-edc` La estación de trabajo debe tener acceso a su. Cuenta de AWS	DevOps ingeniero
Aprovisione el clúster de Kubernetes y configure los espacios de nombres.	Para implementar un clúster EKS predeterminado simplificado en su cuenta, ejecute el siguiente `eksctl` comando	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	en la estación de trabajo en la que clonó el repositorio: `eksctl create cluster` El comando crea la VPC y las subredes públicas y privadas que abarcan tres zonas de disponibilidad diferentes. Una vez creada la capa de red, el comando crea dos instancias `m5.large` EC2 dentro de un grupo de Auto Scaling. Para obtener más informaci ón y ejemplos de resultados, consulte la guía eksctl. Tras aprovisionar el clúster privado, añade el nuevo clúster de EKS a tu configura ción local de Kubernete s ejecutando el siguiente comando: `aws eks update-ku beconfig --name <EKS CLUSTER NAME> --region <AWS REGION>` Este patrón utiliza el para ejecutar todos `eu-west-1` Región de AWS los comandos. Sin embargo, puede ejecutar los mismos	

Tarea	Descripción	Habilidades requeridas
	comandos en el modo que prefiera Región de AWS. Para confirmar que los nodos EKS se están ejecutando y están preparados, ejecute el siguiente comando: `kubectl get nodes`	
Configure los espacios de nombres.	Para crear espacios de nombres para el proveedor y el consumidor, ejecute los siguientes comandos: `kubectl create ns provider` `kubectl create ns consumer` En este patrón, es importante utilizar `provider` y `consumer` como espacios de nombres para adaptarlos a las configuraciones en los siguientes pasos.	DevOps ingeniero

Implemente el servicio de identidad

Tarea	Descripción	Habilidades requeridas
Implemente DAPS mediante AWS CloudFormation.	Para facilitar la administración de las operaciones de DAPS, el servidor DAPS se instala en las instancias EC2.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Para instalar DAPS, utilice la plantilla.AWS CloudFormation Necesitará el certificado ACM y el nombre DNS de la sección de requisitos previos. La plantilla implementa y configura lo siguiente: • Equilibrador de carga de aplicación • Grupo de escalado automático • Instancias EC2 configuradas con datos de usuario para instalar todos los paquetes necesarios • Roles de IAM • DAPS Puede implementar la AWS CloudFormation plantilla iniciando sesión en la AWS CloudFormation consola AWS Management Console y utilizándola. También puede implementar la plantilla mediante un AWS CLI comando como el siguiente: `aws cloudformation create-stack --stack-name daps \ --template-body file://aws-patterns-`	

Tarea	Descripción	Habilidades requeridas
	edc/cloudformation.yml --parameters \ ParameterKey=CertificateARN,ParameterValue=<ACM Certificate ARN> \ ParameterKey=DNSName,ParameterValue=<DNS name> \ ParameterKey=InstanceType,ParameterValue=<EC2 instance type> \ ParameterKey=EnvironmentName,ParameterValue=<Environment Name> --capabilities CAPABILITY_NAMED_IAM El nombre del entorno es de su elección. Recomendamos utilizar un término significativo, por ejemplo `DapsInfrastructure`, porque se reflejará en las etiquetas de los AWS recursos. Para este patrón, `t3.small` es lo suficientemente grande como para ejecutar el flujo de trabajo de DAPS, que tiene tres contenedores Docker. La plantilla despliega las instancias de EC2 en subredes privadas. Esto significa que no se puede	

Tarea	Descripción	Habilidades requeridas
	acceder directamente a las instancias a través de SSH (Secure Shell) desde Internet. Las instancias cuentan con la función de IAM y el AWS Systems Manager agente necesarios para permitir el acceso a las instancias en ejecución a través del Administrador de sesiones, una capacidad de. AWS Systems Manager Se recomienda utilizar el administrador de sesiones para acceder. Como alternati va, puede aprovisionar un host bastión para permitir el acceso SSH desde Internet. Si se utiliza el enfoque de host bastión, es posible que la instancia de EC2 tarde unos minutos más en empezar a ejecutarse. Una vez que la AWS CloudFormation plantilla se haya implementado correctam ente, apunte el nombre DNS al nombre DNS de Applicati on Load Balancer. Para confirmar, ejecute el siguiente comando: `dig <DNS NAME>`	

Tarea	Descripción	Habilidades requeridas
	El resultado debería ser similar al siguiente: `; <<>> DiG 9.16.1-Ubuntu <<>> edc-pattern.think-it.io` `;; global options: +cmd` `;; Got answer:` `;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42344` `;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1` `;; OPT PSEUDOSECTION:` `; EDNS: version: 0, flags:; udp: 65494` `;; QUESTION SECTION:` `;edc-pattern.think-it.io. IN A` `;; ANSWER SECTION:` `edc-pattern.think-it.io. 276 IN CNAME daps-alb-iap9zmwy3kn8-1328773120.eu-west-1.elb.amazonaws.com.` `daps-alb-iap9zmwy3kn8-1328773120.eu-west-1.elb.amazonaws.com. 36 IN A 52.208.240.129` `daps-alb-iap9zmwy3kn8-1328773120.eu-west-1.elb.amazonaws.`	

Tarea	Descripción	Habilidades requeridas
	`com. 36 IN A 52.210.155.124`	

Tarea	Descripción	Habilidades requeridas
Registre los conectores de los participantes en el servicio DAPS.	Desde cualquiera de las instancias EC2 aprovisionadas para DAPS, registre a los participantes: 1. Ejecute el script disponibl e en la instancia EC2 mediante el usuario root: `cd /srv/mvds/omejdn-d aps` 2. Registre el proveedor: `bash scripts/r egister_connector. sh <provider_name>` 3. Registre al consumidor: `bash scripts/r egister_connector. sh <consumer_name>` La elección de los nombres no afecta a los próximos pasos. Se recomienda usar `consumer` o `provider` `companyx` `ycompanyy`. Los comandos de registro también configurarán automáticamente el servicio DAPS con la información necesaria obtenida de los certificados y claves creados.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Mientras esté conectado a un servidor DAPS, recopile la información necesaria para los pasos posteriores de la instalación: 1. Desde `omejdn-daps/config/clients.yml` obtener el `client id` para el proveedor y el consumidor. Los `client id` valores son cadenas largas de dígitos hexadecimales. 2. Desde el `omejdn-daps/keys` directorio, copie el contenido de los `provider.key` archivos `consumer.cert` `consumer.key` `provider.cert` ,, y. Se recomienda copiar y pegar el texto en archivos con nombres similares y con el prefijo «» `daps-` en la estación de trabajo. Debe tener los ID de cliente del proveedor y del consumidor y cuatro archivos en el directorio de trabajo de la estación de trabajo: • El nombre del archivo fuente `consumer.cert`	

Tarea	Descripción	Habilidades requeridas
	pasa a ser el nombre del archivo de la estación de trabajo. `daps-consumer.cert` • El nombre del archivo fuente `consumer.key` pasa a ser el nombre del archivo de la estación de trabajo. `daps-consumer.key` • El nombre del archivo fuente `provider.cert` pasa a ser el nombre del archivo de la estación de trabajo. `daps-provider.cert` • El nombre del archivo fuente `provider.key` pasa a ser el nombre del archivo de la estación de trabajo. `daps-provider.key`	

Despliegue los conectores de los participantes

Tarea	Descripción	Habilidades requeridas
Clona el repositorio EDC de Tractus-X y usa la versión 0.4.1.	La compilación del conector EDC de Tractus-X requiere la implementación y disponibilidad de los servicios PostgreSQL (base de datos de activos) y HashiCorp Vault (administración de secretos).	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Existen muchas versiones diferentes de los gráficos EDC Helm de Tractus-X. Este patrón especifica la versión 0.4.1 porque utiliza el servidor DAPS. Las versiones más recientes utilizan Managed Identity Wallet (MIW) con una implementación distribuida del servicio de identidad. En la estación de trabajo en la que creó los dos espacios de nombres de Kubernetes, clone el repositorio tractusx-edc y compruebe la sucursal. `release/0.4.1` `git clone https://github.com/eclipse-tractusx/tractusx-edc` `cd tractusx-edc` `git checkout release/0.4.1`	

Tarea	Descripción	Habilidades requeridas
Configure el gráfico Tractus-X EDC Helm.	Modifique la configuración de la plantilla del gráfico Tractus-X Helm para permitir que ambos conectores interactúen entre sí. Para ello, debe añadir el espacio de nombres al nombre DNS del servicio para que otros servicios del clúster puedan resolverlo. Estas modificaciones deben realizarse en el `charts/tractusx-connector/templates/_helpers.tpl` archivo. Este patrón proporciona una versión final modificada de este archivo para su uso. Cópielo y colóquelo en la `daps` sección del archivo`charts/tractusx-connector/templates/_helpers.tpl` . Asegúrese de comentar todas las dependencias del DAPS en: `charts/tractusx-connector/Chart.yaml` `dependencies:` `  # IDS Dynamic Attribute Provisioning Service (IAM)` `  #  - name: daps` `  # version: 0.0.1`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	<pre> # repository: "file://./subcharts/ omejdn" # alias: daps # condition: install.daps</pre>	

Tarea	Descripción	Habilidades requeridas
Configure los conectores para usar PostgreSQL en Amazon RDS.	(Opcional) La instancia de Amazon Relational Database Service (Amazon RDS) no es necesaria en este patrón. Sin embargo, recomendamos encarecidamente utilizar Amazon RDS o Amazon Aurora, ya que ofrecen funciones como alta disponibilidad y backup y recuperación. Para reemplazar PostgreSQL en Kubernetes por Amazon RDS, haga lo siguiente: 1. Aprovisione la instancia de Amazon RDS for PostgreSQL. 2. En `Chart.yaml` , comente la sección. `PostgreSQL` 3. En `provider_values.yml` y `consumer_values.yml` , configure la `postgresql` sección de la siguiente manera: `postgresql:` `  auth:` `  database: edc` `  password: <RDS PASSWORD>` `  username: <RDS Username>`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	<pre> jdbcUrl: jdbc:post gresql://<RDS DNS NAME>:5432/edc username: <RDS Username> password: <RDS PASSWORD> primary: persistence: enabled: false readReplicas: persistence: enabled: false</pre>	

Tarea	Descripción	Habilidades requeridas
Configure e implemente el conector del proveedor y sus servicios.	Para configurar el conector del proveedor y sus servicios, haga lo siguiente: 1. Para descargar el `provider_edc.yaml` archivo del `edc_helm_configs` directorio a la carpeta de gráficos de Helm actual, ejecute el siguiente comando: `wget -q https://raw.githubusercontent.com/Think-iT-Labs/aws-patterns-edc/main/edc_helm_configs/provider_edc.yaml> -P charts/tractusx-connector/` 2. Sustituya las siguientes variables (también marcadas en el archivo) por sus valores: • `CLIENT_ID` – El ID generado por el DAPS. `CLIENT_ID` Debe estar `/srv/mvds/omejdn-daps/config/clients.yml/config/clients.yml` en el servidor DAPS. Debe ser una cadena de caracteres hexadecimales.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	• `DAPS_URL`– La URL del servidor DAPS. Debe `https://{DNS name}` usar el nombre DNS que configuró cuando ejecutó la AWS CloudFormation plantilla. • `VAULT_TOKEN` – El token que se utilizará para la autorización de Vault. Elige cualquier valor. • `vault.fullnameOverride` – `vault-provider` . • `vault.hashicorp.url` – `http://vault-provider:8200/` . Los valores anteriores asumen que el nombre de la implementación y el nombre del espacio de nombres son proveedores. 3. Para ejecutar el diagrama de Helm desde su estación de trabajo, utilice los siguientes comandos: `cd charts/tractusx-connector` `helm dependency build`	

Tarea	Descripción	Habilidades requeridas
	`helm upgrade -- install provider ./ -f provider_edc.yaml -n provider`	

Tarea	Descripción	Habilidades requeridas
Añada el certificado y las claves a la bóveda del proveedor.	Para evitar confusiones, genere los siguientes certificados fuera del `tractusx-edc/charts` directorio. Por ejemplo, ejecute el siguiente comando para cambiar a su directorio principal: `cd ~` Ahora tiene que añadir al almacén los secretos que necesita el proveedor. Los nombres de los secretos del almacén son los valores de las claves de la `secretNames:` sección del `provider_edc.yml` archivo. De forma predeterminada, se configuran de la siguiente manera: `secretNames:` `transferProxyTokenSignerPrivateKey: transfer-proxy-token-signer-private-key` `transferProxyTokenSignerPublicKey: transfer-proxy-token-signer-public-key`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	<pre>transferP roxyTokenEncryptio nAesKey: transfer- proxy-token-encryp tion-aes-key dapsPriva teKey: daps-private- key dapsPubli cKey: daps-public-key</pre> Inicialmente se generan una clave de estándar de cifrado avanzado (AES), una clave privada, una clave pública y un certificado autofirmado. Posteriormente, se añaden como secretos a la bóveda. Además, este directorio debe contener los `daps-provider.key` archivos `daps-provider.cert` y archivos que copió del servidor DAPS. 1. Ejecute los comandos siguientes: <pre># generate a private key openssl ecparam -name prime256v1 -genkey -noout -out provider- private-key.pem # generate correspon ding public key openssl ec -in provider-private-k</pre>	

Tarea	Descripción	Habilidades requeridas
	ey.pem -pubout -out provider-public-key.pem # create a self-signed certificate openssl req -new -x509 -key provider-private-key.pem -out provider-cert.pem -days 360 # generate aes key openssl rand -base64 32 > provider-aes.key 2. Antes de añadir los secretos al almacén, conviértalos de líneas múltiples en líneas simples sustituyendo los saltos de línea por: \n cat provider-private-key.pem | sed 's/$/\\\n/'\|tr -d '\\n' > provider-private-key.pem.line cat provider-public-key.pem \| sed 's/$/\\\n/'|tr -d '\\n' > provider-public-key.pem.line cat provider-cert.pem | sed 's/$/\\\\n/'\|tr -d '\\n' > provider-cert.pem.line cat provider-aes.key \| sed 's/$/\\\\n/'|tr -d '\\n' >	

Tarea	Descripción	Habilidades requeridas
	provider-aes.key.l ine ## The following block is for daps certifica te and key openssl x509 -in daps-provider.cert - outform PEM | sed 's/ $/\\\\n/'\|tr -d '\\n' > daps-provider.cert .line cat daps-provider.key \| sed 's/$/\\\\n/'| tr -d '\\n' > daps- provider.key.line 3. Para formatear los secretos que se añadirán a Vault, ejecuta los siguientes comandos: JSONFORMAT='{"cont ent": "%s"}' #create a single line in JSON format printf "${JSONFO RMAT}\\n" "`cat  provider-private- key.pem.line`" > provider-private-k ey.json printf "${JSONFO RMAT}\\n" "`cat  provider-public- key.pem.line`" > provider-public-ke y.json printf "${JSONFO RMAT}\\n" "`cat provider-cert.pem.	

Tarea	Descripción	Habilidades requeridas
	`line`" > provider-cert.json` `printf "${JSONFORMAT}\\n" "`cat provider-aes.key.line`" > provider-aes.json`  `printf "${JSONFORMAT}\\n" "`cat daps-provider.key.line`" > daps-provider.key.json` `printf "${JSONFORMAT}\\n" "`cat daps-provider.cert.line`" > daps-provider.cert.json`  Los secretos están ahora en formato JSON y están listos para añadirse al almacén. 4. Para obtener el nombre del pod del almacén, ejecute el siguiente comando: `kubectl get pods -n provider|egrep "vault|NAME"`  El nombre del pod será similar a`"vault-provider-0"` . Este nombre se utiliza al crear un puerto de reenvío al almacén. El reenvío de puertos permite acceder	

Tarea	Descripción	Habilidades requeridas
	a la bóveda para añadir el secreto. Debe ejecutarlo desde una estación de trabajo que tenga configuradas las credenciales de AWS. 5. Para acceder al almacén, utilice esta opción `kubectl` para configurar un reenvío de puertos: `kubectl port-forward <VAULT_POD_NAME> 8200:8200 -n provider` Ahora debería poder acceder al almacén a través de su navegador o la CLI. Navegador 1. Con el navegador, vaya a http://127.0.0.1:8200, donde se utilizará el puerto de reenvío que configuró. 2. Inicie sesión con el token que configuró anteriorm enteprovider_edc.yml . En el motor de secretos, crea tres secretos. Cada secreto tendrá un `Path for this secret` valor, que es el nombre del secreto que se muestra en la siguiente lista. Dentro de	

Tarea	Descripción	Habilidades requeridas
	la `secret data` sección, el nombre de la clave será `content` y el valor será la única línea de texto del archivo respectivo nombrado `.line`. 3. Los nombres secretos provienen de la `secretNames` sección del `provider_edc.yml` archivo. 4. Cree los siguientes secretos: • Secreto `transfer-proxy-token-signer-private-key` con nombre de archivo `provider-private-key.pem.line` • Secreto `transfer-proxy-token-signer-public-key` con nombre de archivo `provider-cert.pem.line` • Secreto `transfer-proxy-token-encryption-aes-key` con nombre de archivo `provider-aes.key.line`	

Tarea	Descripción	Habilidades requeridas
	• Secreto `daps-private-key` con nombre de archivo `daps-provider.key.line` • Secreto `daps-public-key` con nombre de archivo `daps-provider.cert.line` CLI de Vault La CLI también utilizará el reenvío de puertos que configuró. 1. En su estación de trabajo, instale la CLI de Vault siguiendo las instrucciones de la documentación de HashiCorp Vault. 2. Para iniciar sesión en el almacén con el token que configuró `provider_edc.yml` , ejecute el siguiente comando: `vault login -address=http://127.0.0.1:8200` Con el token correcto, deberías ver el mensaje `"Success! You are now authenticated."`	

Tarea	Descripción	Habilidades requeridas
	3. Para crear los secretos mediante los archivos con formato JSON que creó anteriormente, ejecute el código siguiente: `vault kv put -address=http://127.0.0.1:8200 secret/transfer-proxy-token-signer-private-key @provider-private-key.json` `vault kv put -address=http://127.0.0.1:8200 secret/transfer-proxy-token-signer-public-key @provider-cert.json` `vault kv put -address=http://127.0.0.1:8200 secret/transfer-proxy-token-encryption-aes-key @provider-aes.json` `vault kv put -address=http://127.0.0.1:8200 secret/daps-private-key @daps-provider.key.json` `vault kv put -address=http://127.0.0.1:8200 secret/daps-public-key @daps-provider.cert.json`	

Tarea	Descripción	Habilidades requeridas
Configure e implemente el conector de consumo y sus servicios.	Los pasos para configurar e implementar el consumidor son similares a los que se realizaron para el proveedor: 1. Para copiarlo `consumer_edc.yaml` del repositorio aws-patterns-edc a la carpeta `tractusx-edc/charts/tractusx-connector`, ejecute los siguientes comandos: `cd tractusx-edc` `wget -q https://raw.githubusercontent.com/Think-iT-Labs/aws-patterns-edc/main/edc_helm_configs/consumer_edc.yaml -P charts/tractusx-connector/` 2. Actualice las siguientes variables con sus valores reales: • `CONSUMER_CLIENT_ID` – El ID generado por DAPS. `CONSUMER_CLIENT_ID` Debe estar `config/clients.yml` en el servidor DAPS. • `DAPS_URL`– La misma URL de DAPS que utilizó para el proveedor.	

Tarea	Descripción	Habilidades requeridas
	• `VAULT_TOKEN` – El token que se utilizará para la autorización de Vault. Elige cualquier valor. • `vault.fullnameOverride` – `vault-consumer` • `vault.hashicorp.url` – `http://vault-provider:8200/` Los valores anteriores asumen que el nombre de la implementación y el nombre del espacio de nombres son. `consumer` 3. Para ejecutar el gráfico de Helm, usa los siguientes comandos: `cd charts/tractusx-connector` `helm upgrade --install consumer ./ -f consumer_edc.yaml -n consumer`	

Tarea	Descripción	Habilidades requeridas
Añada el certificado y las claves a la bóveda del consumidor.	Desde el punto de vista de la seguridad, recomendamos volver a generar los certifica dos y las claves de cada participante del espacio de datos. Este patrón regenera los certificados y las claves para el consumidor. Los pasos son muy similares a los del proveedor. Puede comprobar los nombres secretos del `consumer_ edc.yml` archivo. Los nombres de los secretos del almacén son los valores de las claves de la `secretNames:` sección`consumer_edc.yml file`. De forma predeterm inada, se configuran de la siguiente manera: `secretNames: transferP roxyTokenSignerPri vateKey: transfer- proxy-token-signer- private-key transferP roxyTokenSignerPub licKey: transfer- proxy-token-signer- public-key transferP roxyTokenEncryptio`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	<pre>nAesKey: transfer-proxy-token-encryption-aes-key dapsPrivateKey: daps-private-key dapsPublicKey: daps-public-key</pre> Los `daps-consumer.key` archivos `daps-consumer.cert` y que copió del servidor DAPS ya deberían existir en este directorio. 1. Ejecute los comandos siguientes: <pre># generate a private key openssl ecparam -name prime256v1 -genkey -noout -out consumer-private-key.pem # generate corresponding public key openssl ec -in consumer-private-key.pem -pubout -out consumer-public-key.pem # create a self-signed certificate openssl req -new -x509 -key consumer-private-key.pem -out consumer-cert.pem -days 360 # generate aes key</pre>	

Tarea	Descripción	Habilidades requeridas
	`openssl rand -base64 32 > consumer-aes.key` 2. Edite manualmente los archivos para sustituir los saltos de \n línea por ellos o utilice tres comandos similares a los siguientes: `cat consumer-private-key.pem | sed 's/$/\\\n/'\|tr -d '\\n' > consumer-private-key.pem.line` `cat consumer-public-key.pem \| sed 's/$/\\\n/'|tr -d '\\n' > consumer-public-key.pem.line` `cat consumer-cert.pem | sed 's/$/\\\\n/'\|tr -d '\\n' > consumer-cert.pem.line` `cat consumer-aes.key \| sed 's/$/\\\\n/'|tr -d '\\n' > consumer-aes.key.line` `cat daps-consumer.cert | sed 's/$/\\\\n/'\|tr -d '\\n' > daps-consumer.cert.line` `cat daps-consumer.key \| sed 's/$/\\\\n/'| tr -d '\\n' > daps-consumer.key.line`	

Tarea	Descripción	Habilidades requeridas
	3. Para formatear los secretos que se añadirán a Vault, ejecuta los siguientes comandos: `JSONFORMAT='{"content": "%s"}'` `#create a single line in JSON format` `printf "${JSONFORMAT}\\n" "`cat consumer-private-key.pem.line`" > consumer-private-key.json` `printf "${JSONFORMAT}\\n" "`cat consumer-public-key.pem.line`" > consumer-public-key.json` `printf "${JSONFORMAT}\\n" "`cat consumer-cert.pem.line`" > consumer-cert.json` `printf "${JSONFORMAT}\\n" "`cat consumer-aes.key.line`" > consumer-aes.json` `printf "${JSONFORMAT}\\n" "`cat daps-consumer.key.line`" > daps-consumer.key.json` `printf "${JSONFORMAT}\\n" "`cat daps-`	

Tarea	Descripción	Habilidades requeridas
	`consumer.cert.line`" > daps-consumer.cert.json`  Los secretos están ahora en formato JSON y están listos para añadirse al almacén. 4. Para obtener el nombre del pod de la bóveda del consumidor, ejecuta el siguiente comando:  `kubectl get pods -n consumer | egrep "vault|NAME"`  El nombre del pod será similar a `"vault-consumer-0"` . Este nombre se utiliza al crear un puerto de reenvío al almacén. El reenvío de puertos permite acceder a la bóveda para añadir el secreto. Debe ejecutarlo desde una estación de trabajo que tenga configuradas AWS las credenciales. 5. Para acceder al almacén, utilice `kubectl` para configurar un reenvío de puertos:	

Tarea	Descripción	Habilidades requeridas
	`kubectl port-forward <VAULT_POD_NAME> 8201:8200 -n consumer` Esta vez, el puerto local es el 8201, por lo que puede disponer de reenvíos de puertos tanto para el productor como para el consumidor. Navegador Puedes usar tu navegador para conectarte a http://localhost:8201/ para acceder a la bóveda del consumidor y crear los secretos con los nombres y el contenido tal y como se describe. Los secretos y archivos que contienen el contenido son los siguientes: • Secreto `transfer-proxy-token-signer-private-key` con nombre de archivo `consumer-private-key.pem.line` • Secreto `transfer-proxy-token-signer-public-key` con nombre de archivo	

Tarea	Descripción	Habilidades requeridas
	`consumer-cert.pem.line` • Secreto `transfer-proxy-token-encryption-aes-key` con nombre de archivo `consumer-aes.key.line` CLI de Vault Con la CLI de Vault, puede ejecutar los siguientes comandos para iniciar sesión en el almacén y crear los secretos: 1. Inicie sesión en el almacén con el token que configuró `consumer_edc.yml` : `vault login -address=http://127.0.0.1:8201` Con el token correcto, deberías ver el mensaje `"Success! You are now authenticated."` 2. Para crear los secretos con los archivos con formato JSON que creó anteriormente, ejecute el siguiente código:	

Tarea	Descripción	Habilidades requeridas
	`vault kv put -address= http://127.0.0.1:8 201 secret/transfer- proxy-token-signer-p rivate-key @consumer -private-key.json` `vault kv put - address=http://12 7.0.0.1:8201 secret/ transfer-proxy-token -signer-public-key @consumer-cert.json` `vault kv put -address= http://127.0.0.1:8 201 secret/transfer- proxy-token-encrypti on-aes-key @consumer -aes.json` `vault kv put -address= http://127.0.0.1:8 201 secret/daps- private-key @daps-con sumer.key.json` `vault kv put - address=http://12 7.0.0.1:8201 secret/ daps-public-key @daps-consumer.cer t.json`	

Configure un cliente HTTP para interactuar con la API de administración de los conectores

Tarea	Descripción	Habilidades requeridas
Configure el reenvío de puertos.	1. Para comprobar el estado de los pods, ejecuta los siguientes comandos:	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`kubectl get pods -n provider` `kubectl get pods -n consumer` 2. Para asegurarte de que las implementaciones de Kubernetes se realizaron correctamente, consulta los registros de los pods de Kubernetes proveedores y consumidores ejecutando los siguientes comandos: `kubectl logs -n provider <producer control plane pod name>` `kubectl logs -n consumer <consumer control plane pod name>` El clúster es privado y no se puede acceder a él públicamente. Para interactuar con los conectores, utilice la función de reenvío de puertos de Kubernetes para reenviar el tráfico generado por su máquina al plano de control del conector. 1. En el primer terminal, reenvíe las solicitudes del consumidor a la API de	

Tarea	Descripción	Habilidades requeridas
	administración a través del puerto 8300: `kubectl port-forward deployment/consumer-tractusx-connector-controlplane 8300:8081 -n consumer` 2. En el segundo terminal, reenvía las solicitudes del proveedor a la API de administración a través del puerto 8400: `kubectl port-forward deployment/provider-tractusx-connector-controlplane 8400:8081 -n provider`	

Tarea	Descripción	Habilidades requeridas
Cree depósitos S3 para el proveedor y el consumidor.	Actualmente, el conector EDC no utiliza credenciales de AWS temporales, como las que se proporcionan al asumir un rol. El EDC solo admite el uso de una combinación de ID de clave de acceso de IAM y clave de acceso secreta. Se necesitan dos cubos S3 para los pasos posteriores. Se utiliza un depósito de S3 para almacenar los datos puestos a disposición por el proveedor . El otro depósito de S3 es para los datos que recibe el consumidor. El usuario de IAM debe tener permiso para leer y escribir objetos únicamente en los dos cubos con nombre. Es necesario crear y mantener a salvo un identificador de clave de acceso y un par de claves de acceso secretas. Una vez que se haya dado de baja este MVDS, se debe eliminar el usuario de IAM. El siguiente código es un ejemplo de política de IAM para el usuario: `{`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	"Version": "2012-10-17", "Statement": [{ "Sid": "Stmt1708699805237", "Action": ["s3:GetObject", "s3:GetObjectVersion", "s3:ListAllMyBuckets", "s3:ListBucket", "s3:ListBucketMultipartUploads", "s3:ListBucketVersions", "s3:PutObject"], "Effect": "Allow", "Resource": ["arn:aws:s3:::<S3 Provider Bucket>", "arn:aws:s3:::<S3 Consumer Bucket>", "arn:aws:s3:::<S3 Provider Bucket>/*", "arn:aws:s3:::<S3 Consumer Bucket>/*"] }] }	

Tarea	Descripción	Habilidades requeridas
Configure Postman para que interactúe con el conector.	Ahora puede interactuar con los conectores a través de su instancia EC2. Utilice Postman como cliente HTTP y proporcione colecciones de Postman para los conectores del proveedor y del consumidor. Importa las colecciones del `aws-pattern-edc` repositorio a tu instancia de Postman. Este patrón usa variables de colección de Postman para proporcionar información a tus solicitudes.	Desarrollador de aplicaciones, ingeniero de datos

Proporcione los datos de la huella de carbono de la empresa X a través del conector

Tarea	Descripción	Habilidades requeridas
Prepare los datos sobre la intensidad de las emisiones de carbono para compartirlos.	En primer lugar, debe decidir el activo de datos que se va a compartir. Los datos de la empresa X representan la huella de emisiones de carbono de su flota de vehículos. El peso es el peso bruto del vehículo (GVW) en toneladas y las emisiones se expresan en gramos de CO2 por tonelada-kilómetro (g de CO2 e/t-km) según la	Desarrollador de aplicaciones, ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	medición de la rueda al pozo (WTW): • Tipo de vehículo: furgoneta; peso: < 3,5; emisiones: 800 • Tipo de vehículo: camión urbano; peso: 3,5–7,5; emisiones: 315 • Tipo de vehículo: vehículo de transporte de mercancías de tamaño medio (MGV); peso: 7,5–20; emisiones: 195 • Tipo de vehículo: vehículo pesado de transporte de mercancías (HGV); peso: > 20; emisiones: 115 Los datos de ejemplo se encuentran en el `carbon_emissions_data.json` archivo del `aws-patterns-edc` repositorio. La empresa X utiliza Amazon S3 para almacenar objetos. Cree el bucket de S3 y almacene allí el objeto de datos de ejemplo. Los siguientes comandos crean un depósito de S3 con la configuración de seguridad predeterminada. Recomendamos encarecidamente	

Tarea	Descripción	Habilidades requeridas
	consultar las prácticas recomendadas de seguridad para Amazon S3. `aws s3api create-bucket <BUCKET_NAME> --region <AWS_REGION>` `# You need to add '--create-bucket-configuration` `# LocationConstraint=<AWS_REGION>' if you want to create # the bucket outside of us-east-1 region` `aws s3api put-object --bucket <BUCKET_NAME> \` `--key <S3 OBJECT NAME> \` `--body <PATH OF THE FILE TO UPLOAD>` El nombre del bucket de S3 debe ser único a nivel mundial. Para obtener más información sobre las reglas de nomenclatura, consulte la documentación de AWS.	

Tarea	Descripción	Habilidades requeridas
Registre el activo de datos en el conector del proveedor mediante Postman.	Un activo de datos de un conector EDC contiene el nombre de los datos y su ubicación. En este caso, el activo de datos del conector EDC apuntará al objeto creado en el depósito S3: • Conector: proveedor • Solicitud: Crear activo • Variables de recopilación: actualizaciónASSET_NAME . Elija un nombre significativo que represente el activo. • Cuerpo de la solicitud: actualice el cuerpo de la solicitud con el depósito de S3 que creó para el proveedor. `"dataAddress": { "edc:type": "AmazonS3", "name": "Vehicle Carbon Footprint", "bucketName": "<REPLACE WITH THE SOURCE BUCKET NAME>", "keyName": "<REPLACE WITH YOUR OBJECT NAME>", "region": "<REPLACE WITH THE BUCKET REGION>", "accessKeyId": "<REPLACE WITH YOUR ACCESS KEY ID>",`	Desarrollador de aplicaciones, ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	<pre>"secretAc cessKey": "<REPLACE WITH SECRET ACCESS KEY>" }</pre> • Respuesta: una solicitud correcta devuelve la hora de creación y el ID del activo recién creado. <pre>{ "@id": "c89aa31c- ec4c-44ed-9e8c-16 47f19d7583" }</pre> • Variable de colección ASSET_ID: actualice la variable de colección Postman `ASSET_ID` con el identificador que generó automáticamente el conector EDC tras su creación.	

Tarea	Descripción	Habilidades requeridas
Defina la política de uso del activo.	Un activo de datos de la EDC debe estar asociado a políticas de uso claras. En primer lugar, cree la definició n de política en el conector del proveedor. La política de la empresa X es permitir que los participa ntes del espacio de datos utilicen los datos de la huella de emisiones de carbono. • Órgano de la solicitud: • Conector: proveedor • Solicitud: crear una política • Variables de recopilac ión: actualice la `Policy Name` variable con el nombre de la política. • Respuesta: una solicitud correcta devuelve la hora de creación y el identificador de política de la política recién creada. Actualice la variable de recopilación `POLICY_ID` con el ID de la política generada por el conector EDC tras su creación.	Desarrollador de aplicaciones, ingeniero de datos

Tarea	Descripción	Habilidades requeridas
Defina una oferta de contrato de EDC para el activo y su política de uso.	Para permitir que otros participantes soliciten acceso a sus datos, ofrézcalos en un contrato que especifique las condiciones de uso y los permisos: • Conector: proveedor • Solicitud: crear una definició n de contrato • Variables de recopilación: actualice la `Contract Name` variable con un nombre para la oferta o definición del contrato.	Desarrollador de aplicaciones, ingeniero de datos

Descubra los activos y llegue a un acuerdo sobre los contratos definidos

Tarea	Descripción	Habilidades requeridas
Solicite el catálogo de datos que comparte la empresa X.	Como consumidora de datos en el espacio de datos, la empresa Y primero debe descubrir los datos que comparten otros participantes. En esta configuración básica, puede hacerlo pidiéndol e al conector consumidor que solicite directamente al conector proveedor el catálogo de activos disponibl es.	Desarrollador de aplicaciones, ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	• Conector: consumidor • Solicitud: Solicite un catálogo • Respuesta: Todos los activos de datos disponibles del proveedor junto con sus políticas de uso adjuntas. Como consumidor de datos, busque el contrato que le interese y actualice las siguientes variables de recopilación en consecuencia. • `CONTRACT_OFFER_ID` – El identificador de la oferta contractual que el consumidor quiere negociar • `ASSET_ID`– El identificador del activo que el consumidor quiere negociar • `PROVIDER_CLIENT_ID` – El ID del conector del proveedor con el que se va a negociar	

Tarea	Descripción	Habilidades requeridas
Inicie una negociación contractual para obtener los datos de intensidad de emisiones de carbono de la empresa X.	Ahora que ha identificado el activo que quiere consumir, inicie un proceso de negociación del contrato entre el consumidor y el proveedor. • Conector: consumidor • Solicitud: Negociación de contrato • Variables de recopilación: actualice la `CONSUMER_CLIENT_ID` variable con el ID del conector de consumo con el que desee negociar. Es posible que el proceso tarde algún tiempo en alcanzar el estado VERIFICADO. Puede comprobar el estado de la negociación del contrato y el identificador del acuerdo correspondiente mediante la `Get Negotiation` solicitud.	Desarrollador de aplicaciones, ingeniero de datos

Consuma los datos utilizando el acuerdo de contrato

Tarea	Descripción	Habilidades requeridas
Consume datos de puntos finales HTTP.	(Opción 1) Para usar el plano de datos HTTP para consumir	Desarrollador de aplicaciones, ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	datos en el espacio de datos, puede usar webhook.site para emular un servidor HTTP e iniciar el proceso de transferencia en el conector de consumo: • Conector: Consumer • Solicitud: Negociación de contrato • Variables de recopilación: actualice la `Contract Agreement ID` variable con el ID del acuerdo de contrato generado por el conector EDC. • Cuerpo de la solicitud : actualice el cuerpo de la solicitud para `HTTP` especificarlo `dataDestination` junto a la URL del webhook: `{ "dataDestination": { "type": "HttpProxy" }, "privateProperties": { "receiverHttpEndpoint": "<WEBHOOK URL>" } }`	

Tarea	Descripción	Habilidades requeridas
	El conector enviará la información necesaria para descargar el archivo directamente a la URL del webhook. La carga útil recibida es similar a la siguiente: `{ "id": "dcc90391-3819-4b54-b401-1a005a029b78", "endpoint": "http://consumer-tractusx-connector-dataplane.consumer:8081/api/public", "authKey": "Authorization", "authCode": "<AUTH CODE YOU RECEIVE IN THE ENDPOINT>", "properties": { "https://w3id.org/edc/v0.0.1/ns/cid": "vehicle-carbon-footprint-contract:4563abf7-5dc7-4c28-bc3d-97f45e32edac:b073669b-db20-4c83-82df-46b583c4c062" } }` Utilice las credenciales recibidas para obtener el	

Tarea	Descripción	Habilidades requeridas
	activo de S3 que compartió el proveedor. En este último paso, debes enviar la solicitud al plano de datos del consumido r (reenviar los puertos correctamente), tal y como se indica en la carga útil (`endpoint`).	

Tarea	Descripción	Habilidades requeridas
Consume los datos de los depósitos de S3 directamente.	(Opción 2) Utilice la integración de Amazon S3 con el conector EDC y apunte directamente al depósito S3 de la infraestructura de consumo como destino: • Cuerpo de la solicitud: actualice el cuerpo de la solicitud para especificar el bucket de S3 como DataDestination. Debe ser el depósito de S3 que creó anteriormente para almacenar los datos recibidos por el consumidor. `{ "dataDestination": { "type": "AmazonS3", "bucketName": "{{ REPLACE WITH THE DESTINATION BUCKET NAME }}", "keyName": "{{ REPLACE WITH YOUR OBJECT NAME }}", "region": "{{ REPLACE WITH THE BUCKET REGION }}", "accessKeyId": "{{ REPLACE WITH YOUR ACCESS KEY ID }}", "secretAccessKey": "{{ REPLACE`	Desarrollador de aplicaciones, ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	<pre>WITH SECRET ACCESS KEY }}" } } }</pre>	

Resolución de problemas

Problema	Solución
El conector podría plantear un problema relacionado con el formato PEM del certificado.	Concatene el contenido de cada archivo en una sola línea agregando. \n

Recursos relacionados

- DSSC
- Creación de espacios de datos para casos de uso de sostenibilidad (estrategia AWS Prescriptive Guidance de Think-IT)
- AWS para espacios de datos
- Documentación de Tractus-X
- DAPS
- Permitir el intercambio de datos a través de espacios de datos y AWS (entrada del blog)

Información adicional

Especificaciones del espacio de datos

Participantes

Participante	Descripción de la empresa	Enfoque de la empresa
Empresa X	Opera una flota de vehículos en Europa y Sudamérica	Su objetivo es tomar decisione s basadas en datos para

	para transportar diversas mercancías.	reducir la intensidad de su huella de emisiones de carbono.
Empresa Y	Una autoridad reguladora ambiental	Hace cumplir las normas y políticas ambientales diseñadas para monitorear y mitigar el impacto ambiental de las empresas e industria s, incluida la intensidad de las emisiones de carbono.

Caso de negocio

La empresa X utiliza la tecnología del espacio de datos para compartir los datos sobre la huella de carbono con un auditor de cumplimiento, la empresa Y, a fin de evaluar y abordar el impacto ambiental de las operaciones logísticas de la empresa X.

Autoridad en materia de espacio de datos

La autoridad del espacio de datos es un consorcio de las organizaciones que gobiernan el espacio de datos. En este patrón, tanto la empresa X como la empresa Y forman el órgano de gobierno y representan una autoridad federada en materia de espacio de datos.

Componentes del espacio de datos

Componente	Implementación elegida	Información adicional
Protocolo de intercambio de conjuntos de datos	Protocolo Dataspace versión 0.8	• JSON-LD • Vocabulario del catálogo de datos (DCAT)
Conector de espacio de datos	Conector Tractus-X EDC versión 0.4.1	• Extensiones EDC
Políticas de intercambio de datos	Política de USO predeterm inada	• Lenguaje abierto de derechos digitales (ODRL)

Servicios de espacio de datos

Servicio	Implementación	Información adicional
Servicio de identidad	Sistema dinámico de aprovisionamiento de atributos (DAPS)	«Un sistema dinámico de aprovisionamiento de atributos (DAPS) tiene la intención de determinar ciertos atributos de las organizaciones y los conectores. Por lo tanto, los terceros no necesitan confiar en estos últimos siempre que confíen en las afirmaciones del DAPS». — DAPS Para centrarse en la lógica del conector, el espacio de datos se implementa en una máquina Amazon EC2 mediante Docker Compose.
Servicio de detección	Catálogo federado Gaia-X	«El Catálogo Federado constituye un repositorio indexado de las autodescripciones de Gaia-X que permite descubrir y seleccionar los proveedores y sus ofertas de servicios. Las autodescripciones son la información proporcionada por los participantes sobre sí mismos y sobre sus servicios en forma de propiedades y reclamaciones». — Kickstarter del ecosistema Gaia-X

Datos a intercambiar

Activos de datos	Descripción	Formato
Datos de emisiones de carbono	Valores de intensidad para diferentes tipos de vehículos en la región especificada (Europa y Sudamérica) de toda la flota de vehículos	Archivo JSON

Modelo de datos

```
{
  "region": "string",
  "vehicles": [
// Each vehicle type has its Gross Vehicle Weight (GVW) category and its emission
 intensity in grams of CO2 per Tonne-Kilometer (g CO2 e/t-km) according to the "Well-
to-Wheel" (WTW) measurement.
    {
      "type": "string",
      "gross_vehicle_weight": "string",
      "emission_intensity": {
        "CO2": "number",
        "unit": "string"
      }
    }
  ]
}
```

Conector Tractus-X EDC

Para obtener la documentación de cada parámetro EDC de Tractus-X, consulte el archivo de valores original.

La siguiente tabla muestra todos los servicios, junto con sus correspondientes puertos y puntos finales expuestos como referencia.

Nombre del servicio	Puerto y ruta
Plano de control	• administración: – Puerto: 8081 Ruta: `/management`

	• control – Puerto: 8083 Ruta: `/control` • Puerto de protocolo: 8084 Ruta: `/api/v1/dsp` • métricas – Puerto: 9090 Ruta: `/metrics` • observabilidad – Puerto: 8085 Ruta: `/observability`
Plano de datos	predeterminado – Puerto: 8080 Ruta: `/api` público – Puerto: 8081 Ruta: `/api/dataplane/control` proxy – Puerto: 8186 Ruta: `/proxy` métricas – Puerto: 9090 Ruta: `/metrics` observabilidad – Puerto: 8085 Ruta: `/observability`
Almacén	Puerto: 8200
PostgreSQL	Puerto: 5432

Uso AWS Secrets Manager del administrador

Es posible usar Secrets Manager en lugar de HashiCorp Vault como administrador de secretos. Para hacerlo, debe usar o compilar la extensión AWS Secrets Manager EDC.

Serás responsable de crear y mantener tu propia imagen, ya que Tractus-X no ofrece soporte para Secrets Manager.

Para ello, tendrás que modificar los archivos de compilación de Gradle tanto del plano de control como del plano de datos del conector introduciendo la extensión AWS Secrets Manager EDC (consulta este magnífico artefacto para ver un ejemplo) y, a continuación, crear, mantener y hacer referencia a la imagen de Docker.

Para obtener más información sobre la refactorización de la imagen Docker del conector Tractus-X, consulte los gráficos Refactorizar Tractus-X EDC Helm.

Por motivos de simplicidad, evitamos volver a crear la imagen del conector siguiendo este patrón y utilizamos Vault. HashiCorp

Configure la clasificación por idioma para los resultados de las consultas de Amazon Redshift mediante una UDF escalar de Python

Creado por Ethan Stark (AWS)

Entorno: producción	Tecnologías: análisis	Servicios de AWS: Amazon Redshift

Resumen

Este patrón proporciona los pasos y un código de ejemplo para usar una UDF (función definida por el usuario) de Python escalar para configurar una clasificación lingüística que no distinga entre mayúsculas y minúsculas para los resultados de las consultas de Amazon Redshift. Es necesario utilizar una UDF de Python escalar porque Amazon Redshift devuelve los resultados en función del orden binario de UTF-8 y no admite la clasificación por idiomas específicos. Una UDF de Python es un código de procesamiento que no es de SQL que se basa en un programa de Python 2.7 y se ejecuta en un almacenamiento de datos. Puede ejecutar código UDF de Python con una instrucción SQL en una sola consulta. Para obtener más información, consulte la entrada del blog de macrodatos de AWS Introducción a las UDF de Python en Amazon Redshift.

Los datos de muestra de este patrón se basan en el alfabeto turco con fines de demostración. La UDF escalar de Python de este patrón está diseñada para que los resultados de las consultas predeterminados de Amazon Redshift se ajusten al orden lingüístico de los caracteres del idioma turco. Para obtener más información, consulte Ejemplo de lengua turca en la sección Información adicional de este patrón. Puede modificar la UDF escalar de Python en este patrón para otros lenguajes.

Requisitos previos y limitaciones

Requisitos previos

- Clúster de Amazon Redshift con base de datos, esquema y tablas
- Usuario de Amazon Redshift con permisos CREATE TABLE y CREATE FUNCTION

- Python 2.7 o posterior

Limitaciones

La clasificación lingüística utilizada por las consultas en este patrón no distingue entre mayúsculas y minúsculas.

Arquitectura

Pila de tecnología

- Amazon Redshift
- UDF de Python

Herramientas

Servicios de AWS

- Amazon Redshift es un servicio de almacenamiento de datos administrado de varios petabytes en la nube de AWS. Amazon Redshift está integrado en el lago de datos, lo que permite usar los datos para adquirir nueva información para su empresa y sus clientes.

Otras herramientas

- Las funciones definidas por el usuario (UDF) de Python son funciones que puede escribir en Python y luego llamar a instrucciones SQL.

Epics

Desarrolle código para ordenar los resultados de las consultas en orden lingüístico

Tarea	Descripción	Habilidades requeridas
Cree una tabla para los datos de su muestra.	Para crear una tabla en Amazon Redshift e insertar los datos de muestra en la tabla,	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	utilice las siguientes instrucciones SQL: `CREATE TABLE my_table (first_name varchar(30));` `INSERT INTO my_table (first_name) VALUES ('ali'), ('Ali'), ('ırmak'), ('IRMAK'), ('irem'), ('İREM'), ('oğuz'), ('OĞUZ'), ('ömer'), ('ÖMER'), ('sedat'), ('SEDAT'), ('şule'),` Nota: Los primeros nombres de los datos de muestra incluyen caracteres especiales del alfabeto turco. Para obtener más información sobre las consideraciones relativas al idioma turco en este ejemplo, consulte Ejemplo de lengua turca en la sección Información adicional de este patrón.	

Tarea	Descripción	Habilidades requeridas
Compruebe la clasificación predeterminada de los datos de la muestra.	Para ver la clasificación predeterminada de los datos de muestra en Amazon Redshift, ejecute la siguiente consulta: `SELECT first_name FROM my_table ORDER BY first_name;` La consulta devuelve la lista de nombres de la tabla que creó anteriormente: `first_name` `---------------` `Ali` `IRMAK` `OĞUZ` `SEDAT` `ali` `irem` `oğuz` `sedat` `ÖMER` `ömer` `İREM` `ırmak` `ŞULE` `şule` Los resultados de la consulta no están en el orden correcto porque el orden binario predeterminado en UTF-8 no se adapta al orden lingüístico	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	de los caracteres especiales turcos.	

Tarea	Descripción	Habilidades requeridas
Creación de una UDF de Python escalar.	Para crear una UDF de Python escalar, utilice el siguiente código SQL: `CREATE OR REPLACE FUNCTION collate_sort (value varchar) RETURNS varchar IMMUTABLE AS $$ def sort_str(val): import string dictionary = { 'I': 'ı', 'ı': 'h~', 'İ': 'i', 'Ş': 's~', 'ş': 's~', 'Ğ': 'g~', 'ğ': 'g~', 'Ü': 'u~', 'ü': 'u~', 'Ö': 'o~', 'ö': 'o~', 'Ç': 'c~', 'ç': 'c~' } for key, value in dictionary.items(): val = val.replace(key, value) return val.lower()`	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	`    return sort_str(value)` `$$ LANGUAGE plpythonu;`	
Consulta del ejemplo de datos.	Para consultar del ejemplo de datos mediante la UDF de Python, ejecute la siguiente consulta SQL: `SELECT first_name FROM my_table ORDER BY collate_order(first_name);` La consulta ahora devuelve los datos de la muestra en orden lingüístico turco: `first_name` `---------------` `ali` `Ali` `ırmak` `IRMAK` `irem` `İREM` `oğuz` `OĞUZ` `ömer` `Ömer` `sedat` `SEDAT` `şule` `ŞULE`	Ingeniero de datos

Recursos relacionados

- Cláusula ORDER BY (documentación de Amazon Redshift)
- Creación de una UDF de Python escalar (documentación de Amazon Redshift)

Información adicional

Ejemplo de idioma turco

Amazon Redshift devuelve los resultados de las consultas en función de la ordenación binaria de UTF-8, no de una ordenación específica del idioma. Esto significa que si consulta una tabla de Amazon Redshift que contenga caracteres turcos, los resultados de la consulta no se ordenarán según el orden lingüístico del idioma turco. El idioma turco contiene seis caracteres especiales (ç, ı, ğ, ö, ş y ü) que no aparecen en el alfabeto latino. Estos caracteres especiales se colocan al final de un conjunto de resultados ordenados según el orden binario UTF-8, como se muestra en la siguiente tabla.

Orden binario en UTF-8	Ordenamiento lingüístico turco
a	a
b	b
c	c
d	ç (*)
e	d
f	e
g	f
h	g
i	ğ (*)
j	h
k	ı (*)

l	i
m	j
n	k
o	l
p	m
r	n
s	o
t	ö (*)
u	p
v	r
y	s
z	ş (*)
ç (*)	t
ğ (*)	u
ı (*)	ü (*)
ö (*)	v
ş (*)	y
ü (*)	z

Nota: El asterisco (*) indica un carácter especial en el idioma turco.

Como se muestra en la tabla anterior, el carácter especial ç se encuentra entre la c y la d en el orden lingüístico turco, pero aparece después de la z en el orden binario UTF-8. La UDF de Python escalar de este patrón utiliza el siguiente diccionario de reemplazo de caracteres para reemplazar los caracteres especiales turcos por los correspondientes caracteres equivalentes en latín.

Carácter especial turco	Carácter equivalente en latín
ç	c~
ı	h~
ğ	g~
ö	o~
ş	s~
ü	u~

Nota: Se añade un carácter de tilde (~) al final de los caracteres latinos que sustituyen a sus correspondientes caracteres especiales turcos.

Modificar una función UDF de Python escalar

Para modificar la función UDF de Python escalar a partir de este patrón para que la función acepte un parámetro de localización y admita un diccionario de transacciones múltiples, utilice el siguiente código SQL:

```
CREATE OR REPLACE FUNCTION collate_sort (value varchar, locale varchar)
RETURNS varchar
IMMUTABLE
AS
$$
    def sort_str(val):
       import string
       # Turkish Dictionary
       if locale == 'tr-TR':
            dictionary = {
               'I': 'ı',
               'ı': 'h~',
               'İ': 'i',
               'Ş': 's~',
               'ş': 's~',
               'Ğ': 'g~',
               'ğ': 'g~',
               'Ü': 'u~',
```

```
                'ü': 'u~',
                'Ö': 'o~',
                'ö': 'o~',
                'Ç': 'c~',
                'ç': 'c~'
        }
        # German Dictionary
        if locale == 'de-DE':
            dictionary = {
                ....
                ....
        }

        for key, value in dictionary.items():
            val = val.replace(key, value)

        return val.lower()

    return sort_str(value)

$$ LANGUAGE plpythonu;
```

En el siguiente ejemplo de código se muestra cómo se consulta del UDF de Python modificado:

```
SELECT first_name FROM my_table ORDER BY collate_order(first_name, 'tr-TR');
```

Suscripción de una función de Lambda a las notificaciones de eventos de buckets de S3 en diferentes regiones de AWS

Creado por Suresh Konathala (AWS) y Arindom Sarkar (AWS)

Entorno: producción	Tecnologías: Análisis	Servicios de AWS: AWS Lambda; Amazon S3; Amazon SNS; Amazon SQS

Resumen

Notificaciones de eventos de Amazon Simple Storage Service (Amazon S3) publica notificaciones de determinados eventos en su bucket de S3 (por ejemplo, eventos creados por objetos, eventos de eliminación de objetos o eventos de restauración de objetos). Puede usar una función de AWS Lambda para procesar estas notificaciones de acuerdo con los requisitos de su aplicación. Sin embargo, la función de Lambda no puede suscribirse directamente a las notificaciones de los buckets de S3 alojados en distintas regiones de AWS.

El enfoque de este patrón implementa un escenario de distribución ramificada para procesar las notificaciones de Amazon S3 procedentes de buckets de S3 entre regiones mediante un tema del Amazon Simple Notification Service (Amazon SNS) para cada región. Estos temas de SNS regional envían las notificaciones de eventos de Amazon S3 a una cola de Amazon Simple Queue Service (Amazon SQS) en una región central que también contiene la función de Lambda. La función de Lambda se suscribe a esta cola de SQS y procesa las notificaciones de eventos de acuerdo con los requisitos de su organización.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Buckets de S3 existentes en varias regiones, incluida una región central para alojar la cola de Amazon SQS y la función de Lambda.
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada. Para obtener más información, consulte Instalar, actualizar y desinstalar la CLI de AWS en la documentación de AWS CLI.

- Familiaridad con el escenario de distribución ramificada en Amazon SNS. Para obtener más información al respecto, consulte Escenarios comunes de Amazon SNS en la documentación de Amazon SNS.

Arquitectura

El siguiente diagrama muestra la arquitectura para el enfoque de este patrón.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Amazon S3 envía notificaciones de eventos sobre buckets de S3 (por ejemplo, objetos creados, objetos retirados o objetos restaurados) a un tema de SNS de la misma región.
2. El tema de SNS publica el evento en una cola de SQS en la región central.
3. La cola SQS está configurada como el origen de eventos de la función de Lambda y almacena en búfer los mensajes de eventos de la función de Lambda.
4. La función de Lambda sondea la cola de SQS en busca de mensajes y procesa las notificaciones de eventos de Amazon S3 según los requisitos de la aplicación.

Pila de tecnología

- Lambda
- Amazon SNS
- Amazon SQS
- Amazon S3

Herramientas

- AWS CLI: la Interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto para interactuar con los servicios de AWS mediante comandos en el intérprete de comandos de línea de comandos. Con una configuración mínima, puede ejecutar comandos de la CLI de AWS que implementan una funcionalidad equivalente a la proporcionada por la consola de administración de AWS basada en navegador desde un símbolo del sistema.

- AWS CloudFormation: AWS le CloudFormation ayuda a modelar y configurar sus recursos de AWS, a aprovisionarlos de forma rápida y coherente y a gestionarlos durante todo su ciclo de vida. Facilita poder usar una plantilla para describir los recursos y sus dependencias, y lanzarlos y configurarlos juntos como una pila, en lugar de administrarlos de forma individual. Puede administrar y aprovisionar pilas en varias cuentas y regiones de AWS.
- AWS Lambda AWS Lambda es un servicio informático que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo. Solo pagará por el tiempo de computación que consuma, no se aplican cargos cuando el código no se está ejecutando.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) coordina y gestiona la entrega o el envío de mensajes entre publicadores y clientes, incluyendo los servidores web y las direcciones de correo electrónico. Los suscriptores reciben todos los mensajes publicados de los temas a los que están suscritos y todos los suscriptores de un tema reciben los mismos mensajes.
- Amazon SQS: Amazon Simple Queue Service (Amazon SQS) ofrece una cola alojada segura, duradera y disponible que le permite integrar y desacoplar sistemas y componentes de software distribuidos. Amazon SQS admite tanto las colas estándar como las colas FIFO.

Epics

Crear la cola SQS y la función de Lambda en su región central

Tarea	Descripción	Habilidades requeridas
Cree una cola de SQS con un desencadenador Lambda.	Inicie sesión en la consola de administración de AWS y siga las instrucciones del tutorial Uso de Lambda con Amazon SQS de la documentación de AWS Lambda para crear los siguientes recursos en su región central: • Un rol de ejecución de Lambda	AWS DevOps, arquitecto de nube

Tarea	Descripción	Habilidades requeridas
	• Una función de Lambda para procesar los eventos de Amazon S3 • Una cola de SQS Nota: asegúrese de configura r la cola de SQS como origen de eventos de la función de Lambda.	

Cree un tema de SNS y configure las notificaciones de eventos para los buckets de S3 de cada región requerida

Tarea	Descripción	Habilidades requeridas
Cree un tema de SNS para recibir notificaciones de eventos de Amazon S3.	Cree un tema de SNS en una región de la que desee recibir notificaciones de eventos de Amazon S3. Para obtener más información al respecto, consulte Creación de un tema SNS en la documentación de Amazon SNS. Importante: asegúrese de registrar el nombre de recurso de Amazon (ARN) de su tema de SNS.	AWS DevOps, arquitecto de nube
Suscriba el tema SNS a la cola SQS central.	Suscriba su tema de SNS a la cola de SQS alojada en su región central. Para obtener más información al respecto, consulte Suscripción a un	AWS DevOps, arquitecto de nube

Tarea	Descripción	Habilidades requeridas
	tema SNS en la documentación de Amazon SNS.	

Tarea	Descripción	Habilidades requeridas
Actualice la política de acceso del tema SNS.	1. Abra la consola de Amazon SNS, seleccione Temas y, a continuación, elija el tema SNS que creó anteriormente. 2. Seleccione Editar y, a continuación, amplíe la sección Política de acceso (opcional). 3. Adjunte la siguiente política de acceso a su tema de SNS para conceder permisos de `sns:publish` a Amazon S3 y, a continuación, seleccione Guardar: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "0", "Effect": "Allow", "Principal": { "Service": "s3.amazonaws.com" }, "Action": "sns:Publish", "Resource": "arn:aws:sns:us-west-2::s3Events-SNSTopic-us-west-2" } ]`	AWS DevOps, arquitecto de nube

Tarea	Descripción	Habilidades requeridas
	`}`	
Configure las notificaciones para cada bucket de S3 de la región.	Configure las notificaciones de eventos para cada bucket de S3 de la región. Para obtener más información al respecto, consulte Activación y configuración de las notificaciones de eventos mediante la consola de Amazon S3 en la documentación de Amazon S3. Nota: en la sección Destino, elija el tema de SNS y especifique el ARN del tema de SNS que creó anteriormente.	AWS DevOps, arquitecto de nube
Repita esta épica en todas las regiones requeridas.	Importante: repita las tareas de esta épica para cada región de la que desee recibir notificaciones de eventos de Amazon S3, incluida la región central.	AWS DevOps, arquitecto de nube

Recursos relacionados

- Configuración de una política de acceso (documentación de Amazon SQS)
- Configuración de una cola de SQS como fuente de eventos (documentación de AWS Lambda)
- Configuración de una cola de SQS para iniciar una función de Lambda (documentación de Amazon SQS)
- AWS::Lambda::Function recurso (CloudFormation documentación de AWS)

Tres tipos de trabajos de AWS Glue ETL para convertir datos a Apache Parquet

Creado por Adnan Alvee (AWS), Karthikeyan Ramachandran y Nith Govindasivan (AWS)

Entorno: PoC o piloto	Tecnologías: análisis	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: AWS Glue		

Resumen

En la nube de Amazon Web Services (AWS), AWS Glue es un servicio de extracción, transformación y carga (ETL) totalmente administrado. Con AWS Glue puede categorizar datos, limpiarlos, enriquecerlos y trasladarlos de manera fiable entre distintos almacenes y flujos de datos de manera rentable.

Este patrón proporciona diferentes tipos de trabajos en AWS Glue y utiliza tres scripts diferentes para demostrar la creación de trabajos de ETL.

Puede usar AWS Glue para escribir trabajos de ETL en un entorno de intérprete de comandos de Python. También puede crear trabajos ETL por lotes o en streaming mediante Python (PySpark) o Scala en un entorno Apache Spark gestionado. Para empezar a crear trabajos de ETL, este patrón se centra en los trabajos de ETL por lotes utilizando Python shell y Scala. PySpark Los trabajos de intérprete de comandos de Python están pensados para cargas de trabajo que requieren menos potencia de cálculo. El entorno gestionado de Apache Spark está diseñado para cargas de trabajo que requieren una gran potencia de cálculo.

Apache Parquet está diseñado para admitir esquemas de compresión y codificación eficientes. Puede acelerar sus cargas de trabajo de análisis porque almacena los datos en forma de columnas. La conversión de datos a Parquet puede ahorrarle espacio de almacenamiento, costos y tiempo a largo plazo. Para obtener más información sobre Parquet, consulte la entrada del blog Apache Parquet: cómo ser un héroe con el formato de datos en columnas de código abierto.

Requisitos previos y limitaciones

Requisitos previos

- Función de AWS Identity and Access Management (IAM) (si no tiene ninguna función, consulte la sección de información adicional).

Arquitectura

Pila de tecnología de destino

- AWS Glue
- Amazon Simple Storage Service (Amazon S3)
- Apache Parquet

Automatizar y escalar

- Los flujos de trabajo de AWS Glue admiten la automatización total de una canalización de ETL.
- Puede cambiar el número de unidades de procesamiento de datos (DPU), o tipos de trabajo, para escalarlas horizontal y verticalmente.

Herramientas

Servicios de AWS

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Glue es un servicio de ETL totalmente gestionado que le ayuda a clasificar, limpiar, enriquecer y mover datos de forma fiable entre almacenes de datos y flujos de datos.

Otras herramientas

- Apache Parquet es un formato de archivo de datos de código abierto orientado por columnas diseñado para el almacenamiento y la recuperación.

Configuración

Utilice los siguientes ajustes para configurar la potencia de procesamiento de AWS Glue ETL. Para reducir los costos, utilice la configuración mínima cuando ejecute la carga de trabajo que se proporciona en este patrón.

- Intérprete de comandos de Python: puede usar 1 DPU para utilizar 16 GB de memoria o 0,0625 DPU para utilizar 1 GB de memoria. Este patrón usa 0,0625 DPU, que es el valor predeterminado en la consola de AWS Glue.
- Python o Scala para Spark: si elige los tipos de trabajo relacionados con Spark en la consola, AWS Glue utiliza de forma predeterminada 10 trabajadores y el tipo de trabajador G.1X. Este patrón utiliza dos trabajadores, que es el número mínimo permitido, y el tipo de trabajador estándar es suficiente y rentable.

En la siguiente tabla se muestran los distintos tipos de trabajadores de AWS Glue para el entorno Apache Spark. Como un trabajo de intérprete de comandos de Python no utiliza el entorno Apache Spark para ejecutar Python, no se incluye en la tabla.

	Estándar	G.1 X	G.2X
vCPU	4	4	8
Memoria	16 GB	16 GB	32 GB
Espacio en disco	50 GB	64 GB	128 GB
Ejecutor por trabajo	2.	1	1

Código

Para ver el código que se utiliza en este patrón, incluida la configuración del rol de IAM y los parámetros de IAM, consulte la sección de Información adicional.

Epics

Carga de datos

Tarea	Descripción	Habilidades requeridas
Cargue los datos en un bucket de S3 nuevo o en un bucket de S3 ya existente.	Cree utilice un bucket de S3 existente en su cuenta. Cargue el archivo sample_data.csv de la sección de	AWS general

Tarea	Descripción	Habilidades requeridas
	Adjuntos y anote el bucket de S3 y la ubicación del prefijo.	

Cree y ejecute el trabajo de AWS Glue

Tarea	Descripción	Habilidades requeridas
Cree el trabajo de AWS Glue	En la sección ETL de la consola de AWS Glue, añada un trabajo de AWS Glue. Seleccione el tipo de trabajo adecuado, la versión de AWS Glue y el tipo de DPU/traba jador y el número de trabajado res correspondientes. Para más información, consulte la sección Configuración.	Desarrollador, nube o datos
Cambie las ubicaciones de entrada y salida.	Copie el código correspon diente a su trabajo de AWS Glue y cambie la ubicación de entrada y salida que indicó en la descripción de la épica Cargar los datos.	Desarrollador, nube o datos
Configure los parámetros.	Puede utilizar los fragmento s que se proporcionan en la sección de Additional informati on (Información adicional) para establecer los parámetro s de su trabajo de ETL. AWS Glue utiliza cuatro nombres de argumentos internamente: • `--conf`	Desarrollador, nube o datos

Tarea	Descripción	Habilidades requeridas
	• `--debug` • `--mode` • `--JOB_NAME` El parámetro `--JOB_NAME` debe introducirse de forma explícita en la consola de AWS Glue. Elija Trabajos, Edit Job (Editar trabajo), Security configuration, script libraries, and job parameter s (optional) (Configuración de seguridad, bibliotecas de scripts y parámetros de trabajo (opcional)). Introduzc a `--JOB_NAME` como clave y proporcione un valor. También puede utilizar la Interfaz de la línea de comandos de AWS (AWS CLI) o la API de AWS Glue para configurar este parámetro. Spark usa el parámetro `--JOB_NAME` y no es necesario en un trabajo de entorno de intérprete de comandos de Python. Debe añadir `--` antes del nombre de cada parámetro ; de lo contrario, el código no funcionará. Por ejemplo, en el caso de los fragmento s de código, los parámetros de ubicación deben invocarse	

Tarea	Descripción	Habilidades requeridas
	mediante `--input_loc` y `--output_loc` .	
Ejecute el trabajo de ETL.	Ejecute su trabajo y compruebe el resultado. Observe cuánto espacio se ha reducido con respecto al archivo original.	Desarrollador, nube o datos

Recursos relacionados

Referencias

- Apache Spark
- AWS Glue: cómo funciona
- Precios de AWS Glue

Tutoriales y videos

- ¿Qué es AWS Glue?

Información adicional

Rol de IAM

Al crear los trabajos de AWS Glue, puede usar un rol de IAM existente que tenga los permisos que se muestran en el siguiente fragmento de código o un rol nuevo.

Para crear un nuevo rol, utilice el siguiente código YAML.

```
# (c) 2022 Amazon Web Services, Inc. or its affiliates. All Rights Reserved. This AWS
 Content is provided subject to the terms of the AWS Customer
# Agreement available at https://aws.amazon.com/agreement/ or other written agreement
 between Customer and Amazon Web Services, Inc.

AWSTemplateFormatVersion: "2010-09-09"
```

```
Description: This template will setup IAM role for AWS Glue service.

Resources:
  rGlueRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: "Allow"
            Principal:
              Service:
                - "glue.amazonaws.com"
            Action:
              - "sts:AssumeRole"
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole
      Policies:
        - PolicyName: !Sub "${AWS::StackName}-s3-limited-read-write-inline-policy"
          PolicyDocument:
            Version: "2012-10-17"
            Statement:
              - Effect: Allow
                Action:
                  - "s3:PutObject"
                  - "s3:GetObject"
                Resource: "arn:aws:s3:::*/*"
      Tags:
        - Key  : "Name"
          Value : !Sub "${AWS::StackName}"

Outputs:
  oGlueRoleName:
    Description: AWS Glue IAM role
    Value:
      Ref: rGlueRole
    Export:
      Name: !Join [ ":", [ !Ref "AWS::StackName", rGlueRole ] ]
```

AWS Glue (intérprete de comandos de Python)

El código Python usa los Pandas y PyArrow las bibliotecas para convertir los datos a Parquet. La biblioteca Pandas ya está disponible. La PyArrow biblioteca se descarga al ejecutar el patrón, ya que se ejecuta una sola vez. Puede usar archivos de rueda PyArrow para convertirlos en una biblioteca y proporcionar el archivo como un paquete de biblioteca. Para obtener más información, consulte Proporcionar su propia biblioteca de Python

Parámetros del intérprete de comandos de Python de AWS Glue

```
from awsglue.utils import getResolvedOptions

args = getResolvedOptions(sys.argv, ["input_loc", "output_loc"])
```

AWS Glue (intérprete de comandos)

```
from io import BytesIO
import pandas as pd
import boto3
import os
import io
import site
from importlib import reload
from setuptools.command import easy_install
install_path = os.environ['GLUE_INSTALLATION']
easy_install.main( ["--install-dir", install_path, "pyarrow"] )
reload(site)
import pyarrow


input_loc = "bucket-name/prefix/sample_data.csv"
output_loc = "bucket-name/prefix/"


input_bucket = input_loc.split('/', 1)[0]
object_key = input_loc.split('/', 1)[1]


output_loc_bucket = output_loc.split('/', 1)[0]
output_loc_prefix = output_loc.split('/', 1)[1]


s3 = boto3.client('s3')
obj = s3.get_object(Bucket=input_bucket, Key=object_key)
```

```
df = pd.read_csv(io.BytesIO(obj['Body'].read()))


parquet_buffer = BytesIO()
s3_resource = boto3.resource('s3')
df.to_parquet(parquet_buffer, index=False)
s3_resource.Object(output_loc_bucket, output_loc_prefix +  'data' +
 '.parquet').put(Body=parquet_buffer.getvalue())
```

Trabajo de AWS Glue Spark con Python

Para usar un tipo de trabajo de AWS Glue Spark con Python, elija Spark como tipo de trabajo. Elija Spark 3.1, Python 3 con un tiempo de inicio de trabajo mejorado (Glue versión 3.0) como versión AWS Glue.

Parámetros de Python de AWS Glue

```
from awsglue.utils import getResolvedOptions

args = getResolvedOptions(sys.argv, ["JOB_NAME", "input_loc", "output_loc"])
```

Trabajo de AWS Glue Spark con el código de Python

```
import sys
from pyspark.context import SparkContext
from awsglue.context import GlueContext
from awsglue.transforms import *
from awsglue.dynamicframe import DynamicFrame
from awsglue.utils import getResolvedOptions
from awsglue.job import Job


sc = SparkContext()
glueContext = GlueContext(sc)
spark = glueContext.spark_session
job = Job(glueContext)

input_loc = "bucket-name/prefix/sample_data.csv"
output_loc = "bucket-name/prefix/"

inputDyf = glueContext.create_dynamic_frame_from_options(\
    connection_type = "s3", \
```

```
    connection_options = {
        "paths": [input_loc]}, \
    format = "csv",
    format_options={
        "withHeader": True,
        "separator": ","
    })


outputDF = glueContext.write_dynamic_frame.from_options(\
    frame = inputDyf, \
    connection_type = "s3", \
    connection_options = {"path": output_loc \
        }, format = "parquet")
```

En el caso de un gran número de archivos comprimidos de gran tamaño (por ejemplo, 1000 archivos de aproximadamente 3 MB cada uno), utilice el parámetro `compressionType` junto con el parámetro `recurse` para leer todos los archivos disponibles en el prefijo, tal y como se muestra en el código siguiente.

```
input_loc = "bucket-name/prefix/"
output_loc = "bucket-name/prefix/"

inputDyf = glueContext.create_dynamic_frame_from_options(
                    connection_type = "s3",
                    connection_options = {"paths": [input_loc],
                                          "compressionType":"gzip","recurse" :"True",
                                          },
                    format = "csv",
                    format_options={"withHeader": True,"separator": ","}
                    )
```

Para un gran número de archivos pequeños comprimidos (por ejemplo, 1000 archivos de aproximadamente 133 KB cada uno), utilice el parámetro`groupFiles` junto con los parámetros `compressionType` y `recurse`. El parámetro `groupFiles` agrupa los archivos pequeños en varios archivos grandes y el parámetro `groupSize` controla la agrupación según el tamaño especificado en bytes (por ejemplo, 1 MB). El siguiente fragmento de código proporciona un ejemplo del uso de estos parámetros en el código.

```
input_loc = "bucket-name/prefix/"
output_loc = "bucket-name/prefix/"
```

```
inputDyf = glueContext.create_dynamic_frame_from_options(
                    connection_type = "s3",
                    connection_options = {"paths": [input_loc],
                                          "compressionType":"gzip","recurse" :"True",
                                           "groupFiles" :"inPartition",
 "groupSize" :"1048576",
                                          },
                    format = "csv",
                    format_options={"withHeader": True,"separator": ","}
                    )
```

Sin ningún cambio en los nodos de trabajo, esta configuración permite que el trabajo de AWS Glue lea varios archivos (grandes o pequeños, con o sin compresión) y los escriba en el destino en formato Parquet.

Trabajo de AWS Glue Spark con Scala

Para usar un tipo de trabajo de AWS Glue Spark con Scala, elija Spark como tipo de trabajo y un Language (Idioma) como Scala. Elija Spark 3.1, Scala 2 con un tiempo de inicio de trabajo mejorado (Glue versión 3.0) como versión de AWS Glue. Para ahorrar espacio de almacenamiento, en el siguiente ejemplo de AWS Glue with Scala también se utiliza la característica `applyMapping` para convertir tipos de datos.

Parámetros de AWS Glue Scala

```
import com.amazonaws.services.glue.util.GlueArgParser val args =
 GlueArgParser.getResolvedOptions(sysArgs, Seq("JOB_NAME", "inputLoc",
 "outputLoc").toArray)
```

Trabajo de AWS Glue Spark con código Scala

```
import com.amazonaws.services.glue.GlueContext
import com.amazonaws.services.glue.MappingSpec
import com.amazonaws.services.glue.DynamicFrame
import com.amazonaws.services.glue.errors.CallSite
import com.amazonaws.services.glue.util.GlueArgParser
import com.amazonaws.services.glue.util.Job
import com.amazonaws.services.glue.util.JsonOptions
import org.apache.spark.SparkContext
import scala.collection.JavaConverters._
```

```
object GlueScalaApp {
  def main(sysArgs: Array[String]) {

    @transient val spark: SparkContext = SparkContext.getOrCreate()
    val glueContext: GlueContext = new GlueContext(spark)

    val inputLoc = "s3://bucket-name/prefix/sample_data.csv"
    val outputLoc = "s3://bucket-name/prefix/"

    val readCSV = glueContext.getSource("csv", JsonOptions(Map("paths" ->
 Set(inputLoc)))).getDynamicFrame()

    val applyMapping = readCSV.applyMapping(mappings = Seq(("_c0", "string", "date",
 "string"), ("_c1", "string", "sales", "long"),
    ("_c2", "string", "profit", "double")), caseSensitive = false)

    val formatPartition = applyMapping.toDF().coalesce(1)

    val dynamicFrame = DynamicFrame(formatPartition, glueContext)

    val dataSink = glueContext.getSinkWithFormat(
        connectionType = "s3",
        options = JsonOptions(Map("path" -> outputLoc )),
        transformationContext = "dataSink", format =
 "parquet").writeDynamicFrame(dynamicFrame)
  }
}
```

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Visualice los registros de auditoría de Amazon Redshift con Amazon Athena y Amazon QuickSight

Documento creado por Sanket Sirsikar (AWS) y Gopal Krishna Bhatia (AWS)

Entorno: PoC o piloto	Tecnologías: análisis, macrodatos, lagos de datos	Servicios de AWS: Amazon Athena; Amazon Redshift; Amazon S3; Amazon QuickSight

Resumen

La seguridad es una parte integral de las operaciones de base de datos en la nube de Amazon Web Services (AWS). Su organización debe asegurarse de supervisar las actividades y las conexiones de los usuarios de la base de datos para detectar posibles incidentes y riesgos de seguridad. Este patrón ayuda a supervisar las bases de datos con fines de seguridad y solución de problemas, un proceso que suele denominarse auditoría de base de datos.

Este patrón proporciona un script SQL que automatiza la creación de una tabla de Amazon Athena y vistas para un panel de informes en Amazon que le ayuda a auditar los registros de QuickSight Amazon Redshift. Esto garantiza que los usuarios responsables de supervisar las actividades de la base de datos tengan un acceso cómodo a las características de seguridad de los datos.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Un clúster de Amazon Redshift existente. Para obtener más información, consulte Create an Amazon Redshift cluster (Crear un clúster de Amazon Redshift) en la documentación de Amazon Redshift.
- Acceso a un grupo de trabajo de Athena existente. Para obtener más información, consulte How workgroups work (Cómo funcionan los grupos de trabajo) en la documentación de Amazon Athena.
- Un bucket de origen de Amazon Simple Storage Service (Amazon S3) con los permisos de AWS Identity and Access Management (IAM) requeridos. Para obtener más información, consulte

Bucket permissions for Amazon Redshift audit logging (Permisos de bucket para el registro de auditoría de Amazon Redshift) en Database audit logging (Registros de auditoría de bases de datos) de la documentación de Amazon Redshift.

Arquitectura

Pila de tecnología

- Athena
- Amazon Redshift
- Amazon S3
- QuickSight

Herramientas

- Amazon Athena : Athena es un servicio de consultas interactivo que facilita el análisis de datos en Amazon S3 con SQL estándar.
- Amazon QuickSight: QuickSight es un servicio de inteligencia empresarial (BI) escalable, sin servidor, integrable y basado en el aprendizaje automático.
- Amazon Redshift: Amazon Redshift es un servicio de almacenamiento de datos completamente administrado, de nivel empresarial y de escala de petabytes.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet.

Epics

Configurar el clúster de Amazon Redshift

Tarea	Descripción	Habilidades requeridas
Habilite el registro de auditoría para el clúster de Amazon Redshift.	1. Inicie sesión en la consola de administración de AWS, abra la consola de Amazon	Administrador de base de datos, ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	Redshift, seleccione CLUSTERS y, a continuación, el clúster para el que desea habilitar el registro. 2. Seleccione la pestaña Properties (Propiedades) y, a continuación, active la auditoría; para ello, siga las instrucciones de Configuring auditing using the console (Configurar la auditoría mediante la consola) en la documentación de Amazon Redshift.	

Tarea	Descripción	Habilidades requeridas
Habilite el registro en el grupo de parámetros del clúster de Amazon Redshift.	Puede habilitar la auditoría de los registros de conexión, los registros de usuario y los registros de actividad de los usuarios al mismo tiempo mediante la Consola de administración de AWS, la API de referencia de Amazon Redshift o la interfaz de la línea de comandos de AWS (AWS CLI). Para auditar los registros de actividad de los usuarios, también debe habilitar el parámetro `enable_user_activity_logging` de la base de datos. Si habilita solo la característica de registro de auditoría y no el parámetro asociado, los registros de auditoría de la base de datos registrarán únicamente la información de los registros de conexión y de usuario, pero no la del registro de actividad del usuario. El parámetro `enable_user_activity_logging` no está habilitado de forma predeterminada, pero puede activarlo cambiándolo de `false` a `true`.	Administrador de base de datos, ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	Importante: Debe crear un nuevo grupo de parámetros de clúster con el parámetro `user_activity_logging` activado y adjuntarlo a su clúster de Amazon Redshift. Para obtener más información, consulte Modifying a cluster (Modificar un clúster) en la documentación de Amazon Redshift. Para obtener más información sobre esta tarea, consulte Amazon Redshift parameter groups (Grupos de parámetros de Amazon Redshift) y Configuring auditing using the console (Configurar la auditoría mediante la consola) en la documentación de Amazon Redshift.	

Tarea	Descripción	Habilidades requeridas
Configure los permisos del bucket de S3 para el registro de clúster de Amazon Redshift.	Al habilitar el registro, Amazon Redshift recopila la información de los registros y la carga en los archivos de registro almacenados en el bucket de S3. Puede crear un nuevo bucket de S3 o utilizar un bucket existente. Importante: Asegúrese de que Amazon Redshift tenga los permisos de IAM requeridos para tener acceso al bucket de S3. Para obtener más información al respecto, consulte Bucket permissions for Amazon Redshift audit logging (Permisos de bucket para el registro de auditoría de Amazon Redshift) en Database audit logging (Registros de auditoría de bases de datos) de la documentación de Amazon Redshift.	Administrador de base de datos, ingeniero de datos

Crear la tabla y las vistas de Athena

Tarea	Descripción	Habilidades requeridas
Cree la tabla y las vistas de Athena para consultar los datos del registro de auditoría	Abra la consola de Amazon Athena y utilice la consulta del lenguaje de definición de datos (DDL) del script de	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
de Amazon Redshift desde el bucket de S3.	SQL `AuditLogging.sql` (adjunto) para crear la tabla y las vistas de los registros de actividad de los usuarios, los registros de usuarios y los registros de conexión. Para obtener más informaci ón e instrucciones, consulte el tutorial Create tables and run queries (Crear tablas y ejecutar consultas) del taller de Amazon Athena.	

Configure la supervisión de registros en el panel QuickSight

Tarea	Descripción	Habilidades requeridas
Cree un QuickSight cuadro de mando con Athena como fuente de datos.	Abre la QuickSight consola de Amazon y crea un QuickSigh t panel de control siguiendo las instrucciones del tutorial Visualiza QuickSight con Athena del taller de Amazon Athena.	Administrador de base de datos, ingeniero de datos

Recursos relacionados

- Create tables and run queries in Athena (Crear crear tablas y ejecutar consultas en Athena)
- Visualice QuickSight con Athena

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Visualice los informes de credenciales de IAM para todas las cuentas de AWS que utilizan Amazon QuickSight

Creado por Parag Nagwekar (AWS) y Arun Chandapillai (AWS)

Repositorio de códigos: obtenga una visibilidad de sus informes de credenciales de IAM en toda la organización	Entorno: producción	Tecnologías: análisis; asesoramiento; gestión y gobernanza; seguridad, identidad, conformidad
Carga de trabajo: todas las demás cargas de trabajo	Servicios de AWS: Amazon Athena; AWS EventBridge; CloudFormation Amazon; AWS Identity and Access Management; Amazon QuickSight	

Resumen

> Advertencia: los usuarios de IAM tienen credenciales de larga duración, lo que supone un riesgo para la seguridad. Para ayudar a mitigar este riesgo, le recomendamos que brinde a estos usuarios únicamente los permisos que necesitan para realizar la tarea y que los elimine cuando ya no los necesiten.

Puede utilizar los informes de credenciales de AWS Identity and Access Management (IAM) para ayudarle a cumplir los requisitos de seguridad, auditoría y conformidad de su organización. Los informes de credenciales proporcionan una lista de todos los usuarios de sus cuentas de AWS y muestran el estado de sus credenciales, como las contraseñas, claves de acceso y dispositivos de autenticación multifactor (MFA). Puede usar informes de credenciales para varias cuentas de AWS administradas por AWS Organizations.

Este patrón incluye pasos y código para ayudarle a crear y compartir informes de credenciales de IAM para todas las cuentas de AWS de su organización mediante los paneles de Amazon

QuickSight . Puede compartir los paneles con las partes interesadas de su organización. Los informes pueden ayudar a su organización a lograr los siguientes resultados empresariales previstos:

- Identifique los incidentes de seguridad relacionados con los usuarios de IAM
- Realice un seguimiento de la migración en tiempo real de los usuarios de IAM a la autenticación de inicio de sesión único (SSO)
- Realice un seguimiento de las regiones de AWS a las que acceden los usuarios de IAM
- Manténgase en conformidad
- Comparta información con otras partes interesadas

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Las cuentas miembro de una organización
- Un rol de IAM con permisos para acceder a las cuentas de Organizations
- Interfaz de la línea de comandos de AWS (AWS CLI) versión 2, instalada y configurada
- Una suscripción a la edición Amazon QuickSight Enterprise

Arquitectura

Pila de tecnología

- Amazon Athena
- Amazon EventBridge
- Amazon QuickSight
- Amazon Simple Storage Service (Amazon S3)
- AWS Glue
- AWS Identity y Access Management (IAM)
- AWS Lambda
- AWS Organizations

Arquitectura de destino

El siguiente diagrama muestra una arquitectura para configurar un flujo de trabajo que captura los datos de los informes de credenciales de IAM de varias cuentas de AWS.

1. EventBridge invoca una función Lambda a diario.
2. La función de Lambda asume un rol de IAM en todas las cuentas de AWS de la organización. A continuación, la función crea el informe de credenciales de IAM y almacena los datos del informe en un bucket de S3 centralizado. Debe habilitar el cifrado y desactivar el acceso público en el bucket de S3.
3. Un rastreador de AWS Glue rastrea el depósito de S3 a diario y actualiza la tabla de Athena en consecuencia.
4. QuickSight importa y analiza los datos del informe de credenciales y crea un panel que las partes interesadas pueden visualizar y compartir con ellas.

Herramientas

Servicios de AWS

- Amazon Athena es un servicio de consultas interactivo que facilita el análisis de datos en Amazon S3 con SQL estándar.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, funciones de Lambda, puntos de conexión de invocación HTTP que utilizan destinos API o buses de eventos en otras cuentas de AWS.
- Amazon QuickSight es un servicio de inteligencia empresarial (BI) a escala de nube que le ayuda a visualizar, analizar y elaborar informes sobre sus datos en un único panel de control.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.

Código

El código de este patrón está disponible en el GitHub getiamcredsreport-allaccounts-orgrepositorio. Puede usar el código de este repositorio para crear informes de credenciales de IAM en todas las cuentas de AWS en Organizations y almacenarlos en una ubicación central.

Epics

Configuración de la infraestructura

Tarea	Descripción	Habilidades requeridas
Configura la edición Amazon QuickSight Enterprise.	1. Active la edición Amazon QuickSight Enterprise en su cuenta de AWS. Para obtener más informaci ón, consulta Administr ar el acceso de los usuarios dentro de Amazon QuickSight en la QuickSight documentación. 2. Para conceder permisos al panel de control, obtenga el nombre de recurso de Amazon (ARN) de los QuickSight usuarios.	Administrador de AWS DevOps, administrador de la nube, arquitecto de la nube
Integre Amazon QuickSight con Amazon S3 y Athena.	Debe autorizar el uso QuickSight de Amazon S3 y Athena antes de implement ar la pila de AWS CloudForm ation .	Administrador de AWS DevOps, administrador de la nube, arquitecto de la nube

Implementación de la infraestructura

Tarea	Descripción	Habilidades requeridas
Clona el GitHub repositorio.	1. Clone el GitHub getiamcre dsreport-allaccounts-	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	orgrepositorio en su máquina local ejecutando el siguiente comando: `git clone https://github.com/aws-samples/getiamcredsreport-allaccounts-org`	

Tarea	Descripción	Habilidades requeridas
Implemente la infraestructura.	1. Inicie sesión en la consola de administración de AWS y abra la consola de CloudFormation . 2. En el panel de navegación, seleccione Crear pila y, a continuación, seleccione Con nuevos recursos (estándar). 3. En la página Identificar recursos, seleccione Siguiente. 4. En la página Especificar plantilla, en Origen de la plantilla, seleccione Cargar un archivo de plantilla. 5. Elija Elegir archivo, seleccione el `Cloudformation-createcredrepo.yaml` archivo del GitHub repositorio clonado y, a continuación, elija Siguiente. 6. En Parámetros, actualice `IAMRoleName` con su rol de IAM. Esta debe ser el rol de IAM que desea que Lambda asuma en todas las cuentas de la organización. Esta función crea el informe de credenciales. Nota: No es necesario que el rol esté presente en	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	todas las cuentas en este paso de la creación de la pila. 7. En Parámetros, actualice `S3BucketName` con el nombre del bucket de S3 donde Lambda puede almacenar las credenciales de todas las cuentas. 8. En Nombre de la pila, introduzca el nombre de la pila. 9. Seleccione Enviar. 10 Anote el nombre del rol de la función de Lambda.	

Tarea	Descripción	Habilidades requeridas
Cree una política de permisos de IAM.	Cree una política de IAM para cada cuenta de AWS de su organización con los siguientes permisos: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "iam:GenerateCredentialReport", "iam:GetCredentialReport" ], "Resource": "*" } ] }`	AWS DevOps, administrador de nube, arquitecto de nube, ingeniero de datos

Tarea	Descripción	Habilidades requeridas
Cree un rol de IAM con una política de confianza.	1. Cree un rol de IAM para las cuentas de AWS y adjunte la política de permisos que creó en el paso anterior. 2. Adjunte la siguiente política de confianza al rol de IAM: `{ "Version":"2012-10-17", "Statement":[ { "Effect": "Allow", "Principal":{ "AWS":[ "arn:aws:iam::<MasterAccountID>:role/<LambdaRole>" ] }, "Action": "sts:AssumeRole" } ] }` Importante: Sustituya `arn:aws:iam::<MasterAccountID>:role/<LambdaRole>` por el ARN de la función de Lambda que indicó anteriormente. Nota: Las organizaciones suelen utilizar la automatiz	Administrador de la nube, arquitecto de la nube, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	ación para crear funciones de IAM para sus cuentas de AWS. Le recomendamos que utilice esta automatización, si está disponible. Como alternativa, puede utilizar el `CreateRoleforOrg.py` script del repositorio de código . El script requiere una función administrativa existente o cualquier otro rol de IAM que tenga permiso para crear una política y un rol de IAM en cada cuenta de AWS.	
Configura Amazon QuickSight para que visualice los datos.	1. Inicie sesión QuickSight con sus credenciales. 2. Cree un conjunto de datos con Athena (con la base de datos `iamcredreportdb` y la tabla `“cfn_iamc redreport”`) y, a continuación, actualice automáticamente el conjunto de datos. 3. Crea un análisis en QuickSight. 4. Crea un QuickSight panel de control.	AWS DevOps, administrador de nube, arquitecto de nube, ingeniero de datos

Información adicional

Consideraciones adicionales

Considere lo siguiente:

- Después de implementar la infraestructura, puede esperar a que Athena cree los informes en Amazon S3 y los analice hasta que Lambda y AWS Glue se ejecuten según lo programado. CloudFormation Como alternativa, puede ejecutar Lambda manualmente para obtener los informes en Amazon S3 y, a continuación, ejecutar el rastreador AWS Glue para obtener la tabla Athena que se crea a partir de los datos.
- QuickSight es una poderosa herramienta para analizar y visualizar datos en función de los requisitos de su empresa. Puede utilizar los parámetros QuickSight para controlar los datos de los widgets en función de los campos de datos que elija. Además, puedes usar un QuickSight análisis para crear parámetros (por ejemplo, campos de cuenta, fecha y usuario como `partition_0``partition_1`, y `user` respectivamente) a partir de tu conjunto de datos para añadir controles a los parámetros de cuenta, fecha y usuario.
- Para crear sus propios QuickSight paneles, consulte QuickSight Workshops en el sitio web de AWS Workshop Studio.
- Para ver ejemplos de QuickSight cuadros de mando, consulte el repositorio de GitHub getiamcredsreport-allaccounts-orgcódigo.

Resultados empresariales específicos

Puede utilizar esta guía para lograr los siguientes resultados empresariales:

- Identifique los incidentes de seguridad relacionados con los usuarios de IAM: investigue a todos los usuarios de todas las cuentas de AWS de su organización mediante un único panel de control. Puede realizar un seguimiento de la tendencia de las regiones de AWS individuales a las que accedió más recientemente un usuario de IAM y de los servicios que utilizó.
- Realice un seguimiento de la migración en tiempo real de los usuarios de IAM a la autenticación de SSO: mediante el SSO, los usuarios pueden iniciar sesión una vez con una sola credencial y acceder a varias cuentas y aplicaciones de AWS. Si planea migrar sus usuarios de IAM al SSO, este patrón puede ayudarlo a realizar la transición al SSO y a realizar un seguimiento del uso de todas las credenciales de los usuarios de IAM (como el acceso a la consola de administración de AWS o el uso de claves de acceso) en todas las cuentas de AWS.
- Realice un seguimiento de las regiones de AWS a las que acceden los usuarios de IAM: puede controlar el acceso de los usuarios de IAM a las regiones con diversos fines, como la soberanía de los datos y el control de costos. También puede realizar un seguimiento del uso de las regiones por parte de cualquier usuario de IAM.

- Cumpla con las normas: si sigue el principio de privilegios mínimos, solo puede conceder los permisos de IAM específicos necesarios para realizar una tarea específica. Además, puede realizar un seguimiento del acceso a los servicios de AWS, a la consola de administración de AWS y al uso prolongado de las credenciales.
- Comparta información con otras partes interesadas: puede compartir paneles seleccionados con otras partes interesadas, sin darles acceso a los informes de credenciales de IAM ni a las cuentas de AWS.

Más patrones

- ???
- Extraer contenido de archivos PDF automáticamente con Amazon Textract
- Cree una canalización de datos para incorporar, transformar y analizar los datos de Google Analytics con el kit de DataOps desarrollo de AWS
- ???
- Capturar datos de IoT directamente en Amazon S3 de forma rentable con AWS IoT Greengrass
- Crear informes detallados de costos y uso para los clústeres de Amazon EMR mediante el explorador de costos de AWS.
- Crear informes detallados de costos y uso para Amazon RDS y Amazon Aurora
- Crear informes detallados de costos y uso para los trabajos de AWS Glue con el explorador de costos de AWS
- Automatización del intercambio de datos entre cuentas
- Implementar y administrar un lago de datos sin servidor en la nube de AWS mediante el uso de la infraestructura como código
- Inserta un QuickSight panel de Amazon en una aplicación Angular local
- Asegúrese de que el clúster de Amazon Redshift esté cifrado en el momento de su creación
- Asegúrese de que el cifrado de los datos en reposo de Amazon EMR esté habilitado en el momento del lanzamiento
- Extraiga y consulte SiteWise los atributos de metadatos de AWS IoT en un lago de datos
- Genere información de datos mediante AWS Mainframe Modernization y Amazon Q en QuickSight
- Otorgue a las instancias de SageMaker notebook acceso temporal a un CodeCommit repositorio de otra cuenta de AWS
- Identifique y avise cuando los recursos de Amazon Data Firehose no estén cifrados con una clave de AWS KMS
- Migración de un entorno de MongoDB autoalojado a MongoDB Atlas en la nube de AWS
- Migre una base de datos Oracle a Amazon RDS for Oracle mediante adaptadores de archivos planos de GoldenGate Oracle
- Migración de una base de datos de Oracle a Amazon Redshift con AWS DMS y AWS SCT
- Migre datos de un entorno Hadoop local a Amazon S3 con DistCp AWS PrivateLink para Amazon S3

- ???
- Migración de cargas de trabajo de Cloudera en las instalaciones a la plataforma de datos de Cloudera en AWS
- Supervisar los clústeres de Amazon EMR para comprobar el cifrado en tránsito en el momento del lanzamiento
- Configurar un panel de monitoreo de Grafana para AWS ParallelCluster
- Compruebe que los nuevos clústeres de Amazon Redshift tengan puntos de conexión SSL necesarios
- Compruebe que los nuevos clústeres de Amazon Redshift se lanzan en una VPC
- ???

Productividad empresarial

Temas

- Configure una PeopleSoft arquitectura de alta disponibilidad en AWS
- Más patrones

Configure una PeopleSoft arquitectura de alta disponibilidad en AWS

Entorno: producción	Tecnologías: productividad empresarial; infraestructura; aplicaciones web y móviles; bases de datos	Carga de trabajo: Oracle
Servicios de AWS: Amazon EC2 Auto Scaling; Amazon EFS; Elastic Load Balancing (ELB); Amazon RDS		

Resumen

Cuando migra sus PeopleSoft cargas de trabajo a AWS, la resiliencia es un objetivo importante. Garantiza que su PeopleSoft aplicación siempre tenga una alta disponibilidad y pueda recuperarse rápidamente de los errores.

Este patrón proporciona una arquitectura para sus PeopleSoft aplicaciones en AWS a fin de garantizar la alta disponibilidad (HA) en los niveles de red, aplicación y base de datos. Emplea una base de datos Amazon Relational Database Service (Amazon RDS) para Oracle o Amazon RDS para SQL Server en el nivel de base de datos. Esta arquitectura escalable también incluye servicios de AWS como Amazon Route 53, instancias de Linux en Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Block Storage (Amazon EBS), Amazon Elastic File System (Amazon EFS) y un equilibrador de carga de aplicación.

Oracle PeopleSoft proporciona un conjunto de herramientas y aplicaciones para la administración de la fuerza laboral y otras operaciones empresariales.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un PeopleSoft entorno con las licencias necesarias para configurarlo en AWS

- Una nube privada virtual (VPC) configurada en su cuenta de AWS con los siguientes recursos:
  - Al menos dos zonas de disponibilidad
  - Una subred pública y tres subredes privadas en cada zona de disponibilidad
  - Una puerta de enlace NAT y una puerta de enlace de Internet
  - Tablas de enrutamiento en cada subred para enrutar el tráfico
  - Listas de control de acceso a la red (ACL de red) y grupos de seguridad definidos para garantizar la seguridad de la PeopleSoft aplicación de acuerdo con los estándares de su organización

Limitaciones

- Este patrón proporciona una solución de alta disponibilidad (HA). No es compatible con escenarios de recuperación de desastres (DR). En el infrecuente caso de que toda la región de AWS para la implementación de alta disponibilidad dejase de estar disponible, la aplicación dejaría de estar disponible.

Versiones de producto

- PeopleSoft aplicaciones que ejecutan la versión PeopleTools 8.52 y versiones posteriores

Arquitectura

Arquitectura de destino

El tiempo de inactividad o la interrupción de PeopleSoft la aplicación de producción afectan a la disponibilidad de la aplicación y provocan importantes interrupciones en su negocio.

Le recomendamos que diseñe su aplicación de PeopleSoft producción de manera que siempre tenga una alta disponibilidad. Para ello, puede eliminar los puntos únicos de fallo, añadir puntos de cruce o conmutación por error fiables y detectar los fallos. El siguiente diagrama ilustra una arquitectura de alta disponibilidad para PeopleSoft AWS.

Esta implementación de arquitectura utiliza Amazon RDS for Oracle como PeopleSoft base de datos e instancias EC2 que se ejecutan en Red Hat Enterprise Linux (RHEL). También puede usar Amazon RDS para SQL Server como base de datos de Peoplesoft.

Esta arquitectura contiene los siguientes componentes:

- Amazon Route 53 se utiliza como servidor de nombres de dominio (DNS) para enrutar las solicitudes de Internet a la PeopleSoft aplicación.
- AWS WAF le ayuda a protegerse contra exploits y bots web comunes que pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos. AWS Shield Avanzado (no se ilustra) proporciona una protección mucho más amplia.
- El Equilibrador de carga de aplicación equilibra la carga del tráfico HTTP y HTTPS con un enrutamiento de solicitudes avanzado dirigido a los servidores web.
- Los servidores web, los servidores de aplicaciones, los servidores del programador de procesos y los servidores Elasticsearch que admiten la PeopleSoft aplicación se ejecutan en varias zonas de disponibilidad y utilizan Amazon EC2 Auto Scaling.
- La base de datos utilizada por la PeopleSoft aplicación se ejecuta en Amazon RDS en una configuración Multi-AZ.
- El recurso compartido de archivos que utiliza la PeopleSoft aplicación está configurado en Amazon EFS y se utiliza para acceder a los archivos de todas las instancias.
- Amazon EC2 Auto Scaling utiliza Amazon Machine Images (AMI) para garantizar que PeopleSoft los componentes se clonen rápidamente cuando sea necesario.
- Las puertas de enlace NAT conectan las instancias de una subred privada a servicios externos a su VPC y garantizan que los servicios externos no puedan iniciar una conexión con dichas instancias.
- La puerta de enlace de internet es un componente de la VPC de escalado horizontal, redundante y de alta disponibilidad que permite la comunicación entre su VPC e internet.
- Los host bastión de la subred pública proporcionan acceso a los servidores de la subred privada desde una red externa, como Internet o una red en las instalaciones. Los host bastión proporcionan un acceso controlado y seguro a los servidores de las subredes privadas.

Detalles de la arquitectura

La PeopleSoft base de datos está alojada en una base de datos de Amazon RDS for Oracle (o Amazon RDS for SQL Server) en una configuración Multi-AZ. La función Amazon RDS Multi-AZ replica las actualizaciones de la base de datos en dos zonas de disponibilidad para aumentar la durabilidad y la disponibilidad. Amazon RDS conmuta automáticamente a la base de datos en espera en caso de mantenimiento planificado e interrupciones imprevistas.

La PeopleSoft web y el nivel medio se instalan en las instancias EC2. Estas instancias se distribuyen en varias zonas de disponibilidad, y están vinculadas a un grupo de escalado automático. Esto garantiza que estos componentes estén siempre altamente disponibles. Se mantiene el número mínimo de instancias necesarias para garantizar que la aplicación esté siempre disponible y pueda escalarse cuando sea necesario.

Recomendamos usar un tipo de instancia EC2 de la generación actual para las instancias EC2 OEM. Los tipos de instancias de la generación actual, como instancias creadas en AWS Nitro System, son compatibles con las máquinas virtuales de hardware (HVM). Las AMI de HVM son necesarias para beneficiarse de las redes mejoradas, y también ofrecen una mayor seguridad. Las instancias de EC2 que forman parte de cada grupo de escalado automático usan su propia AMI al reemplazar o escalar verticalmente las instancias. Se recomienda seleccionar los tipos de instancias EC2 en función de la carga que desee que gestione la PeopleSoft aplicación y de los valores mínimos recomendados por Oracle para la PeopleSoft aplicación y PeopleTools la versión. Para obtener más información sobre los requisitos de hardware y software, consulte el sitio web de soporte de Oracle.

La PeopleSoft web y el nivel medio comparten una montura de Amazon EFS para compartir informes, archivos de datos y (si es necesario) el `PS_HOME` directorio. Amazon EFS se configura con objetivos de montaje en cada zona de disponibilidad por motivos de rendimiento y costo.

Se aprovisiona un Application Load Balancer para soportar el tráfico que accede a la PeopleSoft aplicación y equilibra la carga del tráfico entre los servidores web de las diferentes zonas de disponibilidad. Un equilibrador de carga de aplicación es un dispositivo de red que proporciona alta disponibilidad en, al menos, dos zonas de disponibilidad. Los servidores web distribuyen el tráfico a diferentes servidores de aplicaciones mediante una configuración de equilibrio de carga. El equilibrador de carga entre el servidor web y el servidor de aplicaciones garantiza que la carga se distribuya de manera uniforme entre las instancias, ayudando a evitar los cuellos de botella y las interrupciones del servicio debido a la sobrecarga de las instancias.

Amazon Route 53 se emplea como servicio de DNS para enrutar el tráfico desde Internet al equilibrador de carga de aplicación. Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad.

Detalles de HA

- Bases de datos: la función Multi-AZ de Amazon RDS opera dos bases de datos en varias zonas de disponibilidad con replicación sincrónica. Esto crea un entorno de alta disponibilidad con conmutación por error automática. Amazon RDS cuenta con una función de detección de eventos de conmutación por error, e inicia una conmutación por error automática cuando se producen

dichos eventos. También puede iniciar una conmutación por error manual a través de la API de Amazon RDS. Para obtener una explicación detallada, consulte la entrada del blog Amazon RDS entre bastidores: Multi-AZ. La conmutación por error es fluida, y la aplicación se vuelve a conectar automáticamente a la base de datos cuando se produce. Sin embargo, cualquier trabajo del programador de procesos durante la conmutación por error genera errores y debe volver a enviarse.

- PeopleSoft servidores de aplicaciones: los servidores de aplicaciones están repartidos en múltiples zonas de disponibilidad y tienen un grupo de Auto Scaling definido para ellos. Si una instancia falla, el grupo de escalado automático la reemplaza inmediatamente por una instancia en buen estado que se clona desde la AMI de la plantilla del servidor de aplicaciones. Se habilita la agrupación por descargas de modo que, cuando una instancia del servidor de aplicaciones deja de funcionar, las sesiones se conmutan automáticamente por error a otro servidor de aplicaciones, y el grupo de escalado automático activa automáticamente otra instancia, abre el servidor de aplicaciones y la registra en el montaje de Amazon EFS. El servidor de aplicaciones recién creado se añade automáticamente a los servidores web mediante el script `PSSTRSETUP.SH` de los servidores web. Esto garantiza que el servidor de la aplicación esté siempre altamente disponible y se recupere de los errores con rapidez.
- Programadores de procesos: los servidores de los programadores de procesos están distribuidos en varias zonas de disponibilidad, y tienen un grupo de escalado automático definido para ellos. Si falla una instancia, el grupo de escalado automático la sustituye inmediatamente por una instancia sana clonada a partir de la AMI de la plantilla de servidor del programador de procesos. Cuando una instancia del programador de procesos deja de funcionar, el grupo de escalado automático activa automáticamente otra instancia y abre el programador de procesos. Todos los trabajos que estaban en ejecución cuando la instancia falló deben volver a enviarse. Esto garantiza que el programador de procesos esté disponible en todo momento y se recupere rápidamente de los errores.
- Servidores Elasticsearch: Los servidores Elasticsearch tienen un grupo de escalado automático definido para ellos. Si falla una instancia, el grupo de escalado automático la sustituye inmediatamente por una instancia sana clonada a partir de la AMI de la plantilla del servidor de Elasticsearch. Cuando una instancia de Elasticsearch deja de funcionar, el equilibrador de carga de aplicación que le envía las solicitudes detecta el error y deja de enviarle tráfico. El grupo de escalado automático activa automáticamente otra instancia y abre la instancia de Elasticsearch. Cuando la instancia de Elasticsearch se recupera, el equilibrador de carga de aplicación detecta que está en buen estado y vuelve a enviarle solicitudes. Esto garantiza que el servidor de Elasticsearch esté siempre altamente disponible y se recupere de los errores con rapidez.

- Servidores web: Los servidores web tienen un grupo de escalado automático definido para ellos. Si falla una instancia, el grupo de escalado automático la sustituye inmediatamente por una instancia sana clonada a partir de la AMI de la plantilla del servidor web. En concreto, cuando una instancia de servidor web se cae, el Equilibrador de carga de aplicación que le sirve las peticiones detecta el fallo y deja de enviarle tráfico. El grupo de escalado automático pone en marcha automáticamente otra instancia y pone en marcha la instancia del servidor web. Cuando la instancia del servidor web vuelve a funcionar, el Equilibrador de carga de aplicación detecta que está en buen estado y comienza a enviarle peticiones de nuevo. Esto garantiza que el servidor web esté siempre altamente disponible y se recupere de los errores con rapidez.

Herramientas

Servicios de AWS

- Los Equilibradores de carga de aplicación distribuyen el tráfico entrante de aplicaciones entre varios destinos, tales como instancias EC2, en varias zonas de disponibilidad.
- Amazon Elastic Block Store (Amazon EBS) proporciona volúmenes de almacenamiento por bloques para su uso con instancias de Amazon Elastic Compute Cloud (Amazon EC2).
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon Elastic File System (Amazon EFS) le ayuda a crear y configurar sistemas de archivos compartidos en la nube de AWS.
- Amazon Relational Database Service (Amazon RDS) le ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS.
- Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad.

Prácticas recomendadas

Prácticas operativas recomendadas

- Cuando utilice AWS, utilice Route 53 para enrutar el tráfico desde Internet y de forma local. PeopleSoft Use la opción de conmutación por error para redirigir el tráfico al sitio de recuperación de desastres (DR) si la instancia de base de datos principal no está disponible.

- Utilice siempre un Application Load Balancer delante del PeopleSoft entorno. Esto garantiza que la carga del tráfico se equilibre en los servidores web de forma segura.
- En la configuración del grupo de destino del equilibrador de carga de aplicación, asegúrese de que la adherencia esté activada con una cookie generada por el equilibrador de carga.

  Nota: Es posible que tengas que usar una cookie basada en aplicación si usa un inicio de sesión único (SSO) externo. Esto garantiza que las conexiones sean consistentes entre los servidores web y los servidores de aplicaciones.
- En el caso de una aplicación de PeopleSoft producción, el tiempo de espera de inactividad de Application Load Balancer debe coincidir con el establecido en el perfil web que utilice. Esto evita que las sesiones de usuario caduquen en la capa del equilibrador de carga.
- Para una aplicación PeopleSoft de producción, establezca el recuento de reciclaje del servidor de aplicaciones en un valor que minimice las pérdidas de memoria.
- Si utiliza una base de datos de Amazon RDS para su aplicación de PeopleSoft producción, tal y como se describe en este patrón, ejecútela en formato Multi-AZ para obtener una alta disponibilidad.
- Si la base de datos se ejecuta en una instancia EC2 para la aplicación de PeopleSoft producción, asegúrese de que la base de datos en espera se ejecute en otra zona de disponibilidad para garantizar una alta disponibilidad.
- Para la DR, asegúrese de que la base de datos de Amazon RDS o la instancia de EC2 tengan un modo de espera configurado en una región de AWS independiente de la base de datos de producción. Esto garantiza que, en caso de que se produzca un desastre en la región, pueda cambiar la aplicación a otra región.
- En cuanto a la RD, use Amazon Elastic Disaster Recovery para configurar los componentes de nivel de aplicación en una región distinta de los componentes de producción. Esto garantiza que, en caso de que se produzca un desastre en la región, pueda cambiar la aplicación a otra región.
- Utilice Amazon EFS (para requisitos de E/S moderados) o Amazon FSx (para requisitos de E/S altos) para almacenar PeopleSoft sus informes, archivos adjuntos y archivos de datos. Esto garantiza que el contenido se almacene en una ubicación central y accesible desde cualquier lugar de la infraestructura.
- Utilice Amazon CloudWatch (básico y detallado) para supervisar los recursos de la nube de AWS que utiliza su PeopleSoft aplicación prácticamente en tiempo real. Esto garantiza que reciba alertas de los problemas al instante y pueda solucionarlos rápidamente antes de que afecten a la disponibilidad del entorno.

- Si utiliza una base de datos de Amazon RDS como base de datos, utilice Enhanced Monitoring. PeopleSoft Esta característica proporciona acceso a más de 50 métricas, incluidas CPU, memoria, E/S del sistema de archivos y E/S del disco.
- Utilice AWS CloudTrail para supervisar las llamadas a la API en los recursos de AWS que utiliza su PeopleSoft aplicación. Esto permite realizar análisis de seguridad, seguimiento de los cambios en los recursos y auditorías de conformidad.

Prácticas recomendadas de seguridad

- Para proteger su PeopleSoft aplicación de vulnerabilidades habituales, como la inyección de SQL o el cross-site scripting (XSS), utilice AWS WAF. Considere la posibilidad de usar AWS Shield Avanzado para obtener servicios de detección y mitigación personalizados.
- Agrega una regla al Application Load Balancer para redirigir el tráfico de HTTP a HTTPS automáticamente y así proteger tu PeopleSoft aplicación.
- Configure un grupo de seguridad independiente para el equilibrador de carga de aplicación. Este grupo de seguridad solo debe permitir el tráfico entrante HTTPS/HTTP, y no el tráfico saliente. Esto garantiza que solo se permita el tráfico previsto y ayuda a proteger la aplicación.
- Use subredes privadas para los servidores de aplicaciones, los servidores web y la base de datos, y use puertas de enlace NAT para el tráfico de Internet saliente. Esto garantiza que no se pueda acceder públicamente a los servidores que respaldan la aplicación y, al mismo tiempo, proporciona acceso público solo a los servidores que lo necesitan.
- Utilice diferentes VPC para ejecutar sus entornos de PeopleSoft producción y de no producción. Use AWS Transit Gateway, emparejamiento de VPC, ACL de red y grupos de seguridad para controlar el flujo de tráfico entre las VPC y, si es necesario, su centro de datos en las instalaciones.
- Siga el principio de privilegio mínimo Conceda acceso a los recursos de AWS que utiliza la PeopleSoft aplicación solo a los usuarios que lo necesiten absolutamente. Otorgue únicamente los privilegios mínimos obligatorios para realizar una tarea. Para obtener más información, consulte el pilar de seguridad del Marco de AWS Well-Architected.
- Siempre que sea posible, utilice AWS Systems Manager para acceder a las instancias EC2 que utiliza la PeopleSoft aplicación.

Prácticas recomendadas de fiabilidad

- Cuando utilice un equilibrador de carga de aplicación, registre un único destino para cada zona de disponibilidad habilitada. Esto aumenta la efectividad del equilibrador de carga.

- Le recomendamos que tenga tres URL distintas para cada entorno de PeopleSoft producción: una URL para acceder a la aplicación, otra para servir al agente de integración y otra para ver los informes. Si es posible, cada URL debe tener sus propios servidores web y servidores de aplicaciones dedicados. Este diseño ayuda a que PeopleSoft la aplicación sea más segura, ya que cada URL tiene una funcionalidad distinta y un acceso controlado. También minimiza el alcance del impacto en caso de que los servicios subyacentes fallen.
- Te recomendamos que configures las comprobaciones de estado de los grupos objetivo del balanceador de cargas de tu PeopleSoft aplicación. Las comprobaciones de estado deben realizarse en los servidores web, y no en las instancias EC2 que ejecutan esos servidores. Esto garantiza que si el servidor web se bloquea o la instancia EC2 que aloja el servidor web deja de funcionar, el equilibrador de carga de aplicación refleje esa información con precisión.
- En el caso PeopleSoft de una aplicación de producción, le recomendamos que distribuya los servidores web en al menos tres zonas de disponibilidad. Esto garantiza que la PeopleSoft aplicación siempre tenga una alta disponibilidad, incluso si una de las zonas de disponibilidad deja de funcionar.
- Para una aplicación PeopleSoft de producción, habilite la agrupación de sacudidas ()`joltPooling=true`. Esto garantiza que su aplicación se conmute por error a otro servidor de aplicaciones si un servidor está inactivo por motivos de aplicación de parches o debido a un fallo de la máquina virtual.
- Para una aplicación de PeopleSoft producción, establézcalo en `1DynamicConfigReload` . Esta configuración se admite en la PeopleTools versión 8.52 y versiones posteriores. Añade nuevos servidores de aplicaciones al servidor web de forma dinámica, sin necesidad de reiniciar los servidores.
- Para minimizar el tiempo de inactividad al aplicar PeopleTools parches, utilice el método de despliegue azul/verde para las configuraciones de lanzamiento grupal de Auto Scaling para los servidores web y de aplicaciones. Para obtener más información, consulte el documento técnico Descripción general de las opciones de implementación en AWS.
- Utilice AWS Backup para hacer copias de seguridad de su PeopleSoft aplicación en AWS. AWS Backup es un servicio rentable, totalmente gestionado y basado en políticas que simplifica la protección de datos a escala.

Prácticas recomendadas de rendimiento

- Termine el SSL en el Application Load Balancer para obtener un rendimiento óptimo del PeopleSoft entorno, a menos que su empresa requiera tráfico cifrado en todo el entorno.

- Cree puntos de enlace de VPC de interfaz para los servicios de AWS, como Amazon Simple Notification Service (Amazon SNS) CloudWatch, de forma que el tráfico sea siempre interno. Esto es rentable y ayuda a mantener la aplicación segura.

Prácticas recomendadas de optimización de costos

- Etiquete todos los recursos que utiliza su PeopleSoft entorno y active las etiquetas de asignación de costes. Estas etiquetas le ayudan a ver y gestionar los costos de sus recursos.
- Para una aplicación PeopleSoft de producción, configure los grupos de Auto Scaling para los servidores web y los servidores de aplicaciones. De este modo, mantiene el número mínimo de servidores web y de aplicaciones para dar soporte a su aplicación. Puede usar políticas de grupo de escalado automático para ampliar o reducir los servidores según sea necesario.
- Use alarmas de facturación para recibir alertas cuando los costos superen el umbral presupuestario que especifique.

Prácticas recomendadas de sostenibilidad

- Utilice la infraestructura como código (IaC) para mantener sus PeopleSoft entornos. Esto permite crear entornos coherentes y a mantener el control de los cambios.

Epics

Migre su PeopleSoft base de datos a Amazon RDS

Tarea	Descripción	Habilidades requeridas
Creación de un grupo de subredes de base de datos.	En la consola de Amazon RDS, en el panel de navegación, elija Grupos de subred y, a continuación, cree un grupo de subredes de base de datos de Amazon RDS con subredes en varias zonas de disponibilidad. Esto es necesario para que la base de datos de Amazon RDS se	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	ejecute en una configuración Multi-AZ.	
Crear la base de datos de Amazon RDS.	Cree una base de datos de Amazon RDS en una zona de disponibilidad de la región de AWS que haya seleccionado para el entorno de PeopleSoft alta disponibilidad. Al crear la base de datos de Amazon RDS, asegúrese de seleccionar la opción Multi-AZ (crear una instancia en espera) y el grupo de subredes de la base de datos que creó en el paso anterior. Para obtener más información, consulte la documentación de Amazon RDS.	Administrador de la nube, administrador de bases de datos de Oracle
Migre su PeopleSoft base de datos a Amazon RDS.	Migre su PeopleSoft base de datos existente a la base de datos de Amazon RDS mediante AWS Database Migration Service (AWS DMS). Para más información, consulte la documentación de AWS DMS y la publicación del blog de AWS Migración de bases de datos de Oracle con un tiempo de inactividad casi nulo mediante AWS DMS.	Administrador de nube, administrador de bases de datos PeopleSoft

Configure su sistema de archivos Amazon EFS

Tarea	Descripción	Habilidades requeridas
Cree un sistema de archivos.	En la consola de Amazon EFS, cree un sistema de archivos y monte los destinos para cada zona de disponibilidad. Para obtener instrucciones, consulte la documentación de Amazon EFS. Cuando haya creado el sistema de archivos, anote su nombre de DNS. Usará esta información cuando monte el sistema de archivos.	Administrador de la nube

Configure su PeopleSoft aplicación y su sistema de archivos

Tarea	Descripción	Habilidades requeridas
Lanzar una instancia EC2.	Lance una instancia EC2 para su PeopleSoft aplicación. Para obtener instrucciones, consulte la documentación de Amazon EC2. • En Nombre, escriba `APP_TEMPLATE` . • En imágenes de SO, seleccione Red Hat. • En Tipo de instancia, elija el tipo de instancia adecuado para su PeopleSoft aplicación. Para obtener más información, consulte los	Administrador de la nube, PeopleSoft administrador

Tarea	Descripción	Habilidades requeridas
	Detalles de arquitectura en la sección Arquitectura.	
Instálelo PeopleSoft en la instancia.	Instale PeopleSoft la aplicación y PeopleTools en la instancia EC2 que creó. Para obtener instrucciones, consulte la documentación de Oracle.	Administrador de la nube, PeopleSoft administrador
Crear el servidor de la aplicación.	Cree el servidor de aplicaciones para la plantilla de AMI y asegúrese de que se conecta correctamente a la base de datos de Amazon RDS.	Administrador de la nube, PeopleSoft administrador

Tarea	Descripción	Habilidades requeridas
Monte el sistema de archivos de Amazon EFS.	Inicie sesión en la instancia EC2 como usuario raíz y ejecute los siguientes comandos para montar el sistema de archivos de Amazon EFS en una carpeta llamada PSFTMNT en el servidor. `sudo su -` `mkdir /psftmnt` `cat /etc/fstab` Añada la línea siguiente al archivo `/etc/fstab` . Use el nombre de DNS que anotó al crear el sistema de archivos. `fs-09e064308f11453 88.efs.us-east-1.a mazonaws.com:/ / psftmnt nfs4 nfsvers=4 .1,rsize=1048576,w size=1048576,hard, timeo=600,retrans= 2,noresvport,_netdev 0 0` `mount -a`	Administrador de la nube, PeopleSoft administrador
Comprobar permisos.	Asegúrese de que la PSFTMNT carpeta tenga los permisos adecuados para que el PeopleSoft usuario pueda acceder a ella correctamente.	Administrador de la nube, PeopleSoft administrador

Tarea	Descripción	Habilidades requeridas
Cree instancias adicionales.	Repita los pasos anteriores de esta épica para crear instancias de plantilla para el programador de procesos, el servidor web y el servidor Elasticsearch. Nombre estas instancias como `PRCS_TEMPLATE` , `WEB_TEMPLATE` y `SRCH_TEMPLATE` . En el servidor web, defina `joltPooling=true` y `DynamicConfigReload=1` .	Administrador de la nube, PeopleSoft administrador

Cree scripts para configurar los servidores

Tarea	Descripción	Habilidades requeridas
Cree un script para instalar el servidor de aplicaciones.	En la `APP_TEMPLATE` instancia de Amazon EC2, cree el siguiente script como PeopleSoft usuario. Asígnele el nombre `appstart.sh` y colóquelo en el directorio `PS_HOME`. Usará este script para abrir el servidor de aplicaciones y también para registrar el nombre del servidor en el soporte de Amazon EFS. `#!/bin/ksh` `. /usr/homes/hcmdemo/.profile.`	PeopleSoft administrador

Tarea	Descripción	Habilidades requeridas
	`psadmin -c configure -d HCMDEMO` `psadmin -c parallelboot -d HCMDEMO` `touch /psftmnt/`echo $HOSTNAME`	
Cree un script para instalar el servidor de programador de procesos.	En la `PRCS_TEMPLATE` instancia de Amazon EC2, cree el siguiente script como PeopleSoft usuario. Asígnele el nombre `prcsstart.sh` y colóquelo en el directorio `PS_HOME`. Usará este script para abrir el servidor de programador de procesos. `#!/bin/ksh` `. /usr/homes/hcmdemo/.profile` `/* The following line ensures that the process scheduler always has a unique name during replacement or scaling activity. */` `sed -i "s/.*PrcsServerName.*/`hostname -I | awk -F. '{print "PrcsServerName=PSUNX"$3$4}'`/" $HOME/appserv/prcs/*/psprcs.cfg` `psadmin -p configure -d HCMDEMO` `psadmin -p start -d HCMDEMO`	PeopleSoft administrador

Tarea	Descripción	Habilidades requeridas
Cree un script para instalar el servidor Elasticsearch.	En la instancia `SRCH_TEMPLATE` de Amazon EC2, como usuario de Elasticsearch, cree el siguiente script. Asígnele el nombre `srchstart.sh` y colóquelo en el directorio `HOME`. `#!/bin/ksh` `/* The following line ensures that the correct IP is indicated in the elasticsearch.yaml file. */` `sed -i "s/.*network.host.*/`hostname -I	awk '{print "host:"$0}'`/" $ES_HOME_DIR/config/elasticsearch.yaml` `nohup $ES_HOME_DIR/bin/elasticsearch &`	PeopleSoft administrador

Tarea	Descripción	Habilidades requeridas
Cree un script para instalar el servidor web.	En la instancia `WEB_TEMPLATE` de Amazon EC2, como usuario del servidor web, cree los siguientes scripts en el directorio `HOME`. `renip.sh`: este script garantiza que el servidor web tenga la IP correcta cuando se clone desde la AMI. `#!/bin/ksh` `hn=`hostname`` `/* On the following line, change the IP with the hostname with the hostname of the web template. */` `for text_file in `find * -type f -exec grep -l '<hostname-of-the-web-template>' {} \;` `do` `sed -e 's/<hostname-of-the-web-template>/'$hn'/g' $text_file > temp` `mv -f temp $text_file` `done`  `psstrsetup.sh` : este script garantiza que el servidor web utilice las direcciones IP correctas del servidor de aplicaciones actualmente en ejecución. Intenta conectarse a cada servidor de aplicaciones en el puerto de descarga	PeopleSoft administrador

Tarea	Descripción	Habilidades requeridas
	y lo añade al archivo de configuración. `#!/bin/ksh` `c2=""` `for ctr in `ls -1 /psftmnt/*.internal`do` `c1=`echo $ctr | awk -F "/" '{print $3}'`/* In the following lines, 9000 is the jolt port. Change it if necessary. */` `if nc -z $c1 9000 2> /dev/null; then` `if [[ $c2 = "" ]]; then` `c2="psserver="`echo $c1`":9000"` `else` `c2=`echo $c2`","`echo $c1`":9000"` `fi` `fi` `done` `webstart.sh` : este script ejecuta los dos scripts anteriores e inicia los servidores web. `#!/bin/ksh` `/* Change the path in the following if necessary. */` `cd /usr/homes/hcmdemo` `./renip.sh` `./psstrsetup.sh`	

Tarea	Descripción	Habilidades requeridas
	`webserv/peoplesoft/bin/startPIA.sh`	
Añada una entrada de crontab.	En la instancia de Amazon EC2 `WEB_TEMPLATE` , como usuario del servidor web, añada la siguiente línea a crontab. Cambie la hora y la ruta para reflejar los valores que necesita. Esta entrada garantiza que su servidor web siempre tenga las entradas correctas del servidor de aplicaciones en el archivo `configuration.properties` . `* * * * * /usr/homes/hcmdemo/psstrsetup.sh`	PeopleSoft administrador

Cree plantillas de grupo de escalado automático y AMI

Tarea	Descripción	Habilidades requeridas
Cree una AMI para la plantilla del servidor de aplicaciones.	En la consola de Amazon EC2, cree una imagen de AMI de la instancia `APP_TEMPLATE` de Amazon EC2. Ponga el nombre `PSAPPSRV-SCG-VER1` a la AMI. Para obtener instrucciones, consulte la documentación de Amazon EC2.	Administrador de la nube, PeopleSoft administrador

Tarea	Descripción	Habilidades requeridas
Cree AMI para el resto de servidores.	Repita el paso anterior para crear AMIs para el programador de procesos, el servidor Elasticsearch y el servidor web.	Administrador de la nube, PeopleSoft administrador

Tarea	Descripción	Habilidades requeridas
Cree una plantilla de lanzamiento para el grupo de escalado automático del servidor de aplicaciones.	Cree una plantilla de lanzamiento para el grupo de escalado automático del servidor de aplicaciones. Asigne el nombre `PSAPPSRV_TEMPLATE.` a la plantilla. En la plantilla, elija la AMI que creó para la instancia `APP_TEMPLATE` . Para obtener instrucciones, consulte la documentación de Amazon EC2. • En la plantilla de lanzamiento, seleccione el tipo de instancia según sus requisitos. • En el campo Datos de usuario de la sección Detalles avanzados, añada las siguientes entradas. Asegúrese de que la ruta y la información del usuario sean correctas. Ha creado el script `appstart.sh` en un paso anterior. `#! /bin/ksh` `su -c “/usr/homes/hcmdemo/appstart.sh” - hcmdemo`	Administrador de la nube, PeopleSoft administrador

Tarea	Descripción	Habilidades requeridas
Cree una plantilla de lanzamiento para el grupo de escalado automático del servidor de programación de procesos.	Repita el paso anterior para crear una plantilla de lanzamiento para el grupo de escalado automático del servidor programador de procesos. Asigne un nombre a la plantilla `PSPRCS_TEMPLATE` . En la plantilla, elija la AMI que creó para el programador de procesos. • En el campo Datos de usuario de la sección Detalles avanzados, añada las siguientes entradas. Asegúrese de que la ruta y la información del usuario sean correctas. Ha creado el script `prcsstart.sh` en un paso anterior. `#! /bin/ksh` `su -c “/usr/homes/hcmdemo/prcsstart.sh” - hcmdemo`	Administrador de la nube, PeopleSoft administrador

Tarea	Descripción	Habilidades requeridas
Cree una plantilla de lanzamiento para el grupo de escalado automático del servidor de Elasticsearch.	Repita los pasos anteriores para crear una plantilla de lanzamiento para el grupo de escalado automático del servidor Elasticsearch. Asigne un nombre a la plantilla `SRCH_TEMPLATE` . En la plantilla, elija la AMI que creó para el servidor de búsqueda. • En el campo Datos de usuario de la sección Detalles avanzados, añada las siguientes entradas. Asegúrese de que la ruta y la información del usuario sean correctas. Ha creado el script `srchstart.sh` en un paso anterior. `#! /bin/ksh` `su -c “/usr/hom` `es/essearch/srchst` `art.sh” - essearch`	Administrador de la nube, PeopleSoft administrador

Tarea	Descripción	Habilidades requeridas
Cree una plantilla de lanzamiento para el grupo de escalado automático del servidor web.	Repita los pasos anteriores para crear una plantilla de lanzamiento para el grupo de escalado automático del servidor web. Asigne un nombre a la plantilla `WEB_TEMPLATE` . En la plantilla, elija la AMI que creó para el servidor web. • En el campo Datos de usuario de la sección Detalles avanzados, añada las siguientes entradas. Asegúrese de que la ruta y la información del usuario sean correctas. Ha creado el script `webstart.sh` en un paso anterior. `#! /bin/ksh` `su -c “/usr/homes/hcmdemo/webstart.sh” - hcmdemo`	Administrador de la nube, PeopleSoft administrador

Crear grupos de escalado automático

Tarea	Descripción	Habilidades requeridas
Cree un grupo de escalado automático para el servidor de aplicaciones.	En la consola de Amazon EC2, cree un grupo de escalado automático llamado `PSAPPSRV_ASG` para el servidor de aplicaciones	Administrador de la nube, PeopleSoft administrador

Tarea	Descripción	Habilidades requeridas
	usando la plantilla `PSAPPSRV_TEMPLATE` . Para obtener instrucciones, consulte la documentación de Amazon EC2. • En la página Elegir opciones de lanzamiento de instancias, seleccione la VPC correcta y, a continuación, seleccione varias subredes de distintas zonas de disponibilidad. • En la página Configurar opciones avanzadas, no seleccione ningún equilibrador de carga. • En la página Configurar tamaño de grupo y políticas de escalado, seleccione los ajustes en función de la carga para la que desee diseñar el sistema y de si desea utilizar una política de escalado. Le recomendamos que establezca la capacidad mínima deseada en 2, como mínimo, para que haya al menos una instancia disponible para atender el tráfico en cualquier momento. Para más información sobre las políticas de escalado automático, consulte la	

Tarea	Descripción	Habilidades requeridas
	documentación de Amazon EC2.	
Cree grupos de escalado automático en el resto de servidores.	Repita el paso anterior para crear grupos de escalado automático para el programador de procesos, el servidor Elasticsearch y el servidor web.	Administrador de la nube, PeopleSoft administrador

Cree y configure grupos de destino

Tarea	Descripción	Habilidades requeridas
Cree un grupo de destino para el servidor web.	En la consola de Amazon EC2, cree un grupo de destino para el servidor web. Para obtener más instrucciones, consulte la documentación de Elastic Load Balancing. Establezca el puerto en el que escucha el servidor web.	Administrador de la nube
Configurar comprobaciones de estado.	Confirme que las comprobaciones de estado tengan los valores correctos según los requisitos de su empresa. Para obtener más información, consulte la Documentación de Elastic Load Balancing.	Administrador de la nube
Cree un grupo de destino para el servidor Elasticsearch.	Repita los pasos anteriores para crear un grupo de destino llamado PSFTSRCH para el servidor de Elasticse	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	arch, y configure el puerto de Elasticsearch correcto.	
Añada grupos de destino a los grupos de escalado automático.	Abra el grupo de escalado automático `PSPIA_ASG` que creó anteriormente. En la pestaña Equilibrador de carga, elija Editar y, a continuación, añada el grupo de destino `PSFTWEB` al grupo de escalado automático. Repite este paso para el grupo de escalado automático de Elasticsearch `PSSRCH_ASG` y añada el grupo objetivo `PSFTSRCH` que creó anteriormente.	Administrador de la nube
Establezca la adherencia de la sesión.	En el grupo de destino `PSFTWEB`, seleccione la pestaña Atributos, elija Editar y defina la adherencia de la sesión. En el tipo de adherencia, seleccione Cookie generada por el equilibrador de carga, y establezca la duración en 1. Para obtener más información, consulte la Documentación de Elastic Load Balancing. Repita este paso para el grupo de destino `PSFTSRCH`.	Administrador de la nube

Crear y configurar equilibradores de carga de aplicaciones

Tarea	Descripción	Habilidades requeridas
Crear un equilibrador de carga para los servidores web.	Cree un equilibrador de carga de aplicación con el nombre `PSFTLB` para equilibrar la carga del tráfico a los servidores web. Para obtener más instrucciones, consulte la documentación de Elastic Load Balancing. • Proporcione el nombre del equilibrador de carga. • En Scheme, elija Internet-facing. • En la sección Mapeo de redes, seleccione la VPC correcta y, al menos, dos subredes públicas de distintas zonas de disponibilidad. • En la sección de Escucha y enrutamiento, seleccione el grupo de destino `PSFTWEB` y especifique el protocolo y el número de puerto.	Administrador de la nube
Cree un equilibrador de carga para los servidores de Elasticsearch.	Cree un equilibrador de carga de aplicación con el nombre `PSFTSCH` para equilibrar la carga del tráfico a los servidores de Elasticsearch. • Proporcione el nombre del equilibrador de carga.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	• En Esquema, seleccione Interno. • En la sección Mapeo de redes, seleccione la VPC y las subredes privadas correctas. • En la sección de Escucha y enrutamiento, seleccione el grupo de destino `PSFTSRCH` y especifique el protocolo y el número de puerto.	
Configure Route 53.	En la consola Amazon Route 53, cree un registro en la zona alojada que servirá a la PeopleSoft aplicación. Para obtener instrucciones, consulte la documentación de Amazon Route 53. Esto garantiza que todo el tráfico pase por el equilibrador de carga `PSFTLB`.	Administrador de la nube

Recursos relacionados

- PeopleSoft Sitio web de Oracle
- Documentación de AWS

Más patrones

- Implementar una aplicación agrupada en Amazon ECS con AWS Copilot
- Despliega canarios de CloudWatch Synthetics con Terraform
- Documente el conocimiento institucional a partir de las entradas de voz mediante Amazon Bedrock y Amazon Transcribe

Nativo en la nube

Temas

- Cree una canalización de procesamiento de vídeo con Amazon Kinesis Video Streams y AWS Fargate
- Supervise los clústeres de SAP RHEL Pacemaker mediante los servicios de AWS
- Importación correcta de un bucket de S3 como CloudFormation pila de AWS
- Más patrones

Cree una canalización de procesamiento de vídeo con Amazon Kinesis Video Streams y AWS Fargate

Documento creado por Piotr Chotkowski (AWS) y Pushparaju Thangavel (AWS)

Entorno: PoC o piloto	Tecnologías: nativas en la nube; desarrollo y pruebas de software; servicios multimedia	Servicios de AWS: AWS Fargate; Amazon Kinesis; Amazon S3

Resumen

Este patrón muestra cómo utilizar Amazon Kinesis Video Streams y AWS Fargate para extraer fotogramas de una transmisión de vídeo y almacenarlos como archivos de imagen en Amazon Simple Storage Service (Amazon S3) para su posterior procesamiento.

El patrón proporciona una aplicación de muestra en forma de proyecto Java Maven. Esta aplicación define la infraestructura de AWS mediante AWS Cloud Development Kit (AWS CDK). Tanto la lógica de procesamiento de fotogramas como las definiciones de infraestructura están escritas en el lenguaje de programación Java. Puede utilizar esta aplicación de muestra como base para desarrollar su propia canalización de procesamiento de vídeo en tiempo real o para crear la etapa de preprocesamiento de vídeo de una canalización con machine learning.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Java SE Development Kit (JDK) 11, instalado
- Apache Maven, instalado
- AWS Cloud Development Kit (AWS CDK), instalado
- Interfaz de la línea de comandos de AWS (AWS CLI) versión 2, instalada
- Docker (necesario para compilar imágenes de Docker con el fin de utilizarlas en las definiciones de tareas de AWS Fargate), instalado

Limitaciones

Este patrón está concebido como prueba de concepto o como base para un desarrollo futuro. No se debe utilizar en su forma actual para implementaciones de producción.

Versiones del producto

- Este patrón se ha probado con la versión 1.77.0 de AWS CDK (consulte las versiones de AWS CDK)
- JDK 11
- CLI de AWS versión 2

Arquitectura

Pila de tecnología de destino

- Amazon Kinesis Video Streams
- Tarea de AWS Fargate
- Cola de Amazon Simple Queue Service (Amazon SQS)
- Bucket S3 de Amazon

Arquitectura de destino

El usuario crea una transmisión de vídeo de Kinesis, carga un vídeo y envía un mensaje JSON que contiene detalles sobre la transmisión de vídeo de Kinesis de entrada y el bucket S3 de salida a una cola de SQS. AWS Fargate, que ejecuta la aplicación principal en un contenedor, extrae el mensaje de la cola de SQS y comienza a extraer los fotogramas. Cada fotograma se guarda en un archivo de imagen y se almacena en el bucket S3 de destino.

Automatizar y escalar

La aplicación de muestra se puede escalar tanto horizontal como verticalmente dentro de una misma Región de AWS. El escalado horizontal se puede lograr aumentando el número de tareas de AWS Fargate implementadas que leen de la cola de SQS. El escalado vertical se puede lograr aumentando el número de subprocesos de división de fotogramas y publicación de imágenes en la aplicación. Estos ajustes se transfieren como variables de entorno a la aplicación en la definición del QueueProcessingFargateServicerecurso en la CDK de AWS. Gracias al diseño de implementación

de la pila de AWS CDK, puede implementar esta aplicación en varias regiones y cuentas de AWS sin ningún esfuerzo adicional.

Herramientas

Herramientas

- AWS CDK es un marco de desarrollo de software para definir la infraestructura y los recursos de la nube mediante lenguajes de programación como Python TypeScript JavaScript, Java y C#/.Net.
- Amazon Kinesis Video Streams es un servicio de AWS completamente administrado que puede utilizar para transmitir vídeos en directo desde dispositivos a la nube de AWS, o bien crear aplicaciones para el procesamiento de vídeo en tiempo real o el análisis de vídeo orientado a lotes.
- AWS Fargate es un motor de cómputo sin servidor para contenedores. Fargate elimina la necesidad de aprovisionar y administrar servidores y le permite centrarse en el desarrollo de sus aplicaciones.
- Amazon S3: es un servicio de almacenamiento de objetos de AWS que ofrece escalabilidad, disponibilidad de datos, seguridad y rendimiento.
- Amazon SQS es un servicio de colas de mensajes completamente administrado que permite el desacople y el escalado de microservicios, sistemas distribuidos y aplicaciones sin servidor.

Código

- Se adjunta un archivo .zip del proyecto de la aplicación de muestra (`frame-splitter-code.zip`).

Epics

Despliegue de la infraestructura

Tarea	Descripción	Habilidades requeridas
Iniciar el daemon de Docker.	Inicie el daemon de Docker en su sistema local. El AWS CDK usa Docker para crear la imagen que se utiliza en la tarea de AWS Fargate.	Desarrollador, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
	Debe ejecutar Docker antes de continuar con el siguiente paso.	
Compilar el proyecto.	Descargue la aplicación de muestra `frame-splitter-code` (adjunta) y extraiga su contenido en una carpeta de su máquina local. Antes de poder implementar la infraestructura, debe crear el proyecto Java Maven. En el símbolo del sistema, navegue hasta el directorio raíz del proyecto y compile el proyecto ejecutando el comando: `mvn clean install`	Desarrollador, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Arrancar el AWS CDK.	(Solo para usuarios iniciales de AWS CDK) Si es la primera vez que utiliza AWS CDK, es posible que tenga que que arrancar el entorno mediante la ejecución del comando AWS CLI: `cdk bootstrap --profile "$AWS_PROFILE_NAME"` donde `$AWS_PROFILE_NAME` contiene el nombre del perfil de AWS obtenido de sus credenciales de AWS. O bien, puede eliminar este parámetro para utilizar el perfil predeterminado. Para obtener más información, consulte la documentación de AWS CDK.	Desarrollador, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Implementar la pila de AWS CDK.	En este paso, debe crear los recursos de infraestructura necesarios (cola de SQS, bucket S3, definición de tareas de AWS Fargate) en su cuenta de AWS, crear la imagen de Docker necesaria para la tarea de AWS Fargate e implementar la aplicación. En el símbolo del sistema, navegue hasta el directorio raíz del proyecto y ejecute el comando: `cdk deploy --profile "$AWS_PROFILE_NAME" --all` donde `$AWS_PROFILE_NAME` contiene el nombre del perfil de AWS obtenido de sus credenciales de AWS. O bien, puede eliminar este parámetro para utilizar el perfil predeterminado. Confirme la implementación. Anote los valores QueueUrly Bucket del resultado de la implementación del CDK; los necesitará en pasos posteriores. El AWS CDK crea los activos, los carga en su cuenta de AWS y crea todos los recursos de infraestructura.	Desarrollador, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
	Puede observar el proceso de creación de recursos en la CloudFormation consola de AWS. Para obtener más información, consulte la CloudFormation documentación de AWS y la documentación de AWS CDK.	

Tarea	Descripción	Habilidades requeridas
Cree una transmisión de vídeo.	En este paso, creará una transmisión de vídeo de Kinesis que servirá como transmisión de entrada para el procesamiento de vídeo. Asegúrese de que ha instalado y configurado la AWS CLI. En la AWS CLI, ejecute: `aws kinesisvideo --profile "$AWS_PROFILE_NAME" create-stream --stream-name "$STREAM_NAME" --data-retention-in-hours "24"` donde `$AWS_PROFILE_NAME` contiene el nombre del perfil de AWS obtenido de sus credenciales de AWS (o elimine este parámetro para utilizar el perfil predeterminado) y `$STREAM_NAME` es cualquier nombre de transmisión válido. Como alternativa, puede crear una transmisión de vídeo mediante la consola de Kinesis siguiendo los pasos indicados en la documentación de Kinesis Video Streams. Anote el nombre de recurso de AWS (ARN)	Desarrollador, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	de la transmisión creada; lo necesitará más adelante.	

Ejecute un ejemplo

Tarea	Descripción	Habilidades requeridas
Subir el vídeo a la transmisión.	En la carpeta del proyecto de la aplicación de muestra `frame-splitter-code`, abra el archivo `ProcessingTaskTest.java` en la carpeta `src/test/java/amazon/awscdk/examples/splitter`. Sustituya las variables `profileName` y `streamName` por los valores que utilizó en los pasos anteriores. Para cargar el vídeo de muestra en la transmisión de vídeo de Kinesis que ha creado en el paso anterior, ejecute: `amazon.awscdk.examples.splitter.ProcessingTaskTest#testExample test` Como alternativa, puede cargar el vídeo mediante uno de los métodos descritos en la documentación de Kinesis Video Streams.	Desarrollador, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Iniciar el procesamiento de vídeo.	Ahora que ha cargado un vídeo a la transmisión de vídeo de Kinesis, puede empezar a procesarlo. Para iniciar la lógica de procesami ento, debe enviar un mensaje con detalles a la cola de SQS que el AWS CDK creó durante la implementación. Para enviar un mensaje utilizando la AWS CLI, ejecute: `aws sqs --profile "$AWS_PROFILE_NAME" send-message --queue-url QUEUE_URL --message-body MESSAGE` where `$AWS_PROFILE_NAME` contiene el nombre del perfil de AWS de sus credenciales de AWS (elimine este parámetro para usar el perfil predeterminado), `QUEUE_URL` es el `QueueUrl`valor de la salida de la CDK de AWS y `MESSAGE` es una cadena JSON con el siguiente formato: `{ "streamARN": "STREAM_ARN", "bucket": "BUCKET_NAME", "s3Directory": "test-output" }`	Desarrollador, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
	donde `STREAM_ARN` es el ARN de la transmisión de vídeo que ha creado en un paso anterior y `BUCKET_NAME` es el valor de Bucket obtenido de la salida de AWS CDK. Al enviar este mensaje, se inicia el procesamiento del vídeo. Como alternativa, puede enviar un mensaje mediante la consola de Amazon SQS, tal y como se describe en la documentación de Amazon SQS.	
Ver imágenes de los fotogramas de vídeo.	Puede ver las imágenes resultantes en el bucket de salida de S3 `s3://BUCKET_NAME/test-output` donde `BUCKET_NAME` es el valor del Bucket obtenido de la salida de AWS CDK.	Desarrollador, DevOps ingeniero

Recursos relacionados

- Documentación de AWS SDK
- Referencia de la API de AWS CDK
- Taller introductorio sobre AWS CDK
- Documentación de Amazon Kinesis Video Streams
- Ejemplo: identificación de objetos en transmisiones de vídeo mediante SageMaker
- Ejemplo: Análisis y renderización de fragmentos de Kinesis Video Streams

- Analice vídeos en directo a escala y en tiempo real con Amazon Kinesis Video Streams y SageMaker Amazon (entrada del blog AWS Machine Learning)
- Introducción de AWS Fargate

Información adicional

Cómo elegir un IDE

Le recomendamos que utilice su IDE de Java favorito para crear y explorar este proyecto.

Limpieza

Cuando termine de ejecutar este ejemplo, elimine todos los recursos implementados para evitar incurrir en costos de infraestructura de AWS adicionales.

Para eliminar la infraestructura y la transmisión de vídeo, utilice estos dos comandos en la AWS CLI:

```
cdk destroy --profile "$AWS_PROFILE_NAME" --all
```

```
aws kinesisvideo --profile "$AWS_PROFILE_NAME" delete-stream --stream-arn "$STREAM_ARN"
```

Como alternativa, puede eliminar los recursos manualmente mediante la CloudFormation consola de AWS para eliminar la CloudFormation pila de AWS y la consola Kinesis para eliminar la transmisión de vídeo de Kinesis. Tenga en cuenta que `cdk destroy` no elimina el bucket S3 de salida ni las imágenes de los repositorios de Amazon Elastic Container Registry (Amazon ECR) (`aws-cdk/assets`). Debe eliminarlos manualmente.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Supervise los clústeres de SAP RHEL Pacemaker mediante los servicios de AWS

Creado por Harsh Toria (AWS), Randy Germann (AWS) y RAVEENDRA Voore (AWS)

Entorno: producción	Tecnologías: nativas de la nube; infraestructura; sistemas operativos	Carga de trabajo: SAP
Servicios de AWS: Amazon CloudWatch; Amazon SNS; Amazon Logs CloudWatch		

Resumen

Este patrón describe los pasos para monitorear y configurar las alertas de un clúster Pacemaker de Red Hat Enterprise Linux (RHEL) para aplicaciones SAP y servicios de bases de datos SAP HANA mediante Amazon y CloudWatch Amazon Simple Notification Service (Amazon SNS).

La configuración le permite monitorear los recursos del clúster SAP SCS o ASCS, Enqueue Replication Server (ERS) y SAP HANA cuando se encuentran en estado «detenido» con la ayuda de flujos de CloudWatch registro, filtros de métricas y alarmas. Amazon SNS envía un correo electrónico a la infraestructura o al equipo de SAP Basis sobre el estado del clúster detenido.

Puede crear los AWS recursos para este patrón mediante AWS CloudFormation scripts o consolas de AWS servicio. Este patrón presupone que está utilizando las consolas; no proporciona CloudFormation scripts ni cubre el despliegue de infraestructura para CloudWatch Amazon SNS. Los comandos Pacemaker se utilizan para establecer la configuración de alertas del clúster.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Amazon SNS está configurado para enviar notificaciones por correo electrónico o móvil.

- Un clúster SAP ASCS/ERS para ABAP o SCS/ERS para Java y un clúster SAP HANA Database RHEL Pacemaker. Para obtener instrucciones, consulte lo siguiente:
  - Configuración de un clúster de SAP HANA
  - Configuración del clúster ABAP/Java de SAP Netweaver

Limitaciones

- Actualmente, esta solución funciona con los clústeres basados en Pacemaker de RHEL, versión 7.3 y posteriores. No se ha probado en los sistemas operativos SUSE.

Versiones de producto

- RHEL 7.3 y versiones posteriores

Arquitectura

Pila de tecnología de destino

- RHEL Pacemaker alerta a un agente impulsado por eventos
- Amazon Elastic Compute Cloud (Amazon EC2)
- CloudWatch alarma
- CloudWatch grupo de registros y filtro de métricas
- Amazon SNS

Arquitectura de destino

El siguiente diagrama ilustra los componentes y los flujos de trabajo de esta solución.

Automatizar y escalar

- Puede automatizar la creación de AWS recursos mediante CloudFormation scripts. También puede usar filtros de métricas adicionales para escalar y cubrir varios clústeres.

Herramientas

Servicios de AWS

- Amazon le CloudWatch ayuda a supervisar las métricas de sus AWS recursos y las aplicaciones en las que se ejecuta AWS en tiempo real.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluyendo los servidores web y las direcciones de correo electrónico.

Herramientas

- CloudWatch El agente (unificado) es una herramienta que recopila métricas, registros y rastreos a nivel del sistema de las instancias de EC2 y recupera métricas personalizadas de sus aplicaciones.
- El agente de alertas Pacemaker (para RHEL 7.3 y versiones posteriores) es una herramienta que inicia una acción cuando se produce un cambio, como cuando un recurso se detiene o se reinicia, en un clúster de Pacemaker.

Prácticas recomendadas

- Para conocer las mejores prácticas sobre el uso de cargas de trabajo de SAP enAWS, consulte SAP Lens for the AWS Well-Architected Framework.
- Tenga en cuenta los costos que implica configurar la CloudWatch supervisión de los clústeres de SAP HANA. Para obtener más información, consulte la CloudWatch documentación.
- Considere la posibilidad de utilizar un localizador o un mecanismo de venta de entradas para las alertas de Amazon SNS.
- Compruebe siempre si hay versiones de alta disponibilidad (HA) de RHEL del paquete RPM para ordenadores, Pacemaker y Fencing Agent. AWS

Epics

Configurar Amazon SNS

Tarea	Descripción	Habilidades requeridas
Cree un tema de SNS.	1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home. 2. En el panel de Amazon SNS, en Common actions (Acciones comunes), elija Create Topic (Crear tema). 3. En el cuadro de diálogo Crear tema nuevo, en Tipo, elija Estándar. 4. En Nombre del tema, introduzca un nombre para el tema (por ejemplo,`my-topic`). 5. Elija Crear nuevo tema. Esto crea un tema de SNS con una política de recursos que le permite publicar notificaciones. 6. Copie el ARN del tema (por ejemplo,`arn:aws:sns:us-east-1:111122223333:my-topic`). Utilizará este ARN en un paso posterior.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Modifique la política de acceso del tema SNS.	1. En la consola Amazon SNS, en el panel de navegación, elija Temas y, a continuación, elija el tema que ha creado. 2. Seleccione Editar y vaya a la sección Política de acceso. 3. Asegúrese de que la política de acceso incluya CloudWatch uno de los directores de servicio a los que se les permite publicar en este tema. Por ejemplo: `{ "Sid": "Allow AWS CloudWatch to Publish to this SNS topic", "Effect": "Allow", "Principal": { "Service": [ "cloudwatch.amazonaws.com" ] }, "Action": "SNS:Publish", "Resource": "arn:aws:sns:us-east-1:111122223333:my-topic" }` 4. Elija Guardar cambios.	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
Suscríbase al tema de SNS.	1. En la consola Amazon SNS, en el panel de navegación, seleccion a Suscripciones, Crear suscripción. 2. En el ARN del tema, pegue el ARN que creó en la primera tarea. 3. En Protocolo, elija Correo electrónico. 4. En el caso de Endpoint, introduzca la dirección de correo electrónico de la persona o el equipo responsable del clúster de SAP Pacemaker y que debe recibir las notificac iones. Por ejemplo, puede ser la dirección de correo electrónico de la lista de distribución de SAP Basis o del equipo de infraestr uctura. 5. Seleccione Crear suscripci ón. 6. Desde su aplicación de correo electrónico, abra el mensaje de Notificac iones de AWS y confirme la suscripción.	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	El navegador web muestra una respuesta de confirmación de Amazon SNS.	

Confirme la configuración del clúster

Tarea	Descripción	Habilidades requeridas
Compruebe el estado del clúster.	Utilice el comando pcs status para confirmar que los recursos están en línea.	Administrador de SAP Basis

Configure las alertas de Pacemaker

Tarea	Descripción	Habilidades requeridas
Configure el agente de alertas Pacemaker en la instancia del clúster principal.	Inicie sesión en la instancia EC2 del clúster principal y ejecute los siguientes comandos: `install --mode=0755 /usr/share/pacemaker/alerts/alert_file.sh.sample` `touch /var/lib/pacemaker/alert_file.sh` `touch /var/log/pcmk_alert_file.log` `chown hacluster:haclient /var/log/pcmk_alert_file.log` `chmod 600 /var/log/pcmk_alert_file.log`	Administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas
	`pcs alert create id=alert_file description="Log events to a file." path=/var/lib/pacemaker/alert_file.sh` `pcs alert recipient add alert_file id=my-alert_logfile value=/var/log/pcmk_alert_file.log`	
Configure el agente de alertas Pacemaker en la instancia del clúster secundario.	Inicie sesión en la instancia EC2 del clúster secundario del clúster secundario y ejecute los siguientes comandos: `install --mode=0755 /usr/share/pacemaker/alerts/alert_file.sh.sample /var/lib/pacemaker/alert_file.sh` `touch /var/log/pcmk_alert_file.log` `chown hacluster:haclient /var/log/pcmk_alert_file.log` `chmod 600 /var/log/pcmk_alert_file.log`	Administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas
Confirme que se creó el recurso de alerta de RHEL.	Utilice el siguiente comando para confirmar que se creó el recurso de alerta: `pcs alert` El resultado del comando tendrá el siguiente aspecto: `[root@xxxxxxx ~]# pcs alert` `Alerts:` `Alert: alert_file (path=/var/lib/pacemaker/alert_file.sh)` `Description: Log events to a file.` `Recipients:` `Recipient: my-alert_logfile (value=/var/log/pcmk_alert_file.log)`	Administrador de SAP Basis

Configure el CloudWatch agente

Tarea	Descripción	Habilidades requeridas
Instale el CloudWatch agente.	Hay varias formas de instalar el CloudWatch agente en una instancia EC2. Para usar la línea de comandos: 1. Descargue el paquete del CloudWatch agente:	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	`wget https://s3.<region>.amazonaws.com/amazoncloudwatch-agent-region/redhat/amd64/latest/amazon-cloudwatch-agent.rpm` dónde `<region>` está ubicada la instancia EC2 (por ejemplo,`us-west-2`). Región de AWS 2. (Opcional) Verifique la firma del paquete. Para obtener instrucciones, consulte Verificar la firma del paquete del CloudWatch agente en la CloudWatch documentación. 3. Instale el paquete en la primera instancia: `sudo rpm -U ./amazon-cloudwatch-agent.rpm` 4. Repita el procedimiento para la instancia secundaria. Para obtener más información, consulte la CloudWatch documentación.	

Tarea	Descripción	Habilidades requeridas
Adjunte una función de IAM a la instancia EC2.	Para permitir que el CloudWatch agente envíe datos desde las instancias, debe adjuntar la CloudWatchAgentServerRolefunción de IAM a cada instancia. O bien, puede añadir una política para el CloudWatch agente a su función de IAM actual. Para obtener más información, consulte la CloudWatch documentación.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Configure el CloudWatch agente para que supervise el archivo de registro del agente de alertas de Pacemaker en la instancia del clúster principal.	1. Configure la instancia del clúster principal ejecutando el comando: `sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-config-wizard` 2. Elija 1 para Linux y, a continuación, seleccione las opciones para su estrategia de supervisión. 3. Para la pregunta «¿Desea supervisar algún archivo de registro?», elija Sí e indique la ruta del archivo de registro de Pacemaker mediante el comando pcs alert. En nuestro caso, lo es`var/log/pcmk_alert_file.log` . 4. Proporcione el nombre del grupo de registros y del flujo de registros. Si no especificas un flujo de registro, el ID de AWS instancia se usa como predeterminado. 5. Repite los pasos 1 a 4 para la instancia del clúster secundario.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Inicie el CloudWatch agente en las instancias del clúster principal y secundario.	Para iniciar el agente, ejecute el siguiente comando en las instancias EC2 de los clústeres principal y secundario: `sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -s -c file:/opt/aws/amazon-cloudwatch-agent/bin/config.json`	Administrador de AWS

Configure los recursos CloudWatch

Tarea	Descripción	Habilidades requeridas
Configure grupos de CloudWatch registros.	1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/ 2. En el panel de navegación, elija Grupos de registros y Crear grupo de registros. 3. Introduzca un nombre para el grupo de registros y, a continuación, elija Crear grupo de registros. El CloudWatch agente transferirá el archivo de	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	alertas de Pacemaker al grupo de CloudWatch registros como un flujo de registro.	

Tarea	Descripción	Habilidades requeridas
Configure filtros CloudWatch métricos.	Los filtros métricos le ayudan a buscar un patrón, por ejemplo, `stop <cluster-resource-name>` en los flujos de CloudWatch registro. Cuando se identific a este patrón, el filtro de métricas actualiza una métrica personalizada. 1. En la CloudWatch consola, en el panel de navegación, elija Grupos de registros. 2. Elija el nombre del grupo de registros que creó en la tarea anterior. 3. Elija Actions (Acciones), Create metric filter (Crear filtro de métricas). 4. En Patrón de filtro, introduzca el patrón de filtro que se va a utilizar, por ejemplo`stop ABC_scs`, para que coincida con el evento de parada de un recurso de clúster de SAP SCS denominado`ABC_scs`. Para obtener más informaci ón, consulte la sintaxis del patrón de filtro en la CloudWatch documenta ción.	Administrador de AWS, administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas
	5. (Opcional) Para probar el patrón de filtro, en Test Pattern (Patrón de prueba), ingrese uno o más eventos de registro a utilizar para probar el patrón. Cada evento de registro debe especificarse en una línea independiente, ya que los saltos de línea se utilizan para separar los eventos de registro en el cuadro de mensajes de eventos de registro. 6. Elija Next (Siguiente) y luego ingrese un nombre para el filtro. 7. En Detalles de la métrica, en Espacio de nombres métrico, introduzca un nombre para el espacio de CloudWatch nombres en el que se publicará la métrica (por ejemplo,). `sapcluster_monitoring` Si este espacio de nombres aún no existe, seleccione Crear nuevo. 8. En Nombre de métrica, introduzca un nombre para la nueva métrica (por ejemplo`sapcluster_<sid>` , dónde `<sid>`	

Tarea	Descripción	Habilidades requeridas
	está el nombre de identific ación del sistema SAP). 9. En Valor métrico, introduzc a 1. Como alternativa, puede introducir un token como`$size`. Esto incrementa la métrica por el valor del número en el campo `size` por cada evento de registro que contenga un campo `size`. 10. En Valor predeterminado, introduzca 0. 11. Elija Create metric filter (Crear filtro de métricas). Cuando el filtro de métrica identifica el patrón en el paso 4, actualiza el valor de la métrica CloudWatch personali zada `sapcluster_abc` a 1. La CloudWatch alarma `SAP-Cluster-QA1-AB C` monitorea la métrica `sapcluster_abc` y envía una notificación de SNS cuando el valor de la métrica cambia a 1. Esto indica que el recurso del clúster se ha detenido y es necesario tomar medidas.	

Tarea	Descripción	Habilidades requeridas
Configure una alarma CloudWatch métrica para las métricas ASCS/SCS y ERS de SAP.	Para crear una alarma basada en una única métrica: 1. En la CloudWatch consola, en el panel de navegación, selecciona Alarmas, Todas las alarmas. 2. Elija Create alarm (Crear alarma). 3. Elija Select Metric (Seleccionar métrica). 4. Busque la métrica personalizada `sapcluster_monitoring` que se creó en la tarea anterior. 5. Elija el nombre de la métrica para SAP SCS (por ejemplo,`sapcluster_<abc>`), que también se creó en la tarea anterior. 6. En la pestaña Métricas graficadas, defina lo siguiente: • En Statistic (Estadística), elija Maximum (Máximo). • Para Periodo, seleccione 1 minuto. • En el tipo de umbral, selecciona Estático y establece el umbral en un valor mayor o igual a 1. **`sapcluster_<sid>`** 7. Elija Siguiente.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	8. En Notificación, seleccion a el tema de redes sociales que creaste en la primera epopeya. 9. En Nombre y descripci ón, proporciona el nombre de la alarma y una breve descripción y, a continuac ión, selecciona Siguiente. 10. Seleccione Crear alarma.	
Configure una alarma CloudWatch métrica para la métrica de SAP HANA.	Repita los pasos para configurar una alarma CloudWatch métrica de la tarea anterior, con estos cambios: • En el paso 5, elija el nombre de la métrica para SAP HANA (por ejemplo, `sapcluste r_db_<abc>`). • Para el paso 6, establezc a el umbral en un valor superior `sapcluste r_<sid>` a 0.	Administrador de AWS

Recursos relacionados

- Activación de scripts para eventos de clúster (documentación de RHEL)
- Cree el archivo de configuración del CloudWatch agente con el asistente (documentación) CloudWatch
- Instalación y ejecución del CloudWatch agente en sus servidores (CloudWatch documentación)

- Cree una CloudWatch alarma basada en un umbral estático (CloudWatch documentación)
- Implementación manual de SAP HANA en AWS con clústeres de alta disponibilidad (documentación de SAP en el AWS sitio web)
- NetWeaver Guías de SAP (documentación de SAP en el AWS sitio web)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Importación correcta de un bucket de S3 como CloudFormation pila de AWS

Creado por Ram Kandaswamy (AWS)

Entorno: producción	Tecnologías: nativas en la nube; almacenamiento y copias de seguridad	Servicios de AWS: Amazon S3; AWS CloudFormation

Resumen

Si utiliza los recursos de Amazon Web Services (AWS), como los buckets de Amazon Simple Storage Service (Amazon S3), y desea utilizar un enfoque de infraestructura como código (IaC), puede importar sus recursos a CloudFormation AWS y gestionarlos como una pila.

Este patrón proporciona los pasos para importar correctamente un bucket de S3 como una CloudFormation pila de AWS. Al utilizar este enfoque de patrón, puede evitar los posibles errores que podrían producirse si importa su bucket de S3 en una sola acción.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Un bucket de S3 y una política de bucket de S3 existentes. Para obtener más información al respecto, consulte Qué política de bucket de S3 debo usar para cumplir con la regla s3- de AWS Config bucket-ssl-requests-only en el Centro de conocimiento de AWS.
- Una clave de AWS Key Management Service (AWS KMS) existente y su alias. Para obtener más información, consulte Trabajar con alias en la documentación de AWS KMS.
- La CloudFormation plantilla de `CloudFormation-template-S3-bucket` AWS de muestra (adjunta), descargada en su ordenador local.

Arquitectura

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El usuario crea una plantilla de AWS CloudFormation con formato JSON o YAML.
2. La plantilla crea una CloudFormation pila de AWS para importar el bucket de S3.
3. La CloudFormation pila de AWS administra el depósito de S3 que especificó en la plantilla.

Pila de tecnología

- AWS CloudFormation
- AWS Identity y Access Management (IAM)
- AWS KMS
- Amazon S3

Herramientas

- AWS CloudFormation: AWS le CloudFormation ayuda a crear y aprovisionar despliegues de infraestructura de AWS de forma predecible y repetitiva.
- AWS Identity and Access Management (IAM) es un servicio web que lo ayuda a controlar el acceso seguro a los servicios de AWS.
- AWS KMS: AWS Key Management Service (AWS KMS) es un servicio de cifrado y administración de claves adaptado a la nube.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet.

Epics

Importe un bucket de S3 con cifrado basado en CMK como una pila de AWS CloudFormation

Tarea	Descripción	Habilidades requeridas
Cree una plantilla para importar el bucket S3 y la CMK.	En su ordenador local, cree una plantilla para importar el bucket de S3 y la CMK	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	mediante la siguiente plantilla de ejemplo: `AWSTemplateFormatVersion: 2010-09-09` `Parameters:` `  bucketName:` `    Type: String` `Resources:` `  S3Bucket:` `    Type: 'AWS::S3::Bucket'` `    DeletionPolicy: Retain` `    Properties:` `      BucketName: !Ref bucketName` `      BucketEncryption:` `        ServerSideEncryptionConfiguration:` `          - ServerSideEncryptionByDefault:` `              SSEAlgorithm: 'aws:kms'` `              KMSMasterKeyID: !GetAtt`	

Tarea	Descripción	Habilidades requeridas
	<pre>- KMSS3Encryption - Arn KMSS3Encryption: Type: 'AWS::KMS ::Key' DeletionPolicy: Retain Properties: Enabled: true KeyPolicy: !Sub |- { "Id": "key- consolepolicy-3", "Version": "2012-10-17", "Statemen t": [{ "Sid": "Enable IAM User Permissions", "Effect": "Allow",</pre>	

Tarea	Descripción	Habilidades requeridas
	"Principal": { "AWS": ["arn:aws:iam::${AWS::AccountId}:root"] }, "Action": "kms:*", "Resource": "*" } }] } EnableKeyRotation: true	

Tarea	Descripción	Habilidades requeridas
Cree la pila.	1. Inicie sesión en la consola de administración de AWS, abra la CloudFormation consola de AWS, elija Ver pila, elija Crear pila y, a continuación, elija Con recursos existentes (importar recursos). 2. Elija Upload a template file (Cargar un archivo de plantilla) y, a continuac ión, cargue el archivo de plantilla que creó anteriorm ente. 3. Introduzca un nombre para su pila y configure las opciones restantes según sus necesidades. 4. Seleccione Create stack (Crear pila) y espere a que el estado de la colección cambie a `IMPORT_CO MPLETE` .	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Cree el alias de la clave KMS.	1. En la CloudFormation consola de AWS, elija Stacks, elija el nombre de la pila que creó anteriormente, elija el panel Template y, a continuación, elija View in Designer. 2. Añada el siguiente fragmento a la sección `Resource` de la plantilla y, a continuación, elija Create stack (Crear pila) y complete el asistente: `KMSS3EncryptionAlias:` `  Type: 'AWS::KMS ::Alias'` `  DeletionPolicy: Retain` `  Properties:` `  AliasName: alias/S3BucketKey` `  TargetKeyId: !Ref KMSS3Encryption` Para obtener más información al respecto, consulte las actualizaciones de la CloudFormation pila de	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	AWS en la CloudFormation documentación de AWS.	

Tarea	Descripción	Habilidades requeridas
Actualice la pila para incluir la política de bucket de S3.	1. En la CloudFormation consola de AWS, elija Stacks, elija el nombre de la pila que creó anteriormente, elija el panel Template y, a continuación, elija View in Designer. 2. Añada el siguiente fragmento a la sección `Resource` de la plantilla y, a continuación, elija Create stack (Crear pila) y complete el asistente: `S3BucketPolicy:` `  Type: 'AWS::S3::BucketPolicy'` `  Properties:` `    Bucket: !Ref S3Bucket` `    PolicyDocument: !Sub |-` `      {` `  "Version": "2008-10-17",` `                  "Id": "restricthttp",`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	<pre>"Statement": [{ "Sid": "denyhttp", "Effect": "Deny", "Principal": { "AWS": "*" }, "Action": "s3:*", "Resource": ["arn:aws:s3:::${S3Bucket}","arn:aws:s3:::${S3Bucket}/*"], "Condition": { "Bool": { "aws:SecureTransport": "false" }</pre>	

Tarea	Descripción	Habilidades requeridas
	<pre>} }] }</pre> Nota: Esta política de bucket de S3 tiene una declaración de denegación que restringe las llamadas a la API que no son seguras.	

Tarea	Descripción	Habilidades requeridas
Actualice la política de claves.	1. En la CloudFormation consola de AWS, elija Stacks, elija el nombre de la pila que creó anteriormente, elija el panel Template y, a continuación, elija View in Designer. 2. Modifique el recurso KMS de la plantilla para incluir la política de claves que permite a los administr adores administrar la CMK. 3. Elija Create stack (Crear pila), elija Next (Siguiente) y, a continuación, complete el asistente según sus necesidades. Para obtener más informaci ón al respecto, consulte Uso de políticas de claves en AWS KMS y Permitir que los administradores de claves administren la CMK en la documentación de AWS KMS.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Adición de etiquetas de nivel de recursos.	1. En la CloudFormation consola de AWS, elija Stacks, elija el nombre de la pila que creó anteriormente, elija el panel Template y, a continuación, elija View in Designer. 2. Añada el siguiente fragmento a la sección `Properties` de recursos de la plantilla y, a continuación, elija Create stack (Crear pila) y complete el asistente: `Tags:` `  - Key: createdBy` `  Value: Cloudformation`	AWS DevOps

Recursos relacionados

- Incorporar los recursos existentes a la CloudFormation administración de AWS
- AWS re:Invent 2017: información detallada sobre AWS CloudFormation (vídeo)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Más patrones

- Acceder a un host bastión mediante Session Manager y Amazon EC2 Instance Connect
- Asocie un CodeCommit repositorio de AWS en una cuenta de AWS con SageMaker Studio en otra cuenta
- Automatice la adición o actualización de entradas de registro de Windows con AWS Systems Manager
- Automatice la formación y el despliegue de Amazon Lookout for Vision para la detección de anomalías
- Automatice la creación de recursos AppStream 2.0 con AWS CloudFormation
- Crear e implementar de forma automática una aplicación Java en Amazon EKS mediante una canalización de CI/CD
- Crear automáticamente una RFC en AMS mediante Python
- ???
- Creación de un PAC de Micro Focus Enterprise Server con Amazon EC2 Auto Scaling y Systems Manager
- Encadene los servicios de AWS mediante un enfoque sin servidor
- Compruebe las instancias EC2 para ver si hay etiquetas obligatorias en el lanzamiento
- Configurar Veritas NetBackup para VMware Cloud on AWS
- Conectarse a una instancia de Amazon EC2 mediante el uso de Session Manager
- ???
- ???
- Cree alarmas para métricas personalizadas mediante la detección de CloudWatch anomalías de Amazon
- Crear una definición de tareas de Amazon ECS y montar un sistema de archivos en instancias EC2 mediante Amazon EFS
- Crear automáticamente canalizaciones de CI dinámicas para proyectos de Java y Python
- Crea automáticamente CloudWatch paneles de Amazon basados en etiquetas
- Implementar una aplicación agrupada en Amazon ECS con AWS Copilot
- Implemente una aplicación de una sola página basada en React en Amazon S3 y CloudFront
- Implementar y depurar clústeres de Amazon EKS

- Implemente y gestione los controles de la Torre de Control de AWS mediante AWS CDK y AWS CloudFormation
- Implementación y administración de los controles de AWS Control Tower mediante Terraform
- Implementar contenedores mediante Elastic Beanstalk
- Implementar funciones de Lambda con imágenes de contenedor
- Documente el conocimiento institucional a partir de las entradas de voz mediante Amazon Bedrock y Amazon Transcribe
- Imponga el etiquetado automático de las bases de datos de Amazon RDS en el lanzamiento
- Estime el costo de una tabla de DynamoDB para la capacidad bajo demanda
- Explore el desarrollo completo de aplicaciones web nativas en la nube con Green Boost
- Exporte tablas de Amazon RDS para SQL Server a un bucket S3 mediante AWS DMS
- Genere recomendaciones personalizadas y reclasificadas con Amazon Personalize
- Genere datos de prueba con un trabajo de AWS Glue y Python
- Reciba notificaciones de Amazon SNS cuando cambie el estado de clave de una clave de AWS KMS
- ???
- Identifique y avise cuando los recursos de Amazon Data Firehose no estén cifrados con una clave de AWS KMS
- Implementar el patrón saga sin servidor mediante AWS Step Functions
- Mejore el rendimiento operativo al habilitar Amazon DevOps Guru en varias regiones, cuentas y unidades organizativas de AWS con la AWS CDK
- Incorporar y migrar instancias de Windows de EC2 a una cuenta de AWS Managed Services
- Administre los productos de AWS Service Catalog en varias cuentas y regiones de AWS
- Migración de una base de datos de Microsoft SQL Server de Amazon EC2 a Amazon DocumentDB mediante AWS DMS
- Migrar registros DNS de forma masiva a una zona alojada privada de Amazon Route 53
- Migre de Oracle 8i o 9i a Amazon RDS para Oracle con AWS DMS SharePlex
- Supervise ElastiCache los clústeres de Amazon para comprobar el cifrado en reposo
- Supervisar los clústeres de Amazon EMR para comprobar el cifrado en tránsito en el momento del lanzamiento
- Supervise ElastiCache los clústeres para grupos de seguridad
- Replicar bases de datos de unidades centrales en AWS mediante Precisely Connect

- Configure la detección de CloudFormation desviaciones de AWS en una organización multirregional y multicuenta
- Estructure un proyecto de Python en una arquitectura hexagonal con AWS Lambda
- Incorporación de inquilinos en la arquitectura SaaS para el modelo de silo mediante C# y AWS CDK
- Actualice las credenciales de la CLI de AWS desde el centro de identidad de IAM de AWS mediante PowerShell
- Usa Terraform para habilitar Amazon automáticamente GuardDuty para una organización
- Vea los registros y las métricas de AWS Network Firewall mediante Splunk

Contenedores y microservicios

Temas

- Genere una dirección IP saliente estática mediante una función de Lambda, Amazon VPC y una arquitectura sin servidor
- Instalación del agente SSM en los nodos de trabajo de Amazon EKS mediante Kubernetes DaemonSet
- Instale el agente SSM y el CloudWatch agente en los nodos de trabajo de Amazon EKS mediante preBootstrapCommands
- Optimizar imágenes de Docker generadas por AWS App2Container
- Coloque los pods de Kubernetes en Amazon EKS mediante la afinidad, las taints y las tolerancias de nodos
- Replicar imágenes filtradas de contenedores de Amazon ECR en todas las cuentas o regiones
- Rotar las credenciales de la base de datos sin reiniciar los contenedores
- Ejecute tareas de Amazon ECS en Amazon WorkSpaces con Amazon ECS Anywhere
- Ejecute un contenedor de Docker de la API web de ASP.NET Core en una instancia Linux de Amazon EC2
- Ejecute cargas de trabajo basadas en mensajes a escala con AWS Fargate
- Ejecutar cargas de trabajo con estado y almacenamiento de datos persistente mediante Amazon EFS en Amazon EKS con AWS Fargate
- Más patrones

Acceda a las aplicaciones de contenedores de forma privada en Amazon ECS mediante AWS PrivateLink y un Network Load Balancer

Creado por Kirankumar Chandrashekar (AWS)

Entorno: producción	Tecnologías: contenedores y microservicios; redes; seguridad, identidad y conformidad; aplicaciones web y móviles	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon EC2; Amazon EC2 Auto Scaling; Amazon EC2 Container Registry; Amazon EFS; Amazon RDS; Amazon VPC; Amazon ECS; Elastic Load Balancing (ELB); AWS Lambda		

Resumen

Este patrón describe cómo alojar de forma privada una aplicación contenedora de Docker en Amazon Elastic Container Service (Amazon ECS) detrás de un Network Load Balancer y cómo acceder a la aplicación mediante AWS. PrivateLink A continuación, puede utilizar una red privada para acceder de forma segura a los servicios de la nube de Amazon Web Services (AWS). Amazon Relational Database Service (Amazon RDS) aloja la base de datos relacional para la aplicación que se ejecuta en Amazon ECS con alta disponibilidad (HA). Se usa Amazon Elastic File System (Amazon EFS) si la aplicación necesita almacenamiento persistente.

El servicio Amazon ECS que ejecuta las aplicaciones de Docker, con un Network Load Balancer en la interfaz, se puede asociar a un punto final de nube privada virtual (VPC) para acceder a él a través de AWS. PrivateLink A continuación, este servicio de punto de conexión de VPC se puede compartir con otras VPC mediante sus puntos de conexión de VPC.

También puede usar AWS Fargate en vez de un grupo de escalado automático de Amazon EC2. Para obtener más información, consulte Acceda a aplicaciones de contenedores de forma privada en Amazon ECS mediante AWS Fargate PrivateLink, AWS y un Network Load Balancer.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Interfaz de la línea de comandos de AWS (AWS CLI) versión 2, instalada y configurada en Linux, macOS o Windows
- Docker, instalado y configurado en Linux, macOS o Windows
- Una aplicación que se ejecuta en Docker

Arquitectura

Pila de tecnología

- Amazon CloudWatch
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon EC2 Auto Scaling
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon ECS
- Amazon RDS
- Amazon Simple Storage Service (Amazon S3)
- AWS Lambda
- AWS PrivateLink
- AWS Secrets Manager
- Equilibrador de carga de aplicación
- Equilibrador de carga de red

- VPC

Automatizar y escalar

- Puede usar AWS CloudFormation para crear este patrón mediante Infrastructure as Code.

Herramientas

- Amazon EC2: Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de AWS.
- Amazon EC2 Auto Scaling: Amazon EC2 Auto Scaling le ayuda a garantizar que cuenta con la cantidad correcta de instancias de Amazon EC2 disponibles para gestionar la carga de su aplicación.
- Amazon ECS: Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores altamente escalable y rápido que facilita la tarea de ejecutar, detener y administrar contenedores en un clúster.
- Amazon ECR: Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor de AWS administrado que es seguro, escalable y fiable.
- Amazon EFS: Amazon Elastic File System (Amazon EFS) ofrece un sistema de archivos NFS sencillo, escalable, elástico y completamente administrado que se utiliza con servicios de nube de AWS y recursos en las instalaciones.
- AWS Lambda: AWS Lambda es un servicio informático para ejecutar código sin aprovisionar ni administrar servidores.
- Amazon RDS: Amazon Relational Database Service (Amazon RDS) es un servicio web que facilita la configuración, el funcionamiento y el escalado de una base de datos relacional en la nube de AWS.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet. Está diseñado para facilitar a los desarrolladores recursos de computación escalables basados en Web.
- AWS Secrets Manager: Secrets Manager permite reemplazar las credenciales codificadas en el código, incluidas las contraseñas, proponiendo una llamada a la API de Secrets Manager para recuperar el secreto mediante programación.
- Amazon VPC: Amazon Virtual Private Cloud (Amazon VPC) permite lanzar recursos de AWS en una red virtual previamente definida.

- Equilibrador de carga elástico: el equilibrador de carga elástico distribuye el tráfico entrante de red o de la aplicación entre varios destinos, por ejemplo, instancias de Amazon EC2, contenedores y direcciones IP en varias zonas de disponibilidad.
- Docker: Docker ayuda a los desarrolladores a empaquetar, enviar y ejecutar cualquier aplicación como un contenedor ligero, portátil y autosuficiente.

Epics

Creación de componentes de redes

Tarea	Descripción	Habilidades requeridas
Cree una VPC.	1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon VPC. Seleccione Crear VPC y, a continuación, VPC y más. 2. Especifique un nombre para su VPC y seleccione un rango de bloques CIDR adecuado. 3. Especifique dos zonas de disponibilidad, dos subredes públicas y cuatro subredes privadas. Dos subredes privadas son para las tareas de Amazon ECS y otras dos subredes privadas son para las bases de datos de Amazon RDS. 4. Especifique una puerta de enlace NAT para cada zona de disponibilidad. 5. Seleccione Crear VPC.	Administrador de la nube

Crear el equilibrador de carga

Tarea	Descripción	Habilidades requeridas
Crear un equilibrador de carga de red.	1. En la consola de Amazon EC2, seleccione la región de AWS que contiene su VPC. 2. En Equilibrio de carga seleccione Equilibradores de carga y Crear equilibrador de carga. 3. Seleccione Equilibrador de carga de red y luego Crear. 4. En la página Configurar el equilibrador de carga, configure el equilibrador de carga de red y el oyente. Importante: Asegúrese de elegir el esquema del equilibrador de carga de red como Interno. 5. Seleccione los ajustes de seguridad aplicables, configure un grupo de seguridad y un grupo de destino. Seleccione Instancia o IP como Tipo de destino en la sección Configurar enrutamiento. Asegúrese de no registrar un destino. 6. Una vez haya configurado todos los ajustes, seleccione Siguiente: Revisar y, a	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	continuación, seleccione Crear.	

Tarea	Descripción	Habilidades requeridas
Cree un Equilibrador de carga de aplicación.	1. En la consola de Amazon EC2, seleccione la región de AWS que contiene su VPC. 2. En Equilibrio de carga seleccione Equilibradores de carga y Crear equilibrador de carga. 3. Seleccione Application Load Balancer (Equilibrador de carga de aplicación) y, a continuación, Create. 4. Configure su equilibrador de carga de aplicación y su oyente. Importante: Asegúrese de elegir el esquema de su equilibrador de carga de aplicaciones como Interno. 5. Seleccione los ajustes de seguridad aplicables, configure un grupo de seguridad y un grupo de destino. Seleccione Instancia o IP como Tipo de destino en la sección Configurar enrutamiento. Asegúrese de no registrar un destino. 6. Una vez haya configurado todos los ajustes, seleccione Siguiente: Revisar y, a	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	continuación, seleccione Crear.	

Crear un sistema de archivos de Amazon EFS

Tarea	Descripción	Habilidades requeridas
Crear un sistema de archivos de Amazon EFS.	1. Abra la consola de Amazon EFS y seleccione Crear sistema de archivos. 2. En el cuadro de diálogo Crear sistema de archivos, especifique un nombre para su sistema de archivos y seleccione su VPC. 3. Seleccione Crear para crear el sistema de archivos. 4. Instale y configure su sistema de archivos de Amazon EFS.	Administrador de la nube
Defina el montaje de los destinos para las subredes.	1. Regrese a la consola de Amazon EFS y seleccion e Sistemas de archivos. La página Sistemas de archivos muestra los sistemas de archivos Amazon EFS de su cuenta. 2. Seleccione el sistema de archivos que creó y seleccione Administrar para mostrar las Zonas de disponibilidad. Para añadir un destino de montaje,	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	seleccione Añadir destino de montaje y añada las cuatro subredes privadas que creó.	
Compruebe que las subredes estén montadas como destinos.	1. En la consola de Amazon EFS, seleccione Sistemas de archivos. 2. Para ver la lista de objetivos de montaje existentes, seleccione Red. Asegúrese de que las cuatro subredes que creó estén incluidas.	Administrador de la nube

Creación de un bucket de S3

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3.	Si es necesario, abra la consola de Amazon S3 y cree un bucket de S3 para almacenar los activos estáticos de la aplicación.	Administrador de la nube

Crear un secreto en Secrets Manager

Tarea	Descripción	Habilidades requeridas
Para cifrar el secreto de Secrets Manager, cree una clave de AWS KMS.	Abra la consola de AWS Key Management Service (AWS KMS) y cree una clave KMS.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Cree un secreto de Secrets Manager para almacenar la contraseña de Amazon RDS.	1. Abra la consola de AWS Secrets Manager y cree un secreto nuevo. Para hacerlo, seleccione Almacenar un nuevo secreto. 2. Seleccione la clave de KMS que creó y guarde su nuevo secreto.	Administrador de la nube

Crear una instancia de Amazon RDS

Tarea	Descripción	Habilidades requeridas
Creación de un grupo de subredes de base de datos.	1. Abra la consola de Amazon RDS y seleccione Grupos de subred. 2. Seleccione Crear un grupo de subred de base de datos, e introduzca un nombre y una descripción para su grupo de subred de base de datos. 3. Seleccione la VPC que creó anteriormente y, a continuación, seleccione las zonas de disponibilidad y las subredes. A continuac ión, seleccione Crear.	Administrador de la nube
Cree una instancia de Amazon RDS.	Cree y configure una instancia de Amazon RDS dentro de las subredes privadas. Asegúrese	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	de que Multi-AZ esté activado para una alta disponibilidad.	
Cargue los datos en la instancia de Amazon RDS.	Cargue los datos relacionales que necesita la aplicación en la instancia de Amazon RDS. Este proceso variará según las necesidades de la aplicación y la forma en que se defina y diseñe el esquema de la base de datos.	Administrador de la nube, administrador de bases de datos

Crear los componentes de Amazon ECS

Tarea	Descripción	Habilidades requeridas
Cree un clúster de ECS.	1. Abra la consola de Amazon ECS y seleccione Clústeres. 2. Seleccione Crear clústeres y configure un clúster de ECS de acuerdo con las especificaciones requeridas.	Administrador de la nube
Cree las imágenes de Docker.	Cree las imágenes de Docker según las instrucciones de la sección Recursos relacionados.	Administrador de la nube
Crear repositorios de Amazon ECR.	1. En la consola de Amazon ECR, seleccione Repositorios. 2. Seleccione Create repository (Crear repositorio) y	Administrador de nube, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	especifique un nombre exclusivo para el repositorio. 3. Configure el repositorio de acuerdo con sus especificaciones, incluyendo el cifrado de AWS KMS si es necesario.	
Autenticar su cliente Docker para el repositorio de Amazon ECR.	Para autenticar su cliente de Docker para el repositorio de Amazon ECR, ejecute el comando `aws ecr get-login-password` en la CLI de AWS.	Administrador de la nube
Pase las imágenes de Docker al repositorio de Amazon ECR.	1. Identifique la imagen de Docker que quiere insertar y ejecute el comando `docker images` en la CLI de AWS. 2. Etiquete su imagen con la combinación de registro, repositorio y etiqueta de imagen opcional de Amazon ECR. 3. Ejecute el comando `docker push` para enviar la imagen de Docker. 4. Repita estos pasos para todas las imágenes requeridas.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Cree una definición de tarea de Amazon ECS.	Para ejecutar contenedores Docker en Amazon ECS, se requiere una definición de tareas. 1. Regrese a la consola de Amazon ECS, seleccione Definiciones de tareas y, a continuación, seleccione Crear nueva definición de tarea. 2. En la página Selección de compatibilidades, seleccione el tipo de lanzamiento que su tarea debe usar y, a continuación, seleccione Siguiente paso. Para obtener ayuda con la configuración de la definición de la tarea, consulte la sección “Crear una definición de tarea” en la sección Recursos relacionados. Importante: Asegúrese de proporcionar las imágenes de Docker que envió a Amazon ECR.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Creación de un servicio de Amazon ECS.	Cree un servicio de Amazon ECS mediante el clúster de ECS que creó anteriormente. Asegúrese de elegir Amazon EC2 como tipo de lanzamien to y seleccione la definición de tarea creada en el paso anterior, así como el grupo de destino del equilibrador de carga de aplicación.	Administrador de la nube

Crear un grupo de Amazon EC2 Auto Scaling

Tarea	Descripción	Habilidades requeridas
Cree una configuración de lanzamiento.	Abra la consola de Amazon ECS y cree una configuración de lanzamiento. Asegúrese de que los datos del usuario tengan el código que permita que las instancias EC2 se unan al clúster de ECS deseado. Para ver un ejemplo del código necesario, consulte la sección Recursos relaciona dos.	Administrador de la nube
Crear un grupo de Amazon EC2 Auto Scaling.	Regrese a la consola de Amazon EC2 y, en Escalado automático, seleccione Grupos de escalado automátic o. Configurar un grupo de Amazon EC2 Auto Scaling. Asegúrese de elegir las	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	subredes privadas y la configuración de lanzamiento que creó anteriormente.	

Configuración de AWS PrivateLink

Tarea	Descripción	Habilidades requeridas
Configure el PrivateLink punto de conexión de AWS.	1. En la consola de Amazon VPC, cree un punto de conexión de AWS PrivateLink . 2. Asocie este punto de conexión con el equilibrador de carga de red, lo que hará que la aplicación alojada en Amazon ECS esté disponible para los clientes de forma privada. Para obtener más información, consulte la sección Recursos relacionados.	Administrador de la nube

Crear un punto de conexión de VPC

Tarea	Descripción	Habilidades requeridas
Cree un punto de conexión de VPC.	Cree un punto de enlace de VPC para el punto de PrivateLink enlace de AWS que creó anteriormente. El nombre de dominio completo	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	(FQDN) del punto final de la VPC apuntará al FQDN del punto final de AWS PrivateLi nk . Esto crea una interfaz de red elástica para el servicio de puntos de conexión de VPC a la que pueden acceder los puntos de conexión de DNS.	

Crear la función de Lambda

Tarea	Descripción	Habilidades requeridas
Crear la función de Lambda.	En la consola de AWS Lambda, cree una función de Lambda para actualizar las direcciones IP del equilibrador de carga de aplicación como destinos del equilibrador de carga de red. Para obtener más información, consulte la entrada del blog «Using static IP addresses for Applicati on Load Balancers (Uso de direcciones IP estáticas para los equilibradores de carga de aplicación)» en la sección Recursos relacionados.	Desarrollador de aplicaciones

Recursos relacionados

Crear los equilibradores de carga:

- Crear un equilibrador de carga de red

- Creación de un equilibrador de carga de aplicación

Crear un sistema de archivos de Amazon EFS:

- Crear un sistema de archivos de Amazon EFS
- Crear destinos de montaje en Amazon EFS

Creación de un bucket de S3:

- Creación de un bucket de S3

Crear un secreto en Secrets Manager:

- Crear claves en AWS KMS
- Crear un secreto en AWS Secrets Manager

Crear una instancia de Amazon RDS:

- Crear una instancia de base de datos de Amazon RDS

Crear los componentes de Amazon ECS:

- Crear un clúster de Amazon ECS
- Crear una imagen de Docker
- Crear un repositorio de Amazon ECR
- Autenticar Docker con el repositorio de Amazon ECR
- Pasar una imagen a un repositorio de Amazon ECR
- Crear una definición de tarea de Amazon ECS
- Creación de un servicio de Amazon ECS

Crear un grupo de Amazon EC2 Auto Scaling:

- Crear una configuración de lanzamiento
- Crear un grupo de escalado automático mediante una configuración de lanzamiento

- Proceso de arranque de instancias de contenedor con datos de usuario de Amazon EC2

Configure AWS PrivateLink:

- Servicios de puntos finales de VPC (AWS) PrivateLink

Crear un punto de conexión de VPC:

- Puntos de enlace de interfaz de VPC (AWS) PrivateLink

Crear la función de Lambda:

- Crear una función de Lambda

Otros recursos:

- Uso de direcciones IP estáticas para los equilibradores de carga de aplicación
- Acceso seguro a los servicios a través de AWS PrivateLink

Acceda a las aplicaciones de contenedores de forma privada en Amazon ECS mediante AWS Fargate PrivateLink, AWS y un Network Load Balancer

Creado por Kirankumar Chandrashekar (AWS)

Entorno: producción	Tecnologías: contenedores y microservicios; redes; seguridad, identidad y conformidad; aplicaciones web y móviles	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Registro de contenedores de Amazon EC2; Amazon ECS; Amazon EFS; Amazon RDS; Amazon VPC; Elastic Load Balancing (ELB); AWS Lambda		

Resumen

Este patrón describe cómo alojar de forma privada una aplicación contenedora de Docker en la nube de Amazon Web Services (AWS) mediante Amazon Elastic Container Service (Amazon ECS) con un tipo de lanzamiento de AWS Fargate, detrás de un Network Load Balancer, y cómo acceder a la aplicación mediante AWS. PrivateLink Amazon Relational Database Service (Amazon RDS) aloja la base de datos relacional para la aplicación que se ejecuta en Amazon ECS con alta disponibilidad (HA). Puede utilizar Amazon Elastic File System (Amazon EFS) si la aplicación requiere almacenamiento permanente.

Este patrón utiliza un tipo de lanzamiento de Fargate para el servicio de Amazon ECS que ejecuta las aplicaciones de Docker, con un equilibrador de carga de red en el front-end. Luego, se puede asociar a un punto final de nube privada virtual (VPC) para acceder a través de AWS. PrivateLink A continuación, este servicio de punto de conexión de VPC se puede compartir con otras VPC mediante sus puntos de conexión de VPC.

Se puede utilizar la tecnología Fargate con Amazon ECS para ejecutar contenedores sin tener que administrar servidores ni clústeres de instancias de Amazon Elastic Compute Cloud (Amazon EC2). También se puede utilizar el grupo de Amazon EC2 Auto Scaling en lugar de Fargate. Para obtener más información, consulte Acceda a aplicaciones de contenedores de forma privada en Amazon ECS mediante AWS PrivateLink y un Network Load Balancer.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Interfaz de la línea de comandos de AWS (AWS CLI) versión 2, instalada y configurada en Linux, macOS o Windows
- Docker, instalado y configurado en Linux, macOS o Windows
- Una aplicación que se ejecuta en Docker

Arquitectura

Pila de tecnología

- Amazon CloudWatch
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon ECS
- Amazon EFS
- Amazon RDS
- Amazon Simple Storage Service (Amazon S3)
- AWS Fargate
- AWS Lambda
- AWS PrivateLink
- AWS Secrets Manager
- Equilibrador de carga de aplicación
- Equilibrador de carga de red

- VPC

Automatizar y escalar

- Puede usar AWS CloudFormation para crear este patrón mediante Infrastructure as Code.

Herramientas

- Amazon ECS: Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores altamente escalable y rápido que facilita la tarea de ejecutar, detener y administrar contenedores en un clúster.
- Amazon ECR: Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor de AWS administrado que es seguro, escalable y fiable.
- Amazon EFS: Amazon Elastic File System (Amazon EFS) ofrece un sistema de archivos NFS sencillo, escalable, elástico y completamente administrado que se utiliza con servicios de nube de AWS y recursos en las instalaciones.
- AWS Fargate: AWS Fargate es una tecnología que se puede utilizar en Amazon ECS para ejecutar contenedores sin tener que administrar servidores ni clústeres de instancias de Amazon EC2.
- AWS Lambda: Lambda es un servicio informático que permite ejecutar código sin aprovisionar ni administrar servidores.
- Amazon RDS: Amazon Relational Database Service (Amazon RDS) es un servicio web que facilita la configuración, el funcionamiento y el escalado de una base de datos relacional en la nube de AWS.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet. Está diseñado para facilitar a los desarrolladores recursos de computación escalables basados en Web.
- AWS Secrets Manager: Secrets Manager le permite reemplazar las credenciales codificadas en el código, incluidas las contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación.
- Amazon VPC: Amazon Virtual Private Cloud (Amazon VPC) permite lanzar recursos de AWS en una red virtual previamente definida.
- Elastic Load Balancing (ELB): Elastic Load Balancing (ELB) distribuye el tráfico entrante de red o de la aplicación entre varios destinos, por ejemplo, instancias EC2, contenedores y direcciones IP en varias zonas de disponibilidad.

- Docker: Docker facilita a los desarrolladores empaquetar, enviar y ejecutar cualquier aplicación como un contenedor ligero, portátil y autosuficiente.

Epics

Creación de componentes de redes

Tarea	Descripción	Habilidades requeridas
Cree una VPC.	1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon VPC. Seleccione Crear VPC y, a continuación, VPC y más. 2. Especifique un nombre para su VPC y seleccione un rango de bloques CIDR adecuado. 3. Especifique dos zonas de disponibilidad, dos subredes públicas y cuatro subredes privadas. Dos subredes privadas son para las tareas de Amazon ECS y otras dos subredes privadas son para las bases de datos de Amazon RDS. 4. Especifique una puerta de enlace NAT para cada zona de disponibilidad. 5. Seleccione Crear VPC.	Administrador de la nube

Crear el equilibrador de carga

Tarea	Descripción	Habilidades requeridas
Crear un equilibrador de carga de red.	1. En la consola de Amazon EC2, seleccione la región de AWS que contiene su VPC. 2. En Equilibrio de carga seleccione Equilibradores de carga y Crear equilibrador de carga. 3. Seleccione Equilibrador de carga de red y luego Crear. 4. En la página Configurar el equilibrador de carga, configure el equilibrador de carga de red y el oyente. Importante: Asegúrese de elegir el esquema del equilibrador de carga de red como interno. 5. Seleccione los ajustes de seguridad aplicables, configure un grupo de seguridad y un grupo de destino. Seleccione IP como Target type (Tipo de destino) en la sección Configure routing (Configurar enrutamiento). Asegúrese de no registrar un destino. 6. Una vez haya configurado todos los ajustes, seleccione Siguiente: Revisar y, a	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	continuación, seleccione Crear. Para obtener ayuda con esta y otras explicaciones, consulte la sección Recursos relaciona dos.	

Tarea	Descripción	Habilidades requeridas
Cree un Equilibrador de carga de aplicación.	1. En la consola de Amazon EC2, seleccione la región de AWS que contiene su VPC. 2. En Equilibrio de carga seleccione Equilibradores de carga y Crear equilibrador de carga. 3. Seleccione Application Load Balancer (Equilibrador de carga de aplicación) y, a continuación, Create. 4. Configure el equilibrador de carga de aplicación y el oyente. Importante: asegúrese de elegir el esquema del equilibrador de carga de aplicación como interno. 5. Seleccione los ajustes de seguridad aplicables, configure un grupo de seguridad y un grupo de destino. Seleccione IP como Target type (Tipo de destino) en la sección Configure routing (Configurar enrutamiento). Asegúrese de no registrar un destino. 6. Una vez haya configurado todos los ajustes, seleccione Siguiente: Revisar y, a	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	continuación, seleccione Crear.	

Crear un sistema de archivos de Amazon EFS

Tarea	Descripción	Habilidades requeridas
Crear un sistema de archivos de Amazon EFS.	1. Abra la consola de Amazon EFS y seleccione Crear sistema de archivos. 2. En el cuadro de diálogo Crear sistema de archivos, especifique un nombre para su sistema de archivos y seleccione su VPC. 3. Seleccione Crear para crear el sistema de archivos. 4. Instale y configure su sistema de archivos de Amazon EFS.	Administrador de la nube
Defina el montaje de los destinos para las subredes.	1. Regrese a la consola de Amazon EFS y seleccion e Sistemas de archivos. La página Sistemas de archivos muestra los sistemas de archivos Amazon EFS de su cuenta. 2. Seleccione el sistema de archivos que creó y, a continuación, seleccione Manage (Administrar) para mostrar la zona de disponibi lidad.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	3. Para añadir un destino de montaje, seleccione Añadir destino de montaje y añada las cuatro subredes privadas que creó.	
Compruebe que las subredes estén montadas como destinos.	1. En la consola de Amazon EFS, seleccione Sistemas de archivos. 2. Para ver la lista de objetivos de montaje existentes, seleccione Red. Asegúrese de que las cuatro subredes que creó estén incluidas.	Administrador de la nube

Creación de un bucket de S3

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3.	Si es necesario, abra la consola de Amazon S3 y cree un bucket de S3 para almacenar los activos estáticos de la aplicación.	Administrador de la nube

Crear un secreto en Secrets Manager

Tarea	Descripción	Habilidades requeridas
Para cifrar el secreto de Secrets Manager, cree una clave de AWS KMS.	Abra la consola de AWS Key Management Service (AWS KMS) y cree una clave KMS.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Cree un secreto de Secrets Manager para almacenar la contraseña de Amazon RDS.	1. Abra la consola de AWS Secrets Manager y cree un secreto nuevo. Para hacerlo, seleccione Almacenar un nuevo secreto. 2. Seleccione la clave de KMS que creó y guarde su nuevo secreto.	Administrador de la nube

Crear una instancia de Amazon RDS

Tarea	Descripción	Habilidades requeridas
Creación de un grupo de subredes de base de datos.	1. Abra la consola de Amazon ECS y seleccione Subnet groups (Grupos de subred). 2. Seleccione Crear un grupo de subred de base de datos, e introduzca un nombre y una descripción para su grupo de subred de base de datos. 3. Seleccione la VPC que creó anteriormente y, a continuación, seleccione las zonas de disponibilidad y las subredes. A continuac ión, seleccione Crear.	Administrador de la nube
Cree una instancia de Amazon RDS.	Cree y configure una instancia de Amazon RDS dentro de las subredes privadas. Asegúrese	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	de que Multi-AZ esté activado, para una alta disponibilidad (HA).	
Cargue los datos en la instancia de Amazon RDS.	Cargue los datos relacionales que necesita la aplicación en la instancia de Amazon RDS. Este proceso variará según las necesidades de la aplicación y la forma en que se defina y diseñe el esquema de la base de datos.	Administrador de base de datos

Crear los componentes de Amazon ECS

Tarea	Descripción	Habilidades requeridas
Cree un clúster de ECS.	1. Abra la consola de Amazon ECS y seleccione Clústeres. 2. Seleccione Crear clústeres y configure un clúster de ECS de acuerdo con las especificaciones requeridas.	Administrador de la nube
Cree las imágenes de Docker.	Cree las imágenes de Docker según las instrucciones de la sección Recursos relacionados.	Administrador de la nube
Cree un repositorio de Amazon ECR.	1. Abra la consola de Amazon ECR y seleccione Repositories.	Administrador de nube, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	2. Seleccione Create repository (Crear repositorio) y especifique un nombre exclusivo para el repositorio. 3. Configure el repositorio de acuerdo con sus especificaciones, incluyendo el cifrado de AWS KMS si es necesario.	
Pase las imágenes de Docker al repositorio de Amazon ECR.	1. Identifique la imagen de Docker que desea insertar y ejecute el comando `docker images` en la AWS CLI. 2. Etiquete su imagen con la combinación de registro, repositorio y etiqueta de imagen opcional de Amazon ECR. 3. Ejecute el comando `docker push` para enviar la imagen de Docker. 4. Repita estos pasos para todas las imágenes requeridas.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Cree una definición de tarea de Amazon ECS.	Para ejecutar contenedores Docker en Amazon ECS, se requiere una definición de tareas. 1. Regrese a la consola de Amazon ECS, seleccione Definiciones de tareas y, a continuación, seleccione Crear nueva definición de tarea. 2. En la página Selección de compatibilidades, seleccione el tipo de lanzamiento que su tarea debe usar y, a continuación, seleccione Siguiente paso. Para obtener ayuda sobre la configuración de la definición de la tarea, consulte la sección «Crear una definición de tarea» en los Recursos relacionados. Importante: Asegúrese de proporcionar las imágenes de Docker que envió a Amazon ECR.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Cree un servicio ECS y seleccione Fargate como tipo de lanzamiento.	1. Cree un servicio de Amazon ECS mediante el clúster de ECS que creó anteriormente. Asegúrese de seleccionar Fargate como tipo de lanzamiento. 2. Seleccione la definición de tarea creada en el paso anterior y, a continuación, el grupo objetivo del equilibra dor de carga de aplicación.	Administrador de la nube

Configurar AWS PrivateLink

Tarea	Descripción	Habilidades requeridas
Configure el PrivateLink punto de conexión de AWS.	1. Abra la consola de Amazon VPC y cree un punto de conexión de AWS PrivateLi nk . 2. Asocie este punto de conexión con el equilibra dor de carga de red, lo que hará que la aplicació n alojada en Amazon ECS esté disponible para los clientes de forma privada. Para obtener más información, consulte la sección Recursos relacionados.	Administrador de la nube

Crear un punto de conexión de VPC

Tarea	Descripción	Habilidades requeridas
Cree un punto de conexión de VPC.	Cree un punto de enlace de VPC para el punto de PrivateLink enlace de AWS que creó anteriormente. El nombre de dominio completo (FQDN) del punto final de la VPC apuntará al FQDN del punto final de AWS PrivateLink . Esto crea una interfaz de red elástica para el servicio de punto de conexión de VPC a la que pueden acceder los puntos de conexión del servicio de nombres de dominio.	Administrador de la nube

Crear la función de Lambda

Tarea	Descripción	Habilidades requeridas
Crear la función de Lambda.	Abra la consola de Lambda y cree una función de Lambda para actualizar las direcciones IP del equilibrador de carga de aplicación como destinos del equilibrador de carga de red. Para obtener más información, consulte la entrada del blog «Using static IP addresses for Application Load Balancers (Uso de direcciones IP estáticas para	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	los equilibradores de carga de aplicación)» en la sección Recursos relacionados.	

Recursos relacionados

Crear los equilibradores de carga:

- Crear un equilibrador de carga de red
- Creación de un equilibrador de carga de aplicación

Crear un sistema de archivos de Amazon EFS:

- Crear un sistema de archivos de Amazon EFS
- Crear destinos de montaje en Amazon EFS

Creación de un bucket de S3:

- Creación de un bucket de S3

Crear un secreto en Secrets Manager:

- Crear claves en AWS KMS
- Crear un secreto en AWS Secrets Manager

Crear una instancia de Amazon RDS:

- Crear una instancia de base de datos de Amazon RDS

Crear los componentes de Amazon ECS:

- Crear un clúster de Amazon ECS
- Crear una imagen de Docker
- Crear un repositorio de Amazon ECR

- Autenticar Docker con el repositorio de Amazon ECR
- Pasar una imagen a un repositorio de Amazon ECR
- Crear una definición de tarea de Amazon ECS
- Creación de un servicio de Amazon ECS

Configure AWS PrivateLink:

- Servicios de puntos finales de VPC (AWS) PrivateLink

Crear un punto de conexión de VPC:

- Puntos de enlace de interfaz de VPC (AWS) PrivateLink

Crear la función de Lambda:

- Crear una función de Lambda

Otros recursos:

- Uso de direcciones IP estáticas para los equilibradores de carga de aplicación
- Acceso seguro a los servicios a través de AWS PrivateLink

Acceda a aplicaciones de contenedores de forma privada en Amazon EKS mediante AWS PrivateLink y un Network Load Balancer

Creado por Kirankumar Chandrashekar (AWS)

Entorno: producción	Tecnologías: contenedores y microservicios; modernización DevOps; seguridad, identidad y cumplimiento	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon EKS; Amazon VPC		

Resumen

Este patrón describe cómo alojar de forma privada una aplicación contenedora de Docker en Amazon Elastic Kubernetes Service (Amazon EKS) detrás de un Network Load Balancer y cómo acceder a la aplicación mediante AWS. PrivateLink A continuación, puede utilizar una red privada para acceder de forma segura a los servicios de la nube de Amazon Web Services (AWS).

El clúster de Amazon EKS que ejecuta las aplicaciones de Docker, con un Network Load Balancer en la interfaz, se puede asociar a un punto final de nube privada virtual (VPC) para acceder a él a través de AWS. PrivateLink A continuación, este servicio de punto de conexión de VPC se puede compartir con otras VPC mediante sus puntos de conexión de VPC.

La configuración descrita por este patrón es una forma segura de compartir el acceso a las aplicaciones entre las VPC y las cuentas de AWS. No requiere configuraciones de enrutamiento ni conectividad especiales, ya que la conexión entre las cuentas del consumidor y del proveedor se encuentra en la red troncal global de AWS y no atraviesa la Internet pública.

Requisitos previos y limitaciones

Requisitos previos

- Docker, instalado y configurado en Linux, macOS o Windows.

- Una aplicación que se ejecuta en Docker.
- Una cuenta de AWS activa.
- Interfaz de la línea de comandos de AWS (AWS CLI) versión 2, instalada y configurada en Linux, macOS o Windows.
- Un clúster de Amazon EKS existente con subredes privadas etiquetadas y configurado para alojar aplicaciones. Para obtener más información, consulte Etiquetado de subredes en la documentación de Amazon EKS.
- Kubectl, instalado y configurado para acceder a los recursos de su clúster de Amazon EKS. Para más información, consulte Instalar kubectl en la documentación de Amazon EKS.

Arquitectura

Pila de tecnología

- Amazon EKS
- AWS PrivateLink
- Equilibrador de carga de red

Automatizar y escalar

- Los manifiestos de Kubernetes se pueden rastrear y administrar en un repositorio basado en Git (por ejemplo, en AWS CodeCommit), y se pueden implementar mediante la integración continua y la entrega continua (CI/CD) en AWS. CodePipeline
- Puede usar AWS CloudFormation para crear este patrón mediante el uso de infraestructura como código (IaC).

Herramientas

- AWS CLI: la interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que permite interactuar con los servicios de AWS mediante comandos en el intérprete de comandos de línea de comandos.

- Equilibrador de carga elástico: el equilibrador de carga elástico distribuye el tráfico entrante de red o de la aplicación entre varios destinos, por ejemplo, instancias de Amazon Elastic Compute Cloud (Amazon EC2), contenedores y direcciones IP en una o más zonas de disponibilidad.

- Amazon EKS: Amazon Elastic Kubernetes Service (Amazon EKS) es un servicio administrado que puede utilizar para ejecutar Kubernetes en AWS sin necesidad de instalar, operar ni mantener su propio plano de control o nodos de Kubernetes.
- Amazon VPC: Amazon Virtual Private Cloud (Amazon VPC) permite lanzar recursos de AWS en una red virtual previamente definida.
- Kubectl – Kubectl es una utilidad de línea de comandos para ejecutar comandos en clústeres de Kubernetes.

Epics

Implementar los archivos de manifiesto de implementación y servicio de Kubernetes

Tarea	Descripción	Habilidades requeridas
Cree el archivo de manifiesto de implementación de Kubernetes.	Cree un archivo de manifiesto de implementación modificando el siguiente archivo de muestra según sus necesidades. `apiVersion: apps/v1` `kind: Deployment` `metadata:` `  name: sample-app` `spec:` `  replicas: 3` `  selector:` `  matchLabels:` `  app: nginx` `  template:` `  metadata:` `  labels:` `  app: nginx` `  spec:`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	<pre>containers: - name: nginx image: public.ecr.aws/z9d2n7e1/nginx:1.19.5 ports: - name: http container Port: 80</pre> Nota: Esta es una muestra de archivo de configuración de NGINX que se implementa mediante la imagen de Docker de NGINX. Para obtener más información, consulte Cómo usar la imagen de Docker de NGINX en la documentación de Docker.	
Implemente el archivo de manifiesto de implementación de Kubernetes.	Ejecute el siguiente comando para aplicar el archivo de manifiesto de implementación a su clúster de Amazon EKS: `kubectl apply -f <your_deployment_file_name>`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Cree el archivo de manifiesto del servicio de Kubernetes.	Cree un archivo de manifiesto de servicio modificando el siguiente archivo de muestra según sus necesidades. `apiVersion: v1` `kind: Service` `metadata:` `  name: sample-service` `  annotations:` `  service.beta.kubernetes.io/aws-load-balancer-type: nlb` `  service.beta.kubernetes.io/aws-load-balancer-internal: "true"` `spec:` `  ports:` `  - port: 80` `  targetPort: 80` `  protocol: TCP` `  type: LoadBalancer` `  selector:` `  app: nginx` Importante: Asegúrese de incluir las siguiente `annotations` para definir un equilibrador de carga de red interno: `service.beta.kubernetes.io/aws-load-balancer-type: nlb` `service.beta.kubernetes.io/aws-l`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`oad-balancer-inter nal: "true"`	
Implemente el archivo de manifiesto del servicio de Kubernetes.	Ejecute el siguiente comando para aplicar el archivo de manifiesto de servicio a su clúster de Amazon EKS: `kubectl apply -f <your_service_file _name>`	DevOps ingeniero

Creación de los puntos de conexión

Tarea	Descripción	Habilidades requeridas
Registre el nombre del equilibrador de carga de red.	Ejecute el siguiente comando para recuperar el nombre del equilibrador de carga de red: `kubectl get svc sample-service -o wide` Registre el nombre del balanceador de carga de red, que es necesario para crear un PrivateLink punto de conexión de AWS.	DevOps ingeniero
Cree un PrivateLink punto de conexión de AWS.	Inicie sesión en la consola de administración de AWS, abra la consola de Amazon VPC y, a continuación, cree un punto de conexión de AWS PrivateLi nk . Al asociar este punto de	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	conexión al equilibrador de carga de red, la aplicación estará disponible de forma privada para los clientes. Para obtener más informaci ón, consulte los servicios de punto final de VPC PrivateLink (AWS) en la documentación de Amazon VPC. Importante: Si la cuenta de consumidor requiere acceso a la aplicación, el ID de cuenta de AWS de la cuenta de consumidor debe añadirse a la lista de directores permitido s para la configuración del PrivateLink punto de conexión de AWS. Para obtener más información, consulte Cómo añadir y eliminar permisos para el servicio de puntos de conexión en la documentación de Amazon VPC.	

Tarea	Descripción	Habilidades requeridas
Cree un punto de conexión de VPC.	En la consola de Amazon VPC, elija Endpoint Services y, a continuación, elija Create Endpoint Service. Cree un punto de enlace de VPC para el punto de enlace de AWS PrivateLink . El nombre de dominio completo (FQDN) del punto de enlace de VPC apunta al FQDN del punto de enlace de AWS. PrivateLink Esto crea una interfaz de red elástica para el servicio de puntos de conexión de VPC a la que pueden acceder los puntos de conexión de DNS.	Administrador de la nube

Recursos relacionados

- Uso de la imagen de Docker NGINX oficial
- Equilibrio de carga de red en Amazon EKS
- Creación de servicios de punto final de VPC (AWS) PrivateLink
- Cómo agregar y eliminar permisos para el servicio de punto de conexión

Activación de mTLS en AWS App Mesh con AWS Private CA en Amazon EKS

Creado por Omar Kahil (AWS), Emmanuel Saliu (AWS) y Muhammad Shahzad (AWS)

Entorno: PoC o piloto	Tecnologías: Contenedores y microservicios	Servicios de AWS: AWS App Mesh; Amazon EKS; AWS Certificate Manager (ACM)

Resumen

Este patrón muestra cómo implementar Mutual Transport Layer Security (mTLS) en Amazon Web Services (AWS) mediante certificados de AWS Private Certificate Authority (AWS Private CA) en AWS App Mesh. Utiliza la API del servicio de descubrimiento secreto (SDS) de Envoy a través del marco de identidad de producción seguro para todos (SPIFFE). SPIFFE es un proyecto de código abierto de Cloud Native Computing Foundation (CNCF) que cuenta con un amplio apoyo de la comunidad y que proporciona una gestión de identidades de la carga de trabajo detallada y dinámica. Para implementar los estándares de SPIFFE, utilice el entorno de tiempo de ejecución de SPIRE SPIFFE.

El uso de mTLS en App Mesh ofrece una autenticación entre pares bidireccional, ya que añade una capa de seguridad sobre TLS y permite que los servicios de la malla verifiquen el cliente que realiza la conexión. El cliente en la relación cliente-servidor también proporciona un certificado X.509 durante el proceso de negociación de la sesión. El servidor utiliza este certificado para identificar y autenticar al cliente. Esto ayuda a verificar si el certificado lo ha emitido una entidad de certificación (CA) de confianza y si el certificado es válido.

Requisitos previos y limitaciones

Requisitos previos

- Un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) con grupos de nodos autogestionados o gestionados
- Controlador App Mesh implementado en el clúster con el SDS activado
- Un certificado privado de AWS Certificate Manager (ACM) emitido por AWS Private CA

Limitaciones

- SPIRE no se puede instalar en AWS Fargate porque el agente de SPIRE debe ejecutarse como Kubernetes. DaemonSet

Versiones de producto

- Gráfico del controlador AWS App Mesh 1.3.0 o posterior

Arquitectura

El siguiente diagrama muestra el clúster de EKS con App Mesh en la VPC. El servidor SPIRE de un nodo de trabajo se comunica con los agentes de SPIRE de otros nodos de trabajo y con AWS Private CA. Envoy se utiliza para la comunicación mTLS entre los nodos de trabajo del agente SPIRE.

El siguiente diagrama muestra los siguientes pasos:

1. Se emite el certificado.
2. Solicite la firma y el certificado.

Herramientas

Servicios de AWS

- AWS Private CA: AWS Private Certificate Authority (AWS Private CA) permite la creación de jerarquías de entidades de certificación (CA) privadas, incluidas las entidades de certificación raíz y subordinadas, sin los costos de inversión y mantenimiento de operar una entidad de certificación en las instalaciones.
- AWS App Mesh: AWS App Mesh es una malla de servicios que facilita el monitoreo y el control de los servicios. App Mesh estandariza la forma en que se comunican sus servicios, ofreciendo visibilidad y controles de tráfico de red coherentes para cada microservicio en una aplicación.
- Amazon EKS: Amazon Elastic Kubernetes Service (Amazon EKS) es un servicio administrado que puede utilizar para ejecutar Kubernetes en AWS sin necesidad de instalar, operar ni mantener su propio plano de control o nodos de Kubernetes.

Otras herramientas

- Helm: Helm es un administrador de paquetes para Kubernetes que le ayuda a instalar y administrar aplicaciones en el clúster de Kubernetes. Este patrón usa Helm para implementar el controlador AWS App Mesh.
- Gráfico del controlador AWS App Mesh – Este patrón utiliza el gráfico del controlador AWS App Mesh para habilitar AWS App Mesh en Amazon EKS.

Epics

Configurar el entorno

Tarea	Descripción	Habilidades requeridas
Configure App Mesh con Amazon EKS.	Siga los pasos básicos de implementación que se proporcionan en el repositorio.	DevOps ingeniero
Instale SPIRE.	Instale SPIRE en el clúster EKS mediante spire_setup.yaml.	DevOps ingeniero
Instale el certificado de AWS Private CA.	Cree e instale un certificado para su raíz privada CA siguiendo las instrucciones de la documentación de AWS.	DevOps ingeniero
Conceda permisos al rol de instancia del nodo del clúster.	Para adjuntar políticas al rol de instancia del nodo del clúster, use el código que se encuentra en la sección de Información adicional.	DevOps ingeniero
Añada el complemento SPIRE para AWS Private CA.	Para añadir el complemento a la configuración del servidor SPIRE, utilice el código que se encuentra en la sección de Información adicional	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	. Sustituya el nombre de recursos de Amazon (ARN) `certificate_authority_arn` por su ARN de CA privado. El algoritmo de firma utilizado debe ser el mismo que el algoritmo de firma de la CA privada. Reemplace `your_region` por su región de AWS. Para obtener más información sobre el complemento, consulte el complemento del servidor: UpstreamAuthority «aws_pca».	
Actualice bundle.cert.	Tras crear el servidor SPIRE, se creará un archivo `spire-bundle.yaml` . Cambie el valor `bundle.crt` del archivo `spire-bundle.yaml` de la CA privada al certificado público.	DevOps ingeniero

Implementación y registro de las cargas de trabajo

Tarea	Descripción	Habilidades requeridas
Registre las entradas de nodos y cargas de trabajo con SPIRE.	Para registrar el nodo y la carga de trabajo (servicios) en el servidor SPIRE, utilice el código del repositorio.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Cree una malla en App Mesh con los mTLS activados.	Cree una nueva malla en App Mesh con todos los componentes de su aplicación de microservicios (por ejemplo, servicio virtual, router virtual y nodos virtuales).	DevOps ingeniero
Inspeccione las entradas registradas.	Puede inspeccionar las entradas registradas de sus nodos y cargas de trabajo ejecutando el siguiente comando. `kubectl exec -n spire spire-server-0 -- /opt/spire/bin/spire-server entry show` Esto mostrará las entradas de los agentes de SPIRE.	DevOps ingeniero

Verificar el tráfico de mTLS

Tarea	Descripción	Habilidades requeridas
Verifique el tráfico de mTLS.	1. Desde el servicio frontend, envíe un encabezado HTTP al servicio backend y verifique que la respuesta es correcta con los servicios registrados en SPIRE. 2. Para la autenticación TLS mutua, puede inspeccionar la estadística `ssl.hands`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`hake` ejecutando el siguiente comando. `kubectl exec -it $POD -n $NAMESPACE -c envoy -- curl http://localhost:9901/stats | grep ssl.handshake` Tras ejecutar el comando anterior, debería ver el recuento `ssl.handshake` de oyentes, que tendrá un aspecto similar al del siguiente ejemplo: `listener.0.0.0.0_15000.ssl.handshake: 2`	

Tarea	Descripción	Habilidades requeridas
Verifique que los certificados se emitan desde AWS Private CA.	Puede comprobar que los complementos se hayan configurado correctamente y que los certificados se están emitiendo desde su CA privada principal consultando los registros de su servidor SPIRE. Ejecute el siguiente comando de la . `kubectl logs spire-server-0 -n spire` A continuación, consulte los registros que se generan. Este código asume que su servidor se llama `spire-server-0` y está alojado en su espacio de nombres SPIRE. Debería comprobar que los complementos se hayan cargado correctamente y que se haya establecido una conexión con su CA privada de origen.	DevOps ingeniero

Recursos relacionados

- Uso de mTLS con SPIFFE/SPIRE en AWS App Mesh en Amazon EKS
- Habilitación de mTLS en AWS App Mesh mediante SPIFFE/SPIRE en un entorno Amazon EKS con varias cuentas
- Tutorial utilizado en este patrón
- Complemento de servidor: UpstreamAuthority «aws_pca»

- Inicio rápido para Kubernetes

Información adicional

Adjuntar permisos al rol de instancia del nodo del clúster

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ACMPCASigning",
            "Effect": "Allow",
            "Action": [
                "acm-pca:DescribeCertificateAuthority",
                "acm-pca:IssueCertificate",
                "acm-pca:GetCertificate",
                "acm:ExportCertificate"
            ],
            "Resource": "*"
        }
    ]
}
AWS Managed Policy: "AWSAppMeshEnvoyAccess"
```

Añadir el complemento SPIRE para ACM

```
Add the SPIRE plugin for ACM
Change certificate_authority_arn to your PCA ARN. The signing algorithm used must be
 the same as the signing algorithm on the PCA. Change your_region to the appropriate
 AWS Region.
UpstreamAuthority "aws_pca" {
    plugin_data {
        region = "your_region"
        certificate_authority_arn = "arn:aws:acm-pca:...."
        signing_algorithm = "your_signing_algorithm"
    }
}
```

Automatizar las copias de seguridad de las instancias de base de datos de Amazon RDS para PostgreSQL mediante AWS Batch

Documento creado por Kirankumar Chandrashekar (AWS)

Entorno: PoC o piloto	Tecnologías: contenedores y microservicios; bases de datos; DevOps	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon RDS; AWS Batch; Amazon CloudWatch; AWS Lambda; Amazon S3		

Resumen

Realizar copias de seguridad de las bases de datos de PostgreSQL es una tarea importante que, por lo general, se puede obtener mediante el programa de utilidad pg_dump, que usa el comando COPY de forma predeterminada para crear un esquema y un volcado de datos de una base de datos de PostgreSQL. Sin embargo, este proceso puede resultar repetitivo si necesita copias de seguridad periódicas de varias bases de datos de PostgreSQL. Si las bases de datos PostgreSQL están alojadas en la nube, también puede aprovechar la función automated backup de copia de seguridad automática que ofrece Amazon Relational Database Service (Amazon RDS) para PostgreSQL. Este patrón describe cómo automatizar las copias de seguridad periódicas de las instancias de base de datos de Amazon RDS para PostgreSQL mediante el programa de utilidad pg_dump.

Nota: En las instrucciones se parte del supuesto de que utiliza Amazon RDS. Sin embargo, también puede utilizar este enfoque para bases de datos PostgreSQL alojadas fuera de Amazon RDS. Para realizar copias de seguridad, la función de Lambda de AWS debe poder acceder a las bases de datos.

Un evento de Amazon CloudWatch Events basado en el tiempo inicia una función Lambda que busca etiquetas de respaldo específicas aplicadas a los metadatos de las instancias de base de datos de PostgreSQL en Amazon RDS. Si las instancias de base de datos de PostgreSQL tienen la etiqueta bkp:AutomatedDBDump = Active y otras etiquetas de backup obligatorias, la función de Lambda envía los trabajos individuales para cada copia de seguridad de la base de datos a AWS Batch.

AWS Batch procesa estos trabajos y carga los datos de copia de seguridad en un bucket de Amazon Simple Storage Service (Amazon S3). En este patrón se utiliza un Dockerfile y un archivo entrypoint.sh para crear una imagen de contenedor de Docker que se usa para realizar copias de seguridad en el trabajo de AWS Batch. Una vez finalizado el proceso de copia de seguridad, AWS Batch registra los detalles de la copia de seguridad en una tabla de inventario de Amazon DynamoDB. Como medida de seguridad adicional, un evento de CloudWatch eventos inicia una notificación de Amazon Simple Notification Service (Amazon SNS) si un trabajo falla en AWS Batch.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Un entorno informático existente, administrado o no administrado. Para obtener más información, consulte Entornos informáticos administrados y no administrados en la documentación de AWS Batch.
- Imagen de Docker de la Interfaz de la línea de comandos (CLI) de AWS, versión 2, instalada y configurada.
- Instancias de base de datos de Amazon RDS para PostgreSQL existentes.
- Un bucket de S3 existente.
- Docker, instalado y configurado en Linux, macOS o Windows.
- Familiaridad con la codificación en Lambda.

Arquitectura

Pila de tecnología

- CloudWatch Eventos de Amazon
- Amazon DynamoDB
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon RDS
- Amazon SNS
- Amazon S3

- AWS Batch
- AWS Key Management Service (AWS KMS)
- AWS Lambda
- AWS Secrets Manager
- Docker

Herramientas

- Amazon CloudWatch Events — CloudWatch Events ofrece una transmisión casi en tiempo real de los eventos del sistema que describen los cambios en los recursos de AWS.
- Amazon DynamoDB: DynamoDB es un servicio de base de datos NoSQL totalmente administrado que ofrece un rendimiento rápido y predecible, así como una perfecta escalabilidad.
- Amazon ECR: Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor de AWS administrado que es seguro, escalable y fiable.
- Amazon RDS: Amazon Relational Database Service (Amazon RDS) es un servicio web que facilita la configuración, el funcionamiento y el escalado de una base de datos relacional en la nube de AWS.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) es un servicio administrado que proporciona la entrega de mensajes de los publicadores a los suscriptores.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet.
- AWS Batch: AWS Batch facilita poder ejecutar cargas de trabajo informáticas por lotes en la nube de AWS.
- AWS KMS – AWS Key Management Service (AWS KMS) es un servicio administrado que permite crear y controlar fácilmente las claves de cifrado que se utilizan para cifrar datos.
- AWS Lambda: Lambda es un servicio informático que facilita poder ejecutar código sin aprovisionar ni administrar servidores.
- AWS Secrets Manager: Secrets Manager permite reemplazar las credenciales codificadas en el código, incluidas las contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación.
- Docker: Docker facilita a los desarrolladores empaquetar, enviar y ejecutar cualquier aplicación como un contenedor ligero, portátil y autosuficiente.

Las instancias de base de datos de PostgreSQL en Amazon RDS deben tener etiquetas aplicadas a sus metadatos. La función de Lambda busca etiquetas para identificar las instancias de base de datos de las que se debe hacer una copia de seguridad y, por lo general, se utilizan las siguientes etiquetas.

Etiqueta	Descripción
bkp:AutomatedDBDump = Active	Identifica una instancia de base de datos de Amazon RDS como candidata para realizar copia de seguridad.
bkp: = AutomatedBackupSecret <secret_name>	Identifica el secreto de Secrets Manager que contiene las credenciales de inicio de sesión de Amazon RDS.
bkp:AutomatedDBDumpS3Bucket = <s3_bucket_name>	Identifica el bucket de S3 al que se enviarán las copias de seguridad.
bkp: base de datos automatizada DumpFrequency BKP: base de datos automatizada DumpTime	Identifica la frecuencia y las horas en las que se deben hacer copias de seguridad de las bases de datos.
bkp:pgdumpcommand = <pgdump_command>	Identifica las bases de datos para las que se deben realizar las copias de seguridad.

Epics

Crear una tabla de inventario en DynamoDB

Tarea	Descripción	Habilidades requeridas
Cree una tabla en DynamoDB.	Inicie sesión en la Consola de administración de AWS, abra la consola de Amazon DynamoDB y cree una tabla. Para obtener ayuda con esta y otras explicaciones, consulte	Administrador de la nube, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	la sección Recursos relaciona dos.	
Confirme que se creó la tabla.	Ejecute el comando `aws dynamodb describe-table --table-name <table-name> | grep TableStatus` . Si la tabla existe, el comando devolverá el resultado `"TableStatus": "ACTIVE",` .	Administrador de la nube, administrador de bases de datos

Cree un tema de SNS para los eventos de trabajo con errores en AWS Batch

Tarea	Descripción	Habilidades requeridas
Cree un tema de SNS.	Abra la consola de Amazon SNS, seleccione Topics (Temas) y cree un tema de SNS con el nombre `JobFailedAlert` . Suscríbase al tema con una dirección de correo electrónico activa y compruebe su bandeja de entrada para confirmar que llegue el correo electrónico de suscripción a SNS de AWS Notifications.	Administrador de la nube
Cree una regla de eventos de trabajo con errores para AWS Batch.	Abre la CloudWatch consola de Amazon, selecciona Eventos y, a continuación, selecciona Crear regla. Seleccione Show advanced options (Mostrar opciones	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	avanzadas) y, a continuac ión, Edit (Editar). En Build a pattern that selects events for processing by your targets (Crear un patrón que seleccione eventos para procesar por los destinos) , sustituya el texto que aparezca con el código de «Failed job event» (Evento de trabajo con errores) de la sección Información adicional . Este código define una regla de CloudWatch eventos que se inicia cuando AWS Batch tiene un `Failed` evento.	
Agregue el destino de la regla del evento.	En Targets (Destinos), seleccione Add target (Agregar destino) y, a continuación, el tema de SNS `JobFailedAlert` . Configure los detalles restantes y cree la regla de eventos de Cloudwatch.	Administrador de la nube

Crear una imagen de Docker y pasarla a un repositorio de Amazon ECR

Tarea	Descripción	Habilidades requeridas
Cree un repositorio de Amazon ECR.	Abra la consola de Amazon ECR y seleccione la región de AWS donde desee crear el repositorio. Seleccione Repositories (Repositorios)	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	y, a continuación, Create repository (Crear repositorio). Configure el repositorio según los requisitos.	
Cree un Dockerfile.	Inicie sesión en Docker y utilice «Sample Dockerfile» (Dockerfile de muestra) y «Sample entrypoint.sh file» (Archivo entrypoint.sh de muestra) de la sección de Información adicional para crear un Dockerfile.	DevOps ingeniero
Cree una imagen de Docker y pásela a un repositorio de Amazon ECR.	Cree el Dockerfile en una imagen de Docker y pásela a un repositorio de Amazon ECR. Para obtener ayuda con esta y otras explicaciones, consulte la sección Recursos relacionados.	DevOps ingeniero

Crear los componentes de AWS Batch

Tarea	Descripción	Habilidades requeridas
Cree una definición de trabajo de AWS Batch.	Abra la consola de AWS Batch y cree una definición de trabajo que incluya el identificador uniforme de recursos (URI) del repositorio de Amazon ECR como la propiedad `Image`.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Configure la cola de trabajos de AWS Batch.	En la consola de AWS Batch, seleccione Job queues (Colas de trabajos) y, a continuación, Create queue (Crear cola). Cree una cola de trabajos que almacene los trabajos hasta que AWS Batch los ejecute en los recursos del entorno informático. Importante: Asegúrese de escribir la lógica para que AWS Batch registre los detalles de la copia de seguridad en la tabla de inventario de DynamoDB.	Administrador de la nube

Crear y programar una función de Lambda

Tarea	Descripción	Habilidades requeridas
Cree una función de Lambda para buscar etiquetas.	Cree una función de Lambda que busque etiquetas en las instancias de base de datos de PostgreSQL e identifique los candidatos a copia de seguridad. Asegúrese de que la función de Lambda pueda identificar la etiqueta `bkp:AutomatedDBDump = Active` y todas las demás etiquetas necesarias. Importante: La función de Lambda también debe poder agregar trabajos a la cola de trabajo de AWS Batch.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Crea un evento de CloudWatch eventos basado en el tiempo.	Abra la CloudWatch consola de Amazon y cree un evento CloudWatch Events que utilice una expresión cron para ejecutar la función Lambda de forma regular. Importante: Todos los eventos programados utilizan la zona horaria UTC.	Administrador de la nube

Probar la automatización de las copias de seguridad

Tarea	Descripción	Habilidades requeridas
Cree una clave de Amazon KMS.	Abra la consola de Amazon KMS y cree una clave de KMS que pueda usarse para cifrar las credenciales de Amazon RDS almacenadas en AWS Secrets Manager.	Administrador de la nube
Crear un secreto de AWS Secrets Manager.	Abra la consola de AWS Secrets Manager y guarde en secreto las credenciales de la base de datos de Amazon RDS para PostgreSQL.	Administrador de la nube
Agregue las etiquetas necesarias a las instancias de base de datos de PostgreSQL.	Abra la consola de Amazon RDS y agregue etiquetas a las instancias de base de datos de PostgreSQL de las que desee hacer una copia de seguridad automática. Puede utilizar las etiquetas de la tabla de la sección Tools	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	(Herramientas). Si necesita copias de seguridad de varias bases de datos de PostgreSQL dentro de la misma instancia de Amazon RDS, utilice `-d test:-d test1` como valor para la etiqueta `bkp:pgdumpcommand` . Importante: `test` y `test1` son nombres de bases de datos. Compruebe que no quede ningún espacio después de los dos puntos (:).	
Verifique la automatización de la copia de seguridad.	Para verificar la automatización de la copia de seguridad , puede invocar la función de Lambda o esperar a que comience la programación de la copia de seguridad. Una vez finalizado el proceso de copia de seguridad, compruebe que la tabla de inventario de DynamoDB tenga una entrada de copia de seguridad válida para las instancias de base de datos de PostgreSQL. Si coinciden, el proceso de automatización de la copia de seguridad se ha realizado correctamente.	Administrador de la nube

Recursos relacionados

Crear una tabla de inventario en DynamoDB

- Crear una tabla de Amazon DynamoDB

Crear un tema de SNS para los eventos de trabajo con errores en AWS Batch

- Crear un tema de Amazon SNS
- Enviar alertas de SNS sobre eventos de trabajo con errores en AWS Batch

Crear una imagen de Docker y pasarla a un repositorio de Amazon ECR

- Crear un repositorio de Amazon ECR
- Escribir un Dockerfile, crear una imagen de Docker y pasarla a Amazon ECR

Crear los componentes de AWS Batch

- Crear una definición de trabajo de AWS Batch
- Configurar el entorno informático y la cola de trabajos de AWS Batch
- Crear una cola de trabajos en AWS Batch

Crear una función de Lambda

- Crear una función de Lambda y escribir código
- Usar Lambda con DynamoDB

Cree un evento de eventos CloudWatch

- Crea un evento de CloudWatch eventos basado en el tiempo
- Utilizar expresiones cron en eventos de Cloudwatch

Probar la automatización de las copias de seguridad

- Crear una clave de Amazon KMS
- Crear un secreto en Secrets Manager
- Agregar etiquetas a una instancia de Amazon RDS

Información adicional

Evento de trabajo con errores:

```
{
  "detail-type": [
    "Batch Job State Change"
  ],
  "source": [
    "aws.batch"
  ],
  "detail": {
    "status": [
      "FAILED"
    ]
  }
}
```

Dockerfile de muestra:

```
FROM alpine:latest
RUN apk --update add py-pip postgresql-client jq bash && \
pip install awscli && \
rm -rf /var/cache/apk/*
ADD entrypoint.sh /usr/bin/
RUN chmod +x /usr/bin/entrypoint.sh
ENTRYPOINT ["entrypoint.sh"]
```

Archivo entrypoint.sh de muestra:

```
 #!/bin/bash
set -e
DATETIME=`date +"%Y-%m-%d_%H_%M"`
```

```
FILENAME=RDS_PostGres_dump_${RDS_INSTANCE_NAME}
FILE=${FILENAME}_${DATETIME}

aws configure --profile new-profile set role_arn arn:aws:iam::${TargetAccountId}:role/
${TargetAccountRoleName}
aws configure --profile new-profile set credential_source EcsContainer

echo "Central Account access provider IAM role is: "
aws sts get-caller-identity

echo "Target Customer Account access provider IAM role is: "
aws sts get-caller-identity --profile new-profile

securestring=$(aws secretsmanager get-secret-value --secret-id $SECRETID --output json
 --query 'SecretString' --region=$REGION --profile new-profile)

if [[ ${securestring} ]]; then
    echo "successfully accessed secrets manager and got the credentials"
    export PGPASSWORD=$(echo $securestring | jq --raw-output | jq -r '.DB_PASSWORD')
    PGSQL_USER=$(echo $securestring | jq --raw-output | jq -r '.DB_USERNAME')
    echo "Executing pg_dump for the PostGres endpoint ${PGSQL_HOST}"
    # pg_dump -h $PGSQL_HOST -U $PGSQL_USER -n dms_sample | gzip -9 -c  | aws s3 cp -
 --region=$REGION  --profile new-profile s3://$BUCKET/$FILE
    # in="-n public:-n private"
    IFS=':' list=($EXECUTE_COMMAND);
    for command in "${list[@]}";
      do
        echo $command;
        pg_dump -h $PGSQL_HOST -U $PGSQL_USER ${command} | gzip -9 -c  | aws s3 cp - --
region=$REGION --profile new-profile s3://${BUCKET}/${FILE}-${command}".sql.gz"
        echo $?;
        if  [[ $? -ne 0 ]]; then
            echo "Error occurred in database backup process. Exiting now....."
            exit 1
        else
            echo "Postgresql dump was successfully taken for the RDS endpoint
 ${PGSQL_HOST} and is uploaded to the following S3 location s3://${BUCKET}/${FILE}-
${command}.sql.gz"
            #write the details into the inventory table in central account
            echo "Writing to DynamoDB inventory table"
            aws dynamodb put-item --table-name ${RDS_POSTGRES_DUMP_INVENTORY_TABLE} --
region=$REGION --item '{ "accountId": { "S": "'"${TargetAccountId}"'" }, "dumpFileUrl":
 {"S": "'"s3://${BUCKET}/${FILE}-${command}.sql.gz"'" }, "DumpAvailableTime": {"S":
 "'"`date +"%Y-%m-%d::%H::%M::%S"` UTC"'"}}'
```

```
            echo $?
            if  [[ $? -ne 0 ]]; then
                echo "Error occurred while putting item to DynamoDb Inventory Table.
 Exiting now....."
                exit 1
            else
                echo "Successfully written to DynamoDb Inventory Table
 ${RDS_POSTGRES_DUMP_INVENTORY_TABLE}"
            fi
        fi
      done;
else
    echo "Something went wrong {$?}"
    exit 1
fi

exec "$@"
```

Automatice la implementación de Node Termination Handler en Amazon EKS mediante una canalización de CI/CD

Creado por Sandip Gangapadhyay (AWS), John Vargas (AWS), Practideep Singh (AWS), Sandeep Gawande (AWS) y Viyoma Sachdeva (AWS)

Repositorio de código: despliegue NTH en EKS	Entorno: producción	Tecnologías: contenedores y microservicios; DevOps
Servicios de AWS: AWS CodePipeline; Amazon EKS; AWS CodeBuild		

Resumen

En la nube de Amazon Web Services (AWS), puede utilizar AWS Node Termination Handler, un proyecto de código abierto, para administrar eficazmente el cierre de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en Kubernetes. AWS Node Termination Handler ayuda a garantizar que el plano de control de Kubernetes responda adecuadamente a los eventos que pueden provocar que la instancia de EC2 deje de estar disponible. Dichos eventos incluyen lo siguiente:

- Mantenimiento programado de la instancia EC2
- Eventos de interrupción de instancias de spot de Amazon EC2
- El grupo de escalado automático se reduce horizontalmente
- Reequilibrio de grupos de escalado automático en todas las zonas de disponibilidad
- Terminación de la instancia EC2 mediante la API o la consola de administración de AWS

Si no se gestiona un evento, es posible que el código de su aplicación no se detenga correctamente. También puede tardar más en recuperar la disponibilidad total o programar accidentalmente el trabajo en los nodos que están dejando de funcionar. El (NTH) `aws-node-termination-handler` puede funcionar en dos modos diferentes: servicio de metadatos de instancias (IMDS) o procesador de colas. Para obtener más información acerca de los dos modos, consulte el archivo Léame.

Este patrón automatiza la implementación de NTH mediante el uso del procesador de cola a través de una canalización de integración y entrega continuas (CI/CD).

Nota: Si utiliza grupos de nodos gestionados por EKS, no necesita `aws-node-termination-handler`.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Un navegador web compatible para su uso con la consola de administración de AWS. Consulte la lista de los navegadores compatibles.
- AWS Cloud Development Kit (AWS CDK), instalado.
- `kubectl`, la herramienta de línea de comandos de Kubernetes, instalada.
- `eksctl`, la interfaz de la línea de comandos de AWS (AWS CLI) para Amazon Elastic Kubernetes Service (Amazon EKS), instalada.
- Un clúster de EKS en ejecución con la versión 1.20 o posterior.
- Grupo de nodos autogestionados adjunto al clúster de EKS. Para crear un clúster de Amazon EKS con un grupo de nodos autogestionado, ejecute el siguiente comando.

```
eksctl create cluster --managed=false --region <region> --name <cluster_name>
```

  Para obtener más información sobre `eksctl`, consulte la documentación de eksctl.
- Proveedor de OpenID Connect (OIDC) de AWS Identity and Access Management (IAM) para su clúster. Para obtener más información, consulte Creación de un proveedor OIDC de IAM para su clúster.

Limitaciones

- Debe utilizar una región de AWS que sea compatible con el servicio Amazon EKS.

Versiones de producto

- Versión de Kubernetes 1.20 o posterior
- `eksctl` versión 0.107.0 o posterior
- CDK de AWS, versión 2.27.0 o posterior

Arquitectura

Pila de tecnología de destino

- Una nube privada virtual (VPC)
- Un Clúster de EKS
- Amazon Simple Queue Service (Amazon SQS)
- IAM
- Kubernetes

Arquitectura de destino

El siguiente diagrama muestra una vista general de los end-to-end pasos necesarios para iniciar la terminación del nodo.

El flujo de trabajo que se muestra en el diagrama consta de los siguientes pasos de alto nivel:

1. El evento de terminación de la instancia EC2 con escalado automático se envía a la cola de SQS.
2. El NTH Pod supervisa los mensajes nuevos en la cola de SQS.
3. El NTH Pod recibe el nuevo mensaje y hace lo siguiente:
   - Acordona el nodo para que el nuevo pod no se ejecute en él.
   - Drena el nodo para evacuar el módulo existente
   - Envía una señal de enlace de ciclo de vida al grupo de escalado automático para que se pueda terminar el nodo.

Automatizar y escalar

- El código lo administra e implementa AWS CDK, con el respaldo de pilas CloudFormation anidadas de AWS.
- El plano de control de Amazon EKS se ejecuta en varias zonas de disponibilidad para garantizar una alta disponibilidad.
- Para el escalado automático, Amazon EKS admite el escalador automático de clústeres de Kubernetes y Karpenter.

Herramientas

Servicios de AWS

- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura de la nube de AWS en código.
- AWS CodeBuild es un servicio de compilación totalmente gestionado que le ayuda a compilar código fuente, ejecutar pruebas unitarias y producir artefactos listos para su implementación.
- AWS CodeCommit es un servicio de control de versiones que le ayuda a almacenar y gestionar repositorios de Git de forma privada, sin necesidad de gestionar su propio sistema de control de código fuente.
- AWS le CodePipeline ayuda a modelar y configurar rápidamente las diferentes etapas de una versión de software y a automatizar los pasos necesarios para publicar cambios de software de forma continua.
- Amazon Elastic Kubernetes Service (Amazon EKS) le ayuda a ejecutar Kubernetes en AWS sin necesidad de instalar ni mantener su propio plano de control o nodos de Kubernetes.
- Amazon EC2 Auto Scaling le ayuda a mantener disponible la aplicación y le permite añadir o quitar automáticamente instancias de Amazon EC2 según las condiciones que defina.
- Amazon Simple Queue Service (Amazon SQS) ofrece una cola alojada segura, duradera y disponible que le permite integrar y desacoplar sistemas y componentes de software distribuidos.

Otras herramientas

- kubectl: es una herramienta de línea de comandos para la ejecución de comandos en clústeres de Kubernetes. Puede usar kubectl para implementar aplicaciones, inspeccionar y administrar los recursos del clúster y ver los registros.

Código

El código de este patrón está disponible en el deploy-nth-to-eksrepositorio de GitHub .com. El repositorio de código contiene los siguientes archivos y carpetas.

- `nth folder`— El diagrama de Helm, los archivos de valores y los scripts para escanear e implementar la CloudFormation plantilla de AWS para Node Termination Handler.
- `config/config.json`: el archivo de parámetros de configuración de la aplicación. Este archivo contiene todos los parámetros necesarios para implementar el CDK.

- `cdk`: el código fuente del CDK de AWS.
- `setup.sh`: el script utilizado para implementar la aplicación del CDK de AWS para crear la canalización de CI/CD necesaria y otros recursos necesarios.
- `uninstall.sh`: el script utilizado para limpiar los recursos.

Para usar el código de muestra, siga las instrucciones en la sección Epics .

Prácticas recomendadas

Para conocer las prácticas recomendadas a la hora de automatizar AWS Node Termination Handler, consulte lo siguiente:

- Guías de prácticas recomendadas de EKS
- Node Termination Handler: configuración

Epics

Configure su entorno

Tarea	Descripción	Habilidades requeridas
Clone el repositorio.	Para clonar el repositorio mediante SSH (Secure Shell), ejecute el siguiente comando. `git clone git@github.com:aws-samples/deploy-nth-to-eks.git` Para clonar el repositorio mediante HTTPS, ejecute el siguiente comando. `git clone https://github.com/aws-samples/deploy-nth-to-eks.git`	Desarrollador de aplicaciones, AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Al clonar el repositorio se crea una carpeta llamada `deploy-nth-to-eks` . Cambie a ese directorio. `cd deploy-nth-to-eks`	
Configure el archivo kubeconfig.	Configure sus credenciales de AWS en su terminal y confirme que tiene derechos para asumir el rol de clúster. Puede utilizar el siguiente código de ejemplo. `aws eks update-kubeconfig --name <Cluster_Name> --region <region>--role-arn <Role_ARN>`	AWS DevOps, DevOps ingeniero, desarrollador de aplicaciones

Implemente el proceso de CI/CD

Tarea	Descripción	Habilidades requeridas
Establezca los parámetros.	Configure los siguientes parámetros obligatorios en el archivo `config/config.json` . • `pipelineName` : el nombre de la canalización de CI/CD que va a crear el CDK de AWS (por ejemplo, `deploy-nth-`	Desarrollador de aplicaciones, AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`to-eks-pipeline`). AWS CodePipeline creará una canalización con este nombre. • `repositoryName` : El CodeCommit repositorio de AWS que se va a crear (por ejemplo,`deploy-nth-to-eks-repo`). El CDK de AWS creará este repositorio y lo configurará como fuente de la canalización de CI/CD. Nota: Esta solución creará este CodeCommit repositorio y la rama (que se proporciona en el siguiente parámetro de rama). • `branch`: el nombre de rama del repositorio (por ejemplo, `main`). Una confirmación con esta rama iniciará la canalización de CI/CD. • `cfn_scan_script` : la ruta del script que se utilizará para escanear la CloudFormation plantilla de AWS en busca de NTH (`scan.sh`). Este script existe en `nth` una carpeta que formará parte del CodeCommit repositorio de AWS.	

Tarea	Descripción	Habilidades requeridas
	• `cfn_deploy_scrip t`: la ruta del script que se utilizará para implement ar la CloudFormation plantilla de AWS para NTH (`installApp.sh`). • `stackName` : El nombre de la CloudFormation pila que se va a implementar. • `eksClusterName` : el nombre del clúster de EKS existente. • `eksClusterRole` : el rol de IAM que se utilizará para acceder al clúster de EKS para todas las llamadas a la API de Kubernetes (por ejemplo, `clusterad min`). Por lo general, este rol se agrega en `aws-auth ConfigMap` . • `create_cluster_rol e` : para crear el rol de IAM `eksClusterRole` , escriba sí. Si desea proporcionar un rol de clúster existente en el parámetro `eksCluste rRole` , escriba no. • `create_iam_oidc_pr ovider` : para crear un proveedor de OIDC de IAM para su clúster, escriba sí. Si ya existe un proveedor	

Tarea	Descripción	Habilidades requeridas
	de IAM OIDC, escriba no. Para obtener más información, consulte Creación de un proveedor OIDC de IAM para su clúster. • `AsgGroupName` : una lista separada por comas de los nombres de los grupos de escalado automático que forman parte del clúster de EKS (por ejemplo, `ASG_Group_1,ASG_Group_2`). • `region`: el nombre de la región de AWS donde se encuentra el clúster (por ejemplo, `us-east-2`). • `install_cdk` : si el CDK de AWS no está instalado actualmente en el equipo, escriba sí. Ejecute el comando `cdk --version` para comprobar si la versión del CDK de AWS instalada es 2.27.0 o posterior. En ese caso, escriba no. Si escribe sí, el script setup.sh ejecutará el comando `sudo npm install -g cdk@2.27.0` para instalar el CDK de AWS en el equipo. El script	

Tarea	Descripción	Habilidades requeridas
	requiere permisos sudo, por lo que debe proporcionar la contraseña de la cuenta cuando se le solicite.	
Cree la canalización de CI/CD para implementar NTH.	Ejecute el script setup.sh. `./setup.sh` El script implementará la aplicación AWS CDK que creará el CodeCommit repositorio con el código de ejemplo, la canalización y los CodeBuild proyectos en función de los parámetros ingresados por el usuario en `config/config.json` el archivo. Este script solicitará la contraseña cuando instale los paquetes npm con el comando sudo.	Desarrollador de aplicaciones, AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Revise la canalización de CI/CD.	Abra la consola de administración de AWS y revise los siguientes recursos creados en la pila. • CodeCommit repositorio con el contenido de la carpeta `nth` • CodeBuild Proyecto AWS`cfn-scan`, que escaneará la CloudFormation plantilla en busca de vulnerabilidades. • CodeBuild proyecto`Nth-Deploy` , que implementará la CloudFormation plantilla de AWS y los gráficos de NTH Helm correspondientes a través de la CodePipeline canalización de AWS. • Una CodePipeline canalización para implementar NTH. Una vez que la canalización se ejecute correctamente, la versión de Helm `aws-node-termination-handler` se instala en el clúster de EKS. Además, se está ejecutando un pod denominado `aws-node-termination-handler` en el espacio	Desarrollador de aplicaciones, AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	de nombres `kube-system` del clúster.	

Pruebe la implementación de NTH

Tarea	Descripción	Habilidades requeridas
Simule un evento de escalado de grupo de escalado automático.	Para simular un evento de reducción horizontal del escalado automático, haga lo siguiente: 1. En la consola de AWS, abra la consola EC2 y elija grupo de escalado automático. 2. Seleccione el grupo de escalado automático que tenga el mismo nombre que el proporcionado en `config/config.json` y elija Editar. 3. Reduzca la capacidad deseada y mínima en 1. 4. Seleccione Actualizar.	
Revise los registros.	Durante el evento de reducción horizontal, el NTH Pod acordonará y drenará el nodo de trabajo correspon diente (la instancia EC2 que se cancelará como parte del evento de reducción horizontal). Para comprobar los registros, utilice el código	Desarrollador de aplicacio nes, AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	de la sección Información adicional.	

Limpieza

Tarea	Descripción	Habilidades requeridas
Limpieza de todos los recursos de AWS.	Para limpiar los recursos creados por este patrón, ejecute el siguiente comando. `./uninstall.sh` Esto limpiará todos los recursos creados en este patrón al eliminar la CloudFormation pila.	DevOps ingeniero

Solución de problemas

Problema	Solución
El registro npm no está configurado correctam ente.	Durante la instalación de esta solución, el script instala npm install para descargar todos los paquetes necesarios. Si, durante la instalaci ón, ve un mensaje que dice “No se puede encontrar el módulo”, es posible que el registro npm no esté configurado correctamente. Para ver la configuración actual del registro, ejecute el siguiente comando. `npm config get registry`

Problema	Solución
	Ejecute el siguiente comando para establecer el registro con `https://registry.npmjs.org/` . `npm config set registry https://registry.npmjs.org`
Retrasar la entrega del mensaje SQS.	Como parte de la solución de problemas, si desea retrasar la entrega de los mensajes de SQS a NTH Pod, puede ajustar el parámetro de retraso de entrega de SQS. Para obtener más información, consulte Colas de retraso de Amazon SQS.

Recursos relacionados

- Código fuente de AWS Node Termination Handler
- Taller de EC2
- AWS CodePipeline
- Amazon Elastic Kubernetes Service (Amazon EKS)
- AWS Cloud Development Kit
- AWS CloudFormation

Información adicional

1. Busque el nombre del NTH Pod.

```
kubectl get pods -n kube-system |grep aws-node-termination-handler
aws-node-termination-handler-65445555-kbqc7   1/1     Running   0          26m
kubectl get pods -n kube-system |grep aws-node-termination-handler
aws-node-termination-handler-65445555-kbqc7   1/1     Running   0          26m
```

2. Consulte los registros. Un registro de ejemplo se ve del siguiente modo. Muestra que el nodo ha sido acordonado y drenado antes de enviar la señal de finalización del enlace de ciclo de vida del grupo de escalado automático.

```
kubectl -n kube-system logs aws-node-termination-handler-65445555-kbqc7
022/07/17 20:20:43 INF Adding new event to the event store
 event={"AutoScalingGroupName":"eksctl-my-cluster-target-nodegroup-
ng-10d99c89-NodeGroup-ZME36IGAP7O1","Description":"ASG Lifecycle Termination
 event received. Instance will be interrupted at 2022-07-17 20:20:42.702
 +0000 UTC \n","EndTime":"0001-01-01T00:00:00Z","EventID":"asg-lifecycle-
term-33383831316538382d353564362d343332362d613931352d383430666165636334333564","InProgress":fal
east-2.compute.internal","NodeProcessed":false,"Pods":null,"ProviderID":"aws:///us-
east-2c/i-0409f2a9d3085b80e","StartTime":"2022-07-17T20:20:42.702Z","State":""}
2022/07/17 20:20:44 INF Requesting instance drain event-id=asg-lifecycle-
term-33383831316538382d353564362d343332362d613931352d383430666165636334333564
 instance-id=i-0409f2a9d3085b80e kind=SQS_TERMINATE node-name=ip-192-168-75-60.us-
east-2.compute.internal provider-id=aws:///us-east-2c/i-0409f2a9d3085b80e
2022/07/17 20:20:44 INF Pods on node node_name=ip-192-168-75-60.us-
east-2.compute.internal pod_names=["aws-node-qchsw","aws-node-termination-
handler-65445555-kbqc7","kube-proxy-mz5x5"]
2022/07/17 20:20:44 INF Draining the node
2022/07/17 20:20:44 ??? WARNING: ignoring DaemonSet-managed Pods: kube-system/aws-node-
qchsw, kube-system/kube-proxy-mz5x5
2022/07/17 20:20:44 INF Node successfully cordoned and drained
 node_name=ip-192-168-75-60.us-east-2.compute.internal reason="ASG Lifecycle
 Termination event received. Instance will be interrupted at 2022-07-17 20:20:42.702
 +0000 UTC \n"
2022/07/17 20:20:44 INF Completed ASG Lifecycle Hook (NTH-K8S-TERM-HOOK) for instance
 i-0409f2a9d3085b80e
```

Crear e implementar de forma automática una aplicación Java en Amazon EKS mediante una canalización de CI/CD

Creado por MAHESH RAGHUNANDANAN (AWS), James Radtke (AWS) y Jomcy Pappachen (AWS)

Repositorio de código: aws-cicd-java-eks	Entorno: producción	Tecnologías: contenedores y microservicios; nativas de la nube; Modernización DevOps
Carga de trabajo: todas las demás cargas de trabajo	Servicios de AWS: AWS CloudFormation; AWS CodeCommit CodePipeline; Amazon EC2 Container Registry; Amazon EKS	

Resumen

Este patrón describe cómo crear una canalización de integración y entrega continuas (CI/CD) que cree e implemente automáticamente una aplicación Java con DevSecOps las prácticas recomendadas en un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) en la nube de Amazon Web Services (AWS). Este patrón utiliza una aplicación de saludo desarrollada con un marco Java Spring Boot y que utiliza Apache Maven.

Puede utilizar el enfoque de este patrón para crear el código de una aplicación Java, empaquetar los artefactos de la aplicación como una imagen de Docker, escanear la imagen por motivos de seguridad y cargarla como un contenedor de carga de trabajo en Amazon EKS. El enfoque de este patrón es útil si desea migrar de una arquitectura monolítica estrechamente acoplada a una arquitectura de microservicios. Este enfoque también le ayuda a supervisar y gestionar todo el ciclo de vida de una aplicación Java, lo que garantiza un mayor nivel de automatización y ayuda a evitar errores o fallos.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.

- Interfaz de la línea de comandos de AWS (AWS CLI) versión 2 instalada y configurada. Para obtener más información, consulte Instalación, actualización y desinstalación de la versión 2 de la CLI de AWS en la documentación de la CLI de AWS.
- La versión 2 de la CLI de AWS debe configurarse con el mismo rol de IAM que crea el clúster de Amazon EKS, ya que solo esa función está autorizada a añadir otras funciones de IAM al `aws-auth ConfigMap`. Para obtener información y los pasos para configurar la CLI de AWS, consulte Conceptos básicos de configuración en la documentación de la CLI de AWS.
- Funciones y permisos de AWS Identity and Access Management (IAM) con acceso total a AWS CloudFormation. Para obtener más información al respecto, consulte Controlar el acceso con IAM en la CloudFormation documentación de AWS.
- Un clúster de Amazon EKS existente, con detalles del nombre del rol de IAM y el nombre de recurso de Amazon (ARN) del rol de IAM de los nodos de trabajo del clúster de EKS.
- Escalador automático de clústeres de Kubernetes instalado y configurado en su clúster de Amazon EKS. Para obtener más información, consulte Escalado automático de clústeres en la documentación de Amazon EKS.
- Acceso al código del GitHub repositorio.

Notas importantes

AWS Security Hub se habilita como parte de las CloudFormation plantillas de AWS que se incluyen en el código. De forma predeterminada, una vez activado Security Hub, se ofrece una prueba gratuita de 30 días, tras la cual hay un costo asociado a este servicio de AWS. Para obtener más información, consulte Precios de AWS Security Hub.

Versiones de producto

- Helm versión 3.4.2 o posterior
- Apache Maven versión 3.6.3 o posterior
- BridgeCrew Compruebe la versión 2.2 o posterior
- Aqua Security Trivy versión 0.37 o posterior

Arquitectura

Pila de tecnología

- AWS CodeBuild

- AWS CodeCommit
- Amazon CodeGuru
- AWS CodePipeline
- Amazon Elastic Container Registry
- Amazon Elastic Kubernetes Service
- Amazon EventBridge
- AWS Security Hub
- Amazon Simple Notification Service (Amazon SNS)

Arquitectura de destino

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El desarrollador actualiza el código de la aplicación Java en la rama base del CodeCommit repositorio, lo que crea una solicitud de extracción (PR).
2. En cuanto se envía el PR, Amazon CodeGuru Reviewer revisa automáticamente el código, lo analiza en función de las prácticas recomendadas para Java y ofrece recomendaciones al desarrollador.
3. Una vez que el PR se fusiona con la rama base, se crea un EventBridge evento de Amazon.
4. El EventBridge evento inicia la CodePipeline canalización, que comienza.
5. CodePipeline ejecuta la etapa de CodeSecurity escaneo (seguridad continua).
6. CodeBuild inicia el proceso de análisis de seguridad, en el que los archivos Helm de implementación de Dockerfile y Kubernetes se escanean con Checkov, y el código fuente de la aplicación se escanea en función de los cambios incrementales en el código. El escaneo del código fuente de la aplicación lo realiza el contenedor de interfaz de línea de comandos (CLI) de CodeGuru Reviewer.
7. Si la etapa de escaneo de seguridad es exitosa, se inicia la etapa de compilación (integración continua).
8. En la etapa de compilación, CodeBuild crea el artefacto, empaqueta el artefacto en una imagen de Docker, escanea la imagen en busca de vulnerabilidades de seguridad mediante Aqua Security Trivy y almacena la imagen en Amazon ECR.

9. Las vulnerabilidades detectadas en el paso 8 se cargan en Security Hub para que los desarrolladores o ingenieros las analicen más a fondo. Security Hub proporciona una descripción general y recomendaciones para corregir las vulnerabilidades.
10. Las notificaciones por correo electrónico de las distintas fases de la CodePipeline canalización se envían a través de Amazon SNS.
11. Una vez completadas las fases de integración continua, CodePipeline pasa a la etapa de implementación (entrega continua).
12. La imagen de Docker se implementa en Amazon EKS como una carga de trabajo de contenedor (pod) mediante gráficos de Helm.
13. El pod de la aplicación está configurado con Amazon CodeGuru Profiler Agent, que enviará los datos de creación de perfiles de la aplicación (CPU, uso del montón y latencia) a Amazon CodeGuru Profiler, lo que ayuda a los desarrolladores a comprender el comportamiento de la aplicación.

Herramientas

Servicios de AWS

- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- AWS CodeBuild es un servicio de compilación totalmente gestionado que le ayuda a compilar código fuente, ejecutar pruebas unitarias y producir artefactos listos para su implementación.
- AWS CodeCommit es un servicio de control de versiones que le ayuda a almacenar y gestionar repositorios de Git de forma privada, sin necesidad de gestionar su propio sistema de control de código fuente.
- Amazon CodeGuru Profiler recopila datos de rendimiento en tiempo de ejecución de sus aplicaciones activas y proporciona recomendaciones que pueden ayudarle a ajustar el rendimiento de las aplicaciones.
- Amazon CodeGuru Reviewer utiliza el análisis de programas y el aprendizaje automático para detectar posibles defectos que son difíciles de encontrar para los desarrolladores y ofrece sugerencias para mejorar el código de Java y Python.
- AWS le CodePipeline ayuda a modelar y configurar rápidamente las diferentes etapas de una versión de software y a automatizar los pasos necesarios para publicar cambios de software de forma continua.

- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable.
- Amazon Elastic Kubernetes Service (Amazon EKS) le ayuda a ejecutar Kubernetes en AWS sin necesidad de instalar ni mantener su propio plano de control o nodos de Kubernetes.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, las funciones de Lambda de AWS, los puntos de conexión de invocación HTTP que utilizan destinos de API o los buses de eventos de otras cuentas de AWS.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Security Hub proporciona una visión completa de su estado de seguridad en AWS. También le permite comprobar si su entorno de AWS cumple con los estándares y las prácticas recomendadas del sector de seguridad.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Otros servicios

- Helm es un administrador de paquetes de código abierto para Kubernetes.
- Apache Maven es una herramienta de software para la comprensión y administración de proyectos.
- BridgeCrew Checkov es una herramienta de análisis de código estático para escanear la infraestructura como archivos de código (IaC) en busca de errores de configuración que puedan provocar problemas de seguridad o de conformidad.
- Aqua Security Trivy es un escáner completo para detectar vulnerabilidades en imágenes de contenedores, sistemas de archivos y repositorios de Git, además de problemas de configuración.

Código

El código de este patrón está disponible en el repositorio. GitHub aws-codepipeline-devsecops-amazoneks

Prácticas recomendadas

- Se ha seguido el principio del privilegio mínimo para las entidades de IAM en todas las fases de esta solución. Si desea ampliar la solución con servicios de AWS adicionales o herramientas de terceros, le recomendamos que siga el principio de privilegios mínimos.
- Si tiene varias aplicaciones Java, le recomendamos que cree canalizaciones de CI/CD independientes para cada aplicación.
- Si tiene una aplicación monolítica, le recomendamos dividirla en microservicios en la medida de lo posible. Los microservicios son más flexibles, facilitan la implementación de aplicaciones como contenedores y proporcionan una mejor visibilidad de la creación y la implementación generales de la aplicación.

Epics

Configuración del entorno

Tarea	Descripción	Habilidades requeridas
Clona el GitHub repositorio.	Para clonar el repositorio, ejecute el siguiente comando. `git clone https://github.com/aws-samples/aws-codepipeline-devsecops-amazoneks`	Desarrollador de aplicaciones, DevOps ingeniero
Cree un bucket de S3 y suba el código.	1. Inicie sesión en la consola de administración de AWS, abra la consola de Amazon S3 y, a continuación, cree un bucket de S3 en la región de AWS en la que planea implementar esta solución. Para obtener más información, consulte Creación de un bucket en la	AWS DevOps, DevOps ingeniero, administrador de la nube, DevOps

Tarea	Descripción	Habilidades requeridas
	documentación de Amazon S3. 2. En el bucket de S3, cree una carpeta llamada `code`. 3. Navegue hasta el lugar donde clonó el repositor io. Para crear una versión comprimida de todo el código con la extensión .zip (`cicdstack.zip`) y validar el archivo .zip, ejecute los siguientes comandos en orden. Nota: Si el comando `python` falla e indica que no se encontró Python, utilice `python3` en su lugar. `cd aws-codepipeline-devsecops-amazoneks` `python -m zipfile -c cicdstack.zip *` `python -m zipfile -t cicdstack.zip` 4. Cargue el archivo `cicdstack.zip` a la carpeta de código que creó previamente en el bucket de S3.	

Tarea	Descripción	Habilidades requeridas
Cree una CloudFormation pila de AWS.	1. Abre la CloudFormation consola de AWS y selecciona Create stack. 2. En el panel Specify Template (Especificar plantilla), elija Upload a template file (Cargar un archivo de plantilla), elija el archivo `cf_templates/codecommit_ecr.yaml` y, a continuación, elija Next (Siguiente). 3. En Especificar los detalles de la pila, introduzca el nombre de la pila y, a continuación, aporte los siguientes valores de los parámetros de entrada: • CodeCommitRepositoryBranchName: el nombre de la sucursal en la que residirá su código (el predeterminado es main) • CodeCommitRepositoryName: el nombre del CodeCommit repositorio que se va a crear. • CodeCommitRepositoryS3Bucket: el nombre del bucket de S3 en el que creaste la carpeta de códigos	AWS DevOps, DevOps

Tarea	Descripción	Habilidades requeridas
	• CodeCommitRepositoryS3: BucketObjKey `code/cicdstack.zip` • ECR RepositoryName: el nombre del repositorio de Amazon ECR que se va a crear 4. Elija Siguiente, utilice la configuración predeterminada para las Opciones de configuración de pila y, a continuación, elija Siguiente. 5. En la sección Review (Revisar), verifique los detalles de la plantilla y la pila y, a continuación, seleccione Create stack (Crear pila). A continuación, se crea la pila, que incluye los repositorios CodeCommit y Amazon ECR. 6. Anote los nombres de los repositorios CodeCommit y de Amazon ECR, que serán necesarios para la configuración de la canalización de CI/CD de Java.	

Tarea	Descripción	Habilidades requeridas
Valide la implementación de la CloudFormation pila.	1. En Stacks en la CloudFormation consola, verifica el estado de la CloudFormation pila que has implementado. El estado de la pila debe ser CREATE COMPLETE. 2. Además, desde la consola, compruebe que Amazon ECR CodeCommit y Amazon ECR se hayan aprovisionado y estén listos.	DevOps ingeniero
Elimine el bucket de S3.	Vacíe y borre el bucket de S3 que creó con anterioridad. Para obtener más información, consulte Eliminación de un bucket en la documentación de Amazon S3.	AWS DevOps, DevOps

Configure los gráficos de Helm

Tarea	Descripción	Habilidades requeridas
Configure los gráficos de Helm de su aplicación Java.	1. En la ubicación en la que clonó el GitHub repositorio, vaya a la carpeta`helm_charts/aws-proserve-java-greeting` . En esta carpeta, el archivo `values.dev.yaml` contiene información sobre	DevOps

Tarea	Descripción	Habilidades requeridas
	la configuración de los recursos de Kubernetes que puede modificar para las implementaciones de contenedores en Amazon EKS. Actualice el parámetro del repositorio de Docker proporcionando el ID de su cuenta de AWS, la región de AWS y el nombre del repositorio de Amazon ECR. `image:` `  repository:` `  <account-id>.dkr.ecr.<region>.amazonaws.com/<app-ecr-repo-name>` 2. El tipo de servicio del pod de Java está establecido en `LoadBalancer` . `service:` `  type: LoadBalancer` `  port: 80` `  targetPort: 8080` `  path: /hello` `  initialDelaySeconds: 60` `  periodSeconds: 30` Para usar un servicio diferente (por ejemplo, `NodePort`), puede cambiar los parámetros. Para	

Tarea	Descripción	Habilidades requeridas
	obtener más información, consulte Documentación Kubernetes en la documentación de Kubernetes. 3. Puede activar el Escalador automático de Kubernetes Horizontal Pod cambiando el parámetro `autoscaling` a `enabled: true`. `autoscaling:` `  enabled: true` `  minReplicas: 1` `  maxReplicas: 100` `  targetCPUUtilizationPercentage: 80` `  # targetMemoryUtilizationPercentage: 80` Puede habilitar diferentes funciones para las cargas de trabajo de Kubernetes cambiando los valores del `values.<ENV>.yaml` archivo, donde `<ENV>` se encuentra su entorno de desarrollo, producción, UAT o control de calidad.	

Tarea	Descripción	Habilidades requeridas
Valide los gráficos de Helm para detectar errores de sintaxis.	1. Desde la terminal, compruebe que Helm v3 esté instalado en su estación de trabajo local ejecutando el siguiente comando. `helm --version` Si Helm v3 no está instalado, instálelo. 2. En la terminal, navegue hasta el directorio de gráficos de Helm (`helm_charts/aws-proserve-java-greeting`) y ejecute el siguiente comando. `helm lint . -f values.dev.yaml` Esto comprobará si hay errores de sintaxis en los gráficos de Helm.	DevOps ingeniero

Configuración de la canalización de CI/CD de Java

Tarea	Descripción	Habilidades requeridas
Crear la canalización de CI/CD.	1. Abra la CloudFormation consola de AWS y elija Create stack.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	2. En el panel Specify Template (Especificar plantilla), elija Upload a template file (Cargar un archivo de plantilla), elija el archivo `cf_templates/build_deployment.yaml` y, a continuación, elija Next (Siguiente). 3. En Specify stack details (Especificar los detalles de la pila), introduzca el Stack name (Nombre de la pila) y, a continuación, aporte los siguientes valores de los parámetros de entrada: • CodeBranchName: Nombre de la rama del CodeCommit repositorio, donde reside su código • EKSClusterName: Nombre de su clúster de EKS (no el `EKSCluster` ID) • EKS CodeBuild AppName: Nombre de la aplicación Helm chart (`aws-proserve-java-greeting`) • WorkerNodeRoleARN de EKS: ARN de la función de IAM de los nodos de trabajo de Amazon EKS	

Tarea	Descripción	Habilidades requeridas
	• EKS WorkerNod eRoleName: Nombre de la función de IAM asignada a los nodos de trabajo de Amazon EKS • EcrDockerRepository: Nombre del repositorio de Amazon ECR donde se almacenarán las imágenes de Docker de su código • EmailRecipient: dirección de correo electrónico a la que se deben enviar las notificaciones de compilación • EnvType: Entorno (por ejemplo, dev, test o prod) • SourceRepoName: Nombre del CodeCommit repositorio, donde reside tu código 4. Seleccione Siguiente. Utilice la configuración predeterminada para las Configure stack options (Opciones de configuración de pila) y, a continuación, elija Next (Siguiente). 5. En la sección Revisar, compruebe los detalles de la CloudFormation plantilla y la pila de AWS y,	

Tarea	Descripción	Habilidades requeridas
	a continuación, seleccione Siguiente. 6. Seleccione Crear pila. 7. Durante la implement ación de la CloudForm ation pila, el propietario de la dirección de correo electrónico que proporcionó en los parámetros recibirá un mensaje para suscribir se a un tema de SNS. Para suscribirse a Amazon SNS, el propietario debe elegir el enlace del mensaje. 8. Una vez creada la pila, abra la pestaña Salidas de la pila y, a continuación, registre el valor ARN de la clave de salida `EksCodeBu ildkubeRoleARN` . Este valor de ARN de IAM se necesitará más adelante para proporcio nar al CodeBuild rol de IAM permisos para implement ar cargas de trabajo en el clúster de Amazon EKS.	

Active la integración entre Security Hub y Aqua Security

Tarea	Descripción	Habilidades requeridas
Active la integración de Aqua Security.	Este paso es necesario para cargar los hallazgos de	Administrador DevOps e ingeniero de AWS

Tarea	Descripción	Habilidades requeridas
	vulnerabilidad de imágenes de Docker reportados por Trivy a Security Hub. Como AWS CloudFormation no admite las integraciones de Security Hub, este proceso debe realizarse manualmente. 1. Abra la consola de AWS Security Hub y vaya a Integraciones. 2. Busque Aqua Security y seleccione Aqua Security: Aqua Security. 3. Seleccione Aceptar los resultados.	

Configure CodeBuild para ejecutar los comandos Helm o kubectl

Tarea	Descripción	Habilidades requeridas
Permite CodeBuild ejecutar comandos Helm o kubectl en el clúster de Amazon EKS.	CodeBuild Para autenticarse y utilizar Helm o *`kubectl`* comandos con el clúster EKS, debe añadir las funciones de IAM al. *`aws-auth ConfigMap`* En este caso, añada el ARN del rol de IAM`EksCodeBuildkubeRoleARN` , que es el rol de IAM creado para que el CodeBuild servicio acceda al clúster de EKS e implemente cargas de trabajo en él. Esta es una	DevOps

Tarea	Descripción	Habilidades requeridas
	actividad que se realiza una vez. Importante: El siguiente procedimiento debe completarse antes de la fase de aprobación de la implementación. CodePipeline 1. Abra el script de intérprete de comandos `cf_templates/kube_aws_auth_configmap_patch.sh` en su entorno Amazon Linux o macOS. 2. Autentifíquese en el clúster de Amazon EKS ejecutando el siguiente comando. `aws eks --region <aws-region> update-kubeconfig --name <eks-cluster-name>` 3. Ejecute el script de intérprete de comandos mediante el siguiente comando, sustituyendo `<rolearn-eks-codebuild-kubectl>` por el valor ARN `EksCodeBuildkubeRoleARN` que registró anteriormente. `bash cf_templates/kube_aws_auth_configmap_patch.sh`	

Tarea	Descripción	Habilidades requeridas
	<rolearn-eks-codebuild-kubectl> aws_auth ConfigMap se configura y se concede el acceso.	

Valide la canalización de CI/CD

Tarea	Descripción	Habilidades requeridas
Compruebe que la canalización de CI/CD se inicie automáticamente.	1. La fase de CodeSecurity análisis del proceso suele fallar si Checkov detecta vulnerabilidades en los gráficos de Dockerfile o Helm. Sin embargo, el objetivo de este ejemplo es establecer un proceso de identificación de posibles vulnerabilidades de seguridad en lugar de corregirlas mediante el proceso de CI/CD, que suele ser un proceso. DevSecOps En el archivo buildspec/buildspec_secscan.yaml , el comando checkov usa la marca --soft-fail para evitar que la canalización falle.	DevOps

Tarea	Descripción	Habilidades requeridas
	<pre>- echo -e "\n Running Dockerfile Scan" - checkov -f code/app/Dockerfile --framework dockerfile --soft-fail --summary-position bottom - echo -e "\n Running Scan of Helm Chart files" - cp -pv helm_charts/$EKS_CODEBUILD_APP_NAME/values.dev.yaml helm_charts/$EKS_CODEBUILD_APP_NAME/values.yaml - checkov -d helm_charts/$EKS_CODEBUILD_APP_NAME --framework helm --soft-fail --summary-position bottom - rm -rfv helm_charts/$EKS_CODEBUILD_APP_NAME/values.yaml</pre> Para que la canalización falle cuando se detecten vulnerabilidades en los gráficos de Dockerfile y Helm, se debe eliminar la opción `--soft-fail` del comando `checkov`. Luego, los desarrolladores	

Tarea	Descripción	Habilidades requeridas
	o ingenieros pueden corregir las vulnerabilidades y registrar los cambios en el repositorio de código CodeCommit fuente. 2. Al igual que en CodeSecurity Scan, la fase de creación utiliza Aqua Security Trivy para identificar las vulnerabilidades de imagen de Docker ALTAS y CRÍTICAS antes de enviar la aplicación a Amazon ECR. En este ejemplo, no estamos haciendo que la canalización de vulnerabilidades en las imágenes de Docker fracase. En el archivo `buildspec/buildspec.yml`, el comando `trivy` incluye una marca `--exit-code` con un valor `0`, por lo que la canalización no falla cuando se informa de vulnerabilidades de imagen de Docker con niveles ALTOS o CRÍTICOS. `- AWS_REGION=$AWS_DEFAULT_REGION AWS_ACCOUNT_ID=$AWS_ACCOUNT_ID trivy -d image --no-progress --ignore-unfixed --exit-code 0 --severit`	

Tarea	Descripción	Habilidades requeridas
	<pre>y HIGH,CRITICAL -- format template -- template "@securit yhub/asff.tpl" -o securityhub/report .asff $AWS_ACCO UNT_ID.dkr.ecr.$AW S_DEFAULT_REGION.a mazonaws.com/$IMAG E_REPO_NAME:$CODEB UILD_RESOLVED_SOUR CE_VERSION</pre> Para que la canalización falle cuando se detecten vulnerabilidades `HIGH,CRTICAL`, cambie el valor de `--exit-code` a `1`. Luego, los desarrolladores o ingenieros pueden corregir las vulnerabilidades y registrar los cambios en el repositorio de código fuente. CodeCommit 3. Las vulnerabilidades de imagen de Docker reportadas por Aqua Security Trivy se cargan en Security Hub. En la consola de AWS Security Hub, vaya a Resultados. Filtre los resultados con Registrar Estado= Activo y Producto = Aqua Security. Esto mostrará una lista de las vulnerabilidades	

Tarea	Descripción	Habilidades requeridas
	de imagen de Docker en Security Hub. Las vulnerabilidades pueden tardar entre 15 minutos y 1 hora en aparecer en Security Hub. Para obtener más información sobre cómo iniciar la canalización mediante el uso CodePipeline, consulte Iniciar una canalización en CodePipeline, Iniciar una canalización manualmente e Iniciar una canalización según un cronograma en la CodePipeline documentación de AWS.	

Tarea	Descripción	Habilidades requeridas
Apruebe la implementación.	1. Una vez finalizada la fase de construcción, hay una puerta de aprobación de la implementación. El revisor o el administrador de versiones deben inspeccionar la compilación y, si se cumplen todos los requisitos, aprobarla. Este es el enfoque recomendado para los equipos que utilizan la entrega continua para la implementación de aplicaciones. 2. Tras la aprobación, la canalización inicia la fase de implementación. 3. Una vez finalizada la fase de implementación, el CodeBuild registro de esta etapa proporciona la URL de la aplicación. Utilice la URL para validar que la aplicación esté lista.	DevOps

Tarea	Descripción	Habilidades requeridas
Valide la creación de perfiles de la aplicación.	Una vez finalizada la implementación y desplegado el pod de la aplicación en Amazon EKS, el agente Amazon CodeGuru Profiler configurado en la aplicación intentará enviar los datos de creación de perfiles de la aplicación (CPU, resumen del montón, latencia y cuellos de botella) a Amazon Profiler. CodeGuru Para la implementación inicial de una aplicación, Amazon CodeGuru Profiler tarda unos 15 minutos en visualizar los datos de creación de perfiles.	AWS DevOps

Recursos relacionados

- CodePipeline Documentación de AWS
- Escaneo de imágenes con Trivy en AWS CodePipeline (entrada del blog)
- Mejora de sus aplicaciones Java con Amazon CodeGuru Profiler (entrada del blog)
- Sintaxis de AWS Security Finding Format (ASFF)
- Patrones de EventBridge eventos de Amazon
- Actualización de Helm

Información adicional

CodeGuru No se debe confundir Profiler con el servicio AWS X-Ray en términos de funcionalidad. CodeGuru Se prefiere Profiler para identificar las líneas de códigos más caras, que pueden provocar

cuellos de botella o problemas de seguridad, y corregirlas antes de que se conviertan en un riesgo potencial. El servicio AWS X-Ray sirve para monitorear el rendimiento de las aplicaciones.

En este patrón, las reglas de eventos se asocian al bus de eventos predeterminado. Si es necesario, puede ampliar el patrón para utilizar un bus de eventos personalizado.

Este patrón utiliza CodeGuru Reviewer como una herramienta estática de pruebas de seguridad de aplicaciones (SAST) para el código de la aplicación. También puedes usar esta canalización para otras herramientas, como SonarQube Checkmarx. Se pueden añadir las instrucciones de configuración de digitalización correspondientes a cualquiera de estas herramientas`buildspec/buildspec_secscan.yaml`, sustituyendo las instrucciones de digitalización de CodeGuru.

Crear una definición de tareas de Amazon ECS y montar un sistema de archivos en instancias EC2 mediante Amazon EFS

Creado por Durga Prasad Cheepuri (AWS)

Entorno: PoC o piloto	Tecnologías: contenedores y microservicios; nativas de la nube; administración y gobierno; almacenamiento y respaldo; aplicaciones web y móviles	Servicios de AWS: Amazon ECS; Amazon EFS

Resumen

Este patrón proporciona códigos de muestra y pasos para crear una definición de tarea de Amazon Elastic Container Service (Amazon ECS) que se ejecute en instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la nube de Amazon Web Services (AWS), mientras se utiliza Amazon Elastic File System (Amazon EFS) para montar un sistema de archivos en esas instancias EC2. Las tareas de Amazon ECS que utilizan Amazon EFS montan automáticamente los sistemas de archivos que especifique en la definición de la tarea y ponen estos sistemas de archivos a disposición de los contenedores de la tarea en todas las zonas de disponibilidad de una región de AWS.

Para cumplir sus requisitos de almacenamiento persistente y almacenamiento compartido, puede utilizar Amazon ECS y Amazon EFS juntos. Por ejemplo, puede usar Amazon EFS para almacenar datos persistentes de usuarios y datos de aplicaciones para sus aplicaciones con pares de contenedores ECS activos y en espera que se ejecuten en diferentes zonas de disponibilidad para lograr una alta disponibilidad. También puede usar Amazon EFS para almacenar datos compartidos a los que se puede acceder en paralelo mediante contenedores de ECS y cargas de trabajo distribuidas.

Para utilizar Amazon EFS con Amazon ECS, puede añadir una o más definiciones de volumen a una definición de tarea. Una definición de volumen incluye un ID de sistema de archivos de Amazon EFS, un ID de punto de acceso y una configuración para la autorización de AWS Identity and Access Management (IAM) o el cifrado en tránsito de la seguridad de la capa de transporte (TLS). Puede usar definiciones de contenedores dentro de las definiciones de tareas para especificar los

volúmenes de definición de tareas que se montan cuando se ejecuta el contenedor. Cuando se ejecuta una tarea que utiliza un sistema de archivos Amazon EFS, Amazon ECS se asegura de que el sistema de archivos esté montado y disponible para los contenedores que necesitan acceder a él.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una nube privada virtual (VPC) con un punto de conexión de red privada virtual (VPN) (VPN) o un router
- (Recomendado) El Agente contenedor Amazon ECS 1.38.0 o posterior para garantizar la compatibilidad con los puntos de acceso de Amazon EFS y las características de autorización de IAM (para obtener más información, consulte la entrada del blog de AWS Nuevo para Amazon EFS – Autorización y puntos de acceso de IAM).

Limitaciones

- Las versiones del agente de contenedor de Amazon ECS anteriores a la 1.35.0 no admiten los sistemas de archivos de Amazon EFS para tareas que utilizan el tipo de lanzamiento de EC2.

Arquitectura

El siguiente diagrama muestra un ejemplo de una aplicación que utiliza Amazon ECS para crear una definición de tarea y montar un sistema de archivos Amazon EFS en instancias EC2 en contenedores de ECS.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Crear un sistema de archivos de Amazon EFS.
2. Cree una definición de tarea con un contenedor.
3. Configure las instancias de contenedor para montar el sistema de archivos de Amazon EFS. La definición de la tarea hace referencia a los montajes de volumen, para que la instancia de contenedor pueda utilizar el sistema de archivos Amazon EFS. Las tareas de ECS tienen acceso al mismo sistema de archivos de Amazon EFS, independientemente de la instancia de contenedor en la que se creen esas tareas.

4. Cree un servicio de Amazon ECS con tres instancias de la definición de tarea.

Pila de tecnología

- Amazon EC2
- Amazon ECS
- Amazon EFS

Herramientas

- Amazon EC2: Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de AWS. Puede utilizar Amazon EC2 para lanzar tantos servidores virtuales como necesite, y puede escalar horizontalmente o reducir horizontalmente.
- Amazon ECS: Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores altamente escalable y rápido para ejecutar, detener y administrar contenedores en un clúster. Las tareas y los servicios se pueden ejecutar en una infraestructura sin servidor administrada por AWS Fargate. Si desea más control sobre su infraestructura, puede ejecutar las tareas y los servicios en un clúster de instancias de EC2 que usted administre.
- Amazon EFS: Amazon Elastic File System (Amazon EFS) ofrece un sistema de archivos NFS sencillo, escalable, elástico y completamente administrado que se utiliza con servicios de nube de AWS y recursos en las instalaciones.
- AWS CLI: la interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto para interactuar con los servicios de AWS mediante comandos en el intérprete de comandos de línea de comandos. Con una configuración mínima, puede ejecutar comandos de la CLI de AWS que implementan una funcionalidad equivalente a la proporcionada por la consola de administración de AWS basada en navegador desde un símbolo del sistema.

Epics

Crear un sistema de archivos de Amazon EFS

Tarea	Descripción	Habilidades requeridas
Crear un sistema de archivos de Amazon EFS mediante la	1. Cree un sistema de archivos Amazon EFS y	AWS DevOps

Tarea	Descripción	Habilidades requeridas
consola de administración de AWS.	seleccione la VPC que incluye sus contenedores. Nota: Si utiliza una VPC diferente, configure una conexión de emparejamiento de VPC. 2. Anote el ID del sistema de archivos.	

Cree una definición de tarea de Amazon ECS mediante un sistema de archivos de Amazon EFS o la CLI de AWS.

Tarea	Descripción	Habilidades requeridas
Cree una definición de tarea mediante un sistema de archivos de Amazon EFS.	Cree una definición de tarea mediante la nueva consola Amazon ECS o la consola Amazon ECS clásica con las siguientes configuraciones: • Si usa la nueva consola, seleccione las instancias Amazon EC2 para el Entorno de la aplicación. Si usa la consola clásica, seleccione EC2 como tipo de lanzamiento. • Añada un volumen. Introduzca un nombre para el volumen, seleccione EFS como tipo de volumen y, a continuación, seleccione el ID del sistema de archivos que	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	indicó anteriormente. Para el directorio raíz, seleccione la ruta del sistema de archivos Amazon EFS que desee alojar en el host de contenedores de Amazon ECS.	

Tarea	Descripción	Habilidades requeridas
Cree una definición de tarea utilizando la CLI de AWS.	1. Para crear una plantilla de JSON con marcadores de posición de parámetros de entrada para la definición de tareas, ejecute el siguiente comando: `aws ecs register-task-definition --generate-cli-skeleton` 2. Para crear la definición de tareas con la plantilla de JSON, ejecute el siguiente comando: `aws ecs register-task-definition --cli-input-json file://<path_to_your_json_file>` 3. Introduzca los parámetros de entrada en su plantilla JSON en función del archivo `task_definition_parameters.json` (adjunto). Nota: Para obtener más información sobre los parámetros de entrada, consulte Parámetros de definición de tareas (documentación de Amazon ECS) y register-task-definition(Referencia	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	de comandos de la CLI de AWS).	

Recursos relacionados

- Definiciones de tareas de Amazon ECS
- Volúmenes de Amazon EFS

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Implementar microservicios de Java en Amazon ECS con AWS Fargate

Creado por Vijay Thompson (AWS) y Sandeep Bondugula (AWS)

Entorno: PoC o piloto	Origen: Contenedores	Destino: Amazon ECS
Tipo R: N/D	Tecnologías: contenedores y microservicios; aplicaciones web y móviles	Servicios de AWS: Amazon ECS

Resumen

Este patrón proporciona orientación para implementar microservicios de Java en contenedores en Amazon Elastic Container Service (Amazon ECS) mediante AWS Fargate. El patrón no utiliza Amazon Elastic Container Registry (Amazon ECR) para la administración de contenedores; en su lugar, las imágenes de Docker se extraen de un hub de Docker.

Requisitos previos y limitaciones

Requisitos previos

- Una aplicación de microservicios de Java existente en un hub de Docker
- Un repositorio público de Docker
- Una cuenta de AWS activa
- Conocimientos de los servicios de AWS, incluyendo Amazon ECS y Fargate
- Marco Docker, Java y Spring Boot
- Amazon Relational Database Service (Amazon RDS) en funcionamiento (opcional)
- Una nube privada virtual (VPC) si la aplicación requiere Amazon RDS (opcional)

Arquitectura

Pila de tecnología de origen

- Microservicios de Java (por ejemplo, implementados en Spring Boot) e implementados en Docker

Arquitectura de origen

Pila de tecnología de destino

- Un clúster de Amazon ECS que aloja cada microservicio mediante Fargate
- Una red de VPC para alojar el clúster de Amazon ECS y los grupos de seguridad asociados
- Una definición de clúster/tarea para cada microservicio que pone en marcha los contenedores mediante Fargate

Arquitectura de destino

Herramientas

Herramientas

- Amazon ECS elimina la necesidad de instalar y operar su propio software de orquestación de contenedores, administrar y escalar un clúster de máquinas virtuales o programar contenedores en esas máquinas virtuales.
- AWS Fargate le permite ejecutar contenedores sin necesidad de administrar servidores o instancias de Amazon Elastic Compute Cloud (Amazon EC2). Se utiliza en conjunto con Amazon Elastic Container Service (Amazon ECS).
- Docker es una plataforma de software que le permite compilar, probar e implementar aplicaciones de forma rápida. Docker agrupa el software en unidades estandarizadas denominadas contenedores que contienen todo lo que el software necesita para ejecutarse, incluyendo las bibliotecas, las herramientas del sistema, el código y el tiempo de ejecución.

Código de Docker

El siguiente Dockerfile especifica la versión del kit de desarrollo de Java (JDK) que se utiliza, dónde se encuentra el archivo de almacenamiento Java (JAR), el número de puerto que está expuesto y el punto de entrada a la aplicación.

```
FROM openjdk:11
ADD target/Spring-docker.jar Spring-docker.jar
EXPOSE 8080
ENTRYPOINT ["java","-jar","Spring-docker.jar"]
```

Epics

Crear nuevas definiciones de tareas

Tarea	Descripción	Habilidades requeridas
Cree una definición de tarea.	Para ejecutar contenedores de Docker en Amazon ECS, se requiere una definición de tareas. Abra la consola de Amazon ECS en https://console.aws.amazon.com/ecs/, seleccione Definiciones de tareas y, a continuación, cree una nueva definición de tarea. Para obtener más información, consulte la documentación de Amazon ECS.	Administrador de sistemas de AWS, desarrollador de aplicaciones
Seleccione el tipo de lanzamiento.	Seleccione Fargate como tipo de lanzamiento.	Administrador de sistemas de AWS, desarrollador de aplicaciones
Configure la tarea.	Defina un nombre de tarea y configure la aplicación con la cantidad adecuada de memoria de tareas y CPU.	Administrador de sistemas de AWS, desarrollador de aplicaciones
Defina el contenedor.	Especifique el nombre del contenedor. Para la imagen, introduzca el nombre del sitio de Docker, el nombre del repositorio y el nombre	Administrador de sistemas de AWS, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	de la etiqueta de la imagen de Docker (`docker.io/sample-repo/sample-application:sample-tag-name`). Establezca los límites de memoria para la aplicación y establezca las asignaciones de puertos (`8080, 80`) para los puertos permitidos.	
Cree la tarea.	Cuando las configuraciones de la tarea y el contenedor se hayan establecido, cree la tarea. Para obtener instrucciones detalladas, consulte los enlaces de la sección Recursos relacionados.	Administrador de sistemas de AWS, desarrollador de aplicaciones

Configure el clúster

Tarea	Descripción	Habilidades requeridas
Crear y configurar un clúster.	Seleccione Solo redes como tipo de clúster, configure el nombre y, a continuación, cree el clúster o utilice un clúster existente si está disponible. Para obtener más información, consulte la documentación de Amazon ECS.	Administrador de sistemas de AWS, desarrollador de aplicaciones

Configurar la tarea

Tarea	Descripción	Habilidades requeridas
Cree una tarea.	Dentro del clúster, seleccione Ejecutar nueva tarea.	Administrador de sistemas de AWS, desarrollador de aplicaciones
Seleccione el tipo de lanzamiento.	Seleccione Fargate como tipo de lanzamiento.	Administrador de sistemas de AWS, desarrollador de aplicaciones
Seleccione la definición de la tarea, la revisión y la versión de la plataforma.	Seleccione la tarea que desee ejecutar, la revisión de la definición de la tarea y la versión de la plataforma.	Administrador de sistemas de AWS, desarrollador de aplicaciones
Seleccione el clúster.	Seleccione el clúster desde el que desea ejecutar la tarea.	Administrador de sistemas de AWS, desarrollador de aplicaciones
Especifique el número de tareas.	Configure el número de tareas que deben ejecutarse. Si lo inicia con dos o más tareas, necesitará un equilibrador de carga para distribuir el tráfico entre las tareas.	Administrador de sistemas de AWS, desarrollador de aplicaciones
Especifique el grupo de tareas.	(Opcional) Especifique un nombre de grupo de tareas para identificar un conjunto de tareas relacionadas como grupo de tareas.	Administrador de sistemas de AWS, desarrollador de aplicaciones
Configure la VPC del clúster, las subredes y los grupos de seguridad.	Configure la VPC del clúster y las subredes en las que desea implementar la aplicación. Cree o actualice grupos de	Administrador de sistemas de AWS, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	seguridad (HTTP, HTTPS y puerto 8080) para proporcio nar acceso a las conexiones entrantes y salientes.	
Configure los ajustes de la IP pública.	Active o desactive la IP pública, en función de si desea utilizar una dirección IP pública para las tareas de Fargate. La opción predeterm inada recomendada es Habilitada.	Administrador de sistemas de AWS, desarrollador de aplicaciones
Revisar la configuración y crear la tarea	Revise la configuración y, a continuación seleccione Ejecutar tarea.	Administrador de sistemas de AWS, desarrollador de aplicaciones

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Copie la URL de la aplicación.	Cuando el estado de la tarea se haya actualizado a En ejecución, seleccione la tarea. En la sección Redes, copie la IP pública.	Administrador de sistemas de AWS, desarrollador de aplicaciones
Pruebe su aplicación.	En su navegador, introduzc a la IP pública para probar la aplicación.	Administrador de sistemas de AWS, desarrollador de aplicaciones

Recursos relacionados

- Conceptos básicos de Docker para Amazon ECS (documentación de Amazon ECS)

- Amazon ECS en AWS Fargate (documentación de Amazon ECS)
- Creación de una definición de tarea (documentación de Amazon ECS)
- Creación de un clúster (documentación de Amazon ECS)
- Configuración de los parámetros básicos del servicio (documentación de Amazon ECS)
- Configuración de una red (documentación de Amazon ECS)
- Implementación de microservicios de Java en Amazon ECS (entrada del blog)

Implemente microservicios Java en Amazon ECS mediante Amazon ECR y AWS Fargate

Creado por Vijay Thompson (AWS) y Sandeep Bondugula (AWS)

Entorno: PoC o piloto	Origen: Contenedores	Destino: Amazon ECS
Tipo R: N/D	Tecnologías: contenedores y microservicios; aplicaciones web y móviles	Servicios de AWS: Amazon ECS

Resumen

Este patrón guía por los pasos para implementar microservicios de Java como aplicaciones en contenedores en Amazon Elastic Container Service (Amazon ECS). El patrón también utiliza Amazon Elastic Container Registry (Amazon ECR) para administrar el contenedor y AWS Fargate para ejecutarlo.

Requisitos previos y limitaciones

Requisitos previos

- Una aplicación de microservicios Java existente que se ejecuta en las instalaciones de Docker
- Una cuenta de AWS activa
- Familiaridad con Amazon ECR, Amazon ECS, AWS Fargate e Interfaz de la línea de comandos de AWS (AWS CLI)
- Familiaridad con el software Java y Docker

Versiones de producto

- Versión 1.7 o posterior de la CLI de AWS

Arquitectura

Pila de tecnología de origen

- Microservicios Java (por ejemplo, desarrollados con Spring Boot) e implementados en las instalaciones
- Docker

Arquitectura de origen

Pila de tecnología de destino

- Amazon ECR
- Amazon ECS
- AWS Fargate

Arquitectura de destino

Herramientas

Herramientas

- Amazon Elastic Container Registry (Amazon ECR) es un registro de contenedores de Docker completamente administrado que facilita el almacenamiento, la administración y la implementación de imágenes de contenedores de Docker. Amazon ECR está integrado con Amazon ECS para simplificar su development-to-production flujo de trabajo. Amazon ECR aloja las imágenes en una arquitectura escalable y de alta disponibilidad, lo que le permite implementar contenedores para sus aplicaciones con fiabilidad. La integración con AWS Identity and Access Management (IAM) proporciona un control a nivel de recursos de cada repositorio.
- Amazon Elastic Container Service (Amazon ECS) es un servicio de organización de contenedores altamente escalable y de alto rendimiento que admite contenedores de Docker y le permite ejecutar y escalar fácilmente aplicaciones en contenedores en AWS. Amazon ECS elimina la necesidad de instalar y operar su propio software de orquestación de contenedores, administrar y escalar un clúster de máquinas virtuales o programar contenedores en esas máquinas virtuales.
- AWS Fargate es un motor de cómputo para Amazon ECS que le permite ejecutar contenedores sin tener que administrar servidores o clústeres. Con AWS Fargate ya no tendrá que aprovisionar, configurar ni escalar clústeres de máquinas virtuales para ejecutar los contenedores. De esta

manera, se elimina la necesidad de elegir tipos de servidores, decidir cuándo escalar los clústeres u optimizar conjuntos de clústeres.

- Docker es una plataforma que le permite crear, probar y entregar aplicaciones en paquetes denominados contenedores.

Código

DockerFile A continuación, se especifica la versión del kit de desarrollo de Java (JDK) que se utiliza, dónde se encuentra el archivo de almacenamiento Java (JAR), el número de puerto que está expuesto y el punto de entrada de la aplicación.

```
FROM openjdk:8
 ADD target/Spring-docker.jar Spring-docker.jar
 EXPOSE 8080
ENTRYPOINT ["java","-jar","Spring-docker.jar"]
```

Epics

Cree un repositorio de Amazon ECR

Tarea	Descripción	Habilidades requeridas
Creación de un repositorio.	Inicie sesión en la consola de administración de AWS y abra la consola de Amazon ECR en https://console.aws.amazon.com/ecr/repositories. Creación de un repositorio privado. Para obtener instrucciones, consulte Creación de un repositorio privado en la documentación de Amazon ECR.	Desarrollador, administrador del sistema
Suba el proyecto.	Abra el repositorio y seleccione Ver comandos push. Siga los pasos que se muestran	Desarrollador, administrador del sistema

Tarea	Descripción	Habilidades requeridas
	para cargar el proyecto. (Estos pasos solo funcionan cuando utiliza la versión 1.7 o posterior de la CLI de AWS). Cuando se complete la carga, copie la URL de la compilación en el repositorio. Utilizará esta URL cuando cree un contenedor en Amazon ECS.	

Cree y gire el contenedor

Tarea	Descripción	Habilidades requeridas
Cree una definición de tarea.	Para ejecutar contenedores de Docker en Amazon ECS, se requiere una definición de tareas. Abra la consola de Amazon ECS en https://console.aws.amazon.com/ecs/, elija las Definiciones de tareas y cree una nueva definición de tareas. Para obtener más información, consulte Crear una definición de tareas en la documentación de Amazon ECS.	Desarrollador, administrador del sistema
Elija el tipo de lanzamiento.	Elija Fargate como tipo de lanzamiento.	Desarrollador, administrador del sistema
Configure la tarea.	Defina un nombre de tarea y configure la aplicación con la cantidad adecuada de memoria de tareas y CPU.	Desarrollador, administrador del sistema

Tarea	Descripción	Habilidades requeridas
Defina el contenedor.	Añada el contenedor e indique un nombre, la URL del repositorio de Amazon ECR, los límites de memoria y la asignación de puertos. Los puertos 8080 y 80 están configurados para la asignación de puertos. Configure los ajustes restantes en función de los requisitos de su aplicación.	Desarrollador, administrador del sistema
Cree la tarea.	Cuando las configuraciones de la tarea y el contenedor se hayan establecido, cree la tarea. Para obtener instrucciones, consulte el enlace de la sección Recursos relacionados.	Desarrollador, administrador del sistema

Cree un clúster de Amazon ECS y configure un servicio

Tarea	Descripción	Habilidades requeridas
Cree o elija un clúster.	Un clúster de Amazon ECS proporciona una agrupación lógica de tareas o servicios. Puede optar por utilizar un clúster existente o crear uno nuevo. Si decide crear un clúster nuevo, elija el tipo de clúster en función de sus necesidades. En nuestro ejemplo, seleccionamos un	Desarrollador, administrador del sistema

Tarea	Descripción	Habilidades requeridas
	clúster de redes. Proporcione un nombre para el clúster y elija si desea crear una nueva nube privada virtual (VPC) para utilizarla en las tareas de Fargate.	
Cree un servicio.	Dentro del clúster, seleccione Crear servicio.	Desarrollador, administrador del sistema
Elija el tipo de lanzamiento.	Elija Fargate como tipo de lanzamiento.	Desarrollador, administrador del sistema
Seleccione la definición de la tarea, la revisión y la versión de la plataforma.	Elija la tarea que desee ejecutar y, a continuación, revise la definición de la tarea y la versión de la plataforma.	Desarrollador, administrador del sistema
Seleccione el clúster.	Seleccione el clúster en el que desea crear el servicio en la lista desplegable.	Desarrollador, administrador del sistema
Introduzca un nombre de servicio.	Especifique un nombre exclusivo para el servicio que va a crear.	Desarrollador, administrador del sistema
Especifique el número de tareas.	Configure el número de tareas que deben ejecutarse cuando se inicie el servicio. Si lo inicia con dos o más tareas, se necesita un equilibrador de carga para equilibrar las tareas. El número mínimo de tareas que se deben configura r es una.	Desarrollador, administrador del sistema

Tarea	Descripción	Habilidades requeridas
Establezca los porcentajes sanos mínimo y máximo.	Configure los porcentajes de mantenimiento mínimo y máximo para la aplicación o acepte la opción predeterm inada que se proporciona.	Desarrollador, administrador del sistema
Configure los ajustes de implementación.	Elija el tipo de implementación en función de sus requisitos. Puede elegir una actualización progresiva o una implement ación azul/verde.	Desarrollador, administrador del sistema
Configure la VPC del clúster, las subredes y los grupos de seguridad.	Configure la VPC del clúster, las subredes en las que desea implementar la aplicación y los grupos de seguridad (HTTP, HTTPS y el puerto 8080) para proporcionar acceso a las conexiones entrantes/saliente s.	Desarrollador, administrador del sistema
Configure los ajustes de la IP pública.	Active o desactive la IP pública, en función de si desea utilizar una dirección IP pública para las tareas de Fargate.	Desarrollador, administrador del sistema
Configuración del equilibrador de carga.	Configure el equilibrador de carga si vas a lanzar el servicio con más de una tarea. Debe crear un equilibrador de carga y su grupo objetivo antes de lanzar el servicio.	Desarrollador, administrador del sistema

Tarea	Descripción	Habilidades requeridas
Configurar el escalado automático.	Configure su servicio para que utilice el servicio de escalado automático de Amazon ECS para ajustar el número deseado de tareas hacia arriba o hacia abajo, en función de sus requisitos.	Desarrollador, administrador del sistema
Revise la configuración y, a continuación, cree el servicio.	Revise la configuración del servicio y, a continuación, seleccione Crear servicio.	Desarrollador, administrador del sistema

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Pruebe la aplicación.	Pruebe la aplicación mediante el DNS público que se crea cuando se implementa la tarea. Si la aplicación tiene un equilibrador de carga, pruébela utilizándolo y, a continuación, proceda a realizar la transición.	Desarrollador, administrador del sistema

Recursos relacionados

- Conceptos básicos de Docker para Amazon ECS (documentación de Amazon ECS)
- Amazon ECS en AWS Fargate (documentación de Amazon ECS)
- Creación de un repositorio privado (documentación de Amazon ECR)
- Creación de una definición de tarea (documentación de Amazon ECS)
- Definiciones de contenedores (documentación de Amazon ECS)
- Creación de un clúster (documentación de Amazon ECS)

- Configuración de los parámetros básicos del servicio (documentación de Amazon ECS)
- Configuración de una red (documentación de Amazon ECS)
- Configuración del servicio para utilizar un equilibrador de carga (documentación de Amazon ECS)
- Configuración del servicio para utilizar el servicio de escalado automático (documentación de Amazon ECS)

Implementar microservicios de Java en Amazon ECS mediante Amazon ECR y el equilibrio de carga

Tipo R: N/D	Origen: Java	Destino: Amazon ECS
Creado por: AWS	Entorno: PoC o piloto	Tecnologías: aplicaciones web y móviles; contenedores y microservicios
Servicios de AWS: Amazon ECS		

Resumen

Este patrón describe los pasos para implementar una arquitectura de microservicios de Java en contenedores en Amazon Elastic Container Service (Amazon ECS) para facilitar el escalado y acelerar el desarrollo de sus aplicaciones. Esto permite la innovación y acelera la introducción time-to-market de nuevas funciones.

El patrón también utiliza Amazon Elastic Container Registry (Amazon ECR) para almacenar y gestionar los contenedores basados en Docker, y una plantilla de CloudFormation AWS con un script de Python para automatizar la configuración de la infraestructura. El patrón se basa en la entrada Implementación de microservicios de Java en Amazon Elastic Container Service, que está publicada en el blog de AWS Compute.

Los microservicios ofrecen un enfoque arquitectónico y organizativo para el desarrollo de software, en el que el software se compone de servicios pequeños e independientes que se comunican a través de interfaces de programación de aplicaciones (API) bien definidas. Estos servicios son propiedad de equipos pequeños e independientes.

Amazon ECS es un servicio de orquestación de contenedores de alto rendimiento y alta escalabilidad. Es compatible con contenedores de Docker y le permite ejecutar y escalar aplicaciones en contenedores en AWS con rapidez. Con Amazon ECS, ya no tiene que instalar y operar su software de orquestación de contenedores, administrar y escalar un clúster de máquinas virtuales (VM) ni programar contenedores en esas máquinas virtuales.

Con simples llamadas a la API, puede lanzar y detener aplicaciones compatibles con Docker, consultar el estado completo de su solicitud y acceder a muchas funciones naturales, como las funciones de AWS Identity and Access Management (IAM), los grupos de seguridad, los balanceadores de carga, los Amazon Events CloudWatch , las plantillas CloudFormation de AWS y los registros de AWS. CloudTrail

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Código fuente de los microservicios de Java, con el kit de desarrollo de Java, versión 1.7 o posterior
- Una clave de acceso y una clave de acceso secreta para un usuario de la cuenta
- Interfaz de la línea de comandos de AWS (AWS CLI)
- Java, kit de desarrollo de software (SDK) de AWS para Python (Boto3) y software Docker
- Conocimientos del uso de las tecnologías anteriores
- Familiaridad con los servicios de AWS, como Amazon ECS CloudFormation, AWS y Elastic Load Balancing

Arquitectura

Pila de tecnología de origen

- Microservicios implementados en Java e implementados en Apache Tomcat en un entorno en las instalaciones

Pila de tecnología de destino

- El equilibrador de carga de aplicación que inspecciona la solicitud del cliente. Según las reglas de enrutamiento, el equilibrador de cargas dirige la solicitud a una instancia y un puerto del grupo de destino que coincidan con el estado.
- Un grupo de destino para cada microservicio. Los servicios correspondientes utilizan los grupos de destino para registrar las instancias de contenedor disponibles. Cada grupo de destino tiene una ruta, por lo que cuando llama a la ruta para un microservicio concreto, se asigna al grupo de destino correcto. Esto le permite usar un equilibrador de carga de aplicación para prestar servicio

a todos los microservicios a los que acceda la ruta. Por ejemplo, https:///owner/* se aplicaría y dirigiría al microservicio Owner.

- Un clúster de Amazon ECS que aloja los contenedores de cada microservicio.
- Una red de Amazon Virtual Private Cloud (Amazon VPC) para alojar el clúster de Amazon ECS y los grupos de seguridad asociados.
- Un repositorio de Amazon Elastic Container Registry (Amazon ECR) para cada microservicio.
- Una definición de servicio o tarea para cada microservicio, que pone en marcha los contenedores en las instancias del clúster de Amazon ECS.

Arquitectura de destino

Herramientas

- Amazon ECS: Amazon ECS le permite lanzar y detener aplicaciones basadas en contenedores con llamadas API simples, le permite obtener el estado de su clúster de un servicio centralizado y le brinda acceso a muchas características familiares de Amazon Elastic Compute Cloud (Amazon EC2).
- Amazon ECR: Amazon Elastic Container Registry (Amazon ECR) es un registro de contenedores de Docker completamente administrado que facilita el almacenamiento, la administración y la implementación de imágenes de contenedores de Docker. Amazon ECR está integrado con Amazon ECS para simplificar su development-to-production flujo de trabajo. Amazon ECR aloja las imágenes en una arquitectura escalable y de alta disponibilidad, lo que le permite implementar contenedores para sus aplicaciones con fiabilidad. La integración con AWS Identity and Access Management (IAM) proporciona un control a nivel de recursos de cada repositorio.

Epics

Cree una CloudFormation plantilla de AWS para configurar un clúster de Amazon ECS para alojar los microservicios de Java

Tarea	Descripción	Habilidades requeridas
Aprovisione una instancia Linux Amazon EC2, instale		Ops

Tarea	Descripción	Habilidades requeridas
Docker y cree un archivo Docker para cada microserv icio.		
Configure las imágenes de Docker en Amazon ECR.	Use un Dockerfile para insertar la imagen compilarl a y etiquetarla para su nuevo repositorio. Haga lo mismo para cada microservicio. Inserte las imágenes recién etiquetadas al repositorio.	Ops
Cree una CloudFormation plantilla de AWS.	Cree una CloudFormation plantilla de AWS para aprovisionar la nube privada virtual (VPC), el clúster de Amazon ECS y Amazon Relational Database Service (Amazon RDS).	Ops

Aprovisionamiento de servicios de AWS

Tarea	Descripción	Habilidades requeridas
Cree la infraestructura de AWS con la CloudFormation plantilla que creó anteriorm ente.	Utilice el script de Python en https://github.com/awslabs/amazon-ecs-java-microservices/blob/master/2_ECS_Java_Spring_ PetClinic _Microservices/setup.py para invocar la CloudFormation plantilla de AWS que creó anteriormente. Esta plantilla crea la infraestructura de AWS	Ops

Tarea	Descripción	Habilidades requeridas
	que necesita para el entorno de destino.	
Cree repositorios, tareas, servicios, el equilibrador de carga de aplicación y grupos de destino de Amazon ECR.	El script de Python lee los resultados de la CloudForm ation plantilla de AWS y utiliza las llamadas a la API BOTO3 para crear repositorios, tareas y servicios de Amazon ECR, el Application Load Balancer y grupos objetivo.	Ops

Recursos relacionados

- Implementación de microservicios de Java en Amazon Elastic Container Service (entrada del blog de AWS Compute)
- Script de Python
- Documentación de Amazon ECS
- Conceptos básicos de Docker para Amazon ECS
- AWS SDK para Python
- Documentación de Amazon VPC
- Documentación de Amazon ECR

Implementar recursos y paquetes de Kubernetes con Amazon EKS y un repositorio de gráficos de Helm en Amazon S3

Creado por Sagar Panigrahi (AWS)

Entorno: PoC o piloto	Tecnologías: contenedores y microservicios; DevOps	Servicios de AWS: Amazon EKS

Resumen

Este patrón le ayuda a administrar las aplicaciones de Kubernetes de forma eficiente, independientemente de su complejidad. El patrón integra Helm en sus canalizaciones de integración y entrega continuas (CI/CD) existentes para implementar aplicaciones en un clúster de Kubernetes. Helm es un administrador de paquetes de Kubernetes que le ayuda a gestionar las aplicaciones de Kubernetes. Los gráficos de Helm le ayudan a definir, instalar y actualizar aplicaciones complejas de Kubernetes. Los gráficos se pueden versionar y almacenar en repositorios de Helm, lo que mejora el tiempo medio de restauración (MTTR) durante las interrupciones.

Este patrón utiliza Amazon Elastic Kubernetes Service (Amazon EKS) para el clúster de Kubernetes. Utiliza Amazon Simple Storage Service (Amazon S3) como repositorio de gráficos de Helm, de modo que todos los desarrolladores de la organización puedan gestionar y acceder a los gráficos de forma centralizada.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de Amazon Web Services (AWS) activa con una nube privada virtual (VPC)
- Un clúster de Amazon EKS
- Nodos de trabajo configurados dentro del clúster de Amazon EKS y preparados para soportar cargas de trabajo
- Kubectl para configurar el archivo kubeconfig de Amazon EKS para el clúster de destino en la máquina cliente
- Acceso de AWS Identity and Access Management (IAM) para crear el bucket de S3
- Acceso de IAM (mediante programación o de rol) a Amazon S3 desde la máquina cliente

- Administración de código fuente y una canalización de CI/CD

Limitaciones

- En este momento no se admite la actualización, la eliminación o la administración de las definiciones de recursos personalizadas (CRD).
- Si utiliza un recurso que hace referencia a una CRD, la CRD debe instalarse por separado (fuera del gráfico).

Versiones de producto

- Helm v3.6.3

Arquitectura

Pila de tecnología de destino

- Amazon EKS
- Amazon VPC
- Amazon S3
- Gestión de código fuente
- Helm
- Kubectl

Arquitectura de destino

Automatizar y escalar

- AWS se CloudFormation puede utilizar para automatizar la creación de la infraestructura. Para obtener más información, consulte Creación de recursos de Amazon EKS con AWS CloudFormation en la documentación de Amazon EKS.
- Helm se incorporará a su herramienta de automatización de CI/CD existente para automatizar el empaquetado y el control de versiones de los gráficos de Helm (algo fuera del alcance de este patrón).

- GitVersion o bien, se pueden utilizar los números de compilación de Jenkins para automatizar el control de versiones de los gráficos.

Herramientas

Herramientas

- Amazon EKS: Amazon Elastic Kubernetes Service (Amazon EKS) es un servicio administrado para ejecutar Kubernetes en AWS sin necesidad de crear ni mantener su propio plano de control de Kubernetes. Kubernetes es un sistema de código abierto para automatizar la implementación, escalado y administración de las aplicaciones en contenedores.
- Helm: Helm es un administrador de paquetes para Kubernetes que le ayuda a instalar y administrar aplicaciones en su clúster de Kubernetes.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet. Puede utilizar Amazon S3 para almacenar y recuperar cualquier cantidad de datos en cualquier momento y desde cualquier parte de la web.
- Kubectl: Kubectl es una utilidad de la línea de comandos para la ejecución de comandos en clústeres de Kubernetes.

Código

Se adjunta el código de ejemplo.

Epics

Configurar e inicializar Helm

Tarea	Descripción	Habilidades requeridas
Instalar el cliente Helm.	Para descargar e instalar el cliente Helm en su sistema local, utilice el siguiente comando. `sudo curl https://raw.githubusercontent.com/helm/helm/m`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`aster/scripts/get-helm-3 | bash`	
Validar la instalación de Helm.	Para validar que Helm puede comunicarse con el servidor API de Kubernetes del clúster de Amazon EKS, ejecute `helm version`.	DevOps ingeniero

Crear e instalar un gráfico de Helm en el clúster de Amazon EKS

Tarea	Descripción	Habilidades requeridas
Crear un gráfico de Helm para NGINX.	Para crear un gráfico de Helm llamado `my-nginx` en la máquina cliente, ejecute `helm create my-nginx`.	DevOps ingeniero
Revisar la estructura del gráfico.	Para revisar la estructura del gráfico, ejecute el comando tree `tree my-nginx/ .`	DevOps ingeniero
Desactive la creación de cuentas de servicio en el gráfico.	En `values.yaml` , en la sección `serviceAccount` , establezca la clave `create` en `false`. Esta opción está desactivada porque no es necesario crear una cuenta de servicio para este patrón.	DevOps ingeniero
Validar (lint) el gráfico modificado para detectar errores sintácticos.	Para validar el gráfico para detectar cualquier error sintáctico antes de instalarl o en el clúster de destino,	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	ejecute `helm lint my-nginx/` .	
Instale el gráfico para implementar los recursos de Kubernetes.	Para ejecutar la instalación del gráfico de Helm, utilice el siguiente comando. `helm install --name my-nginx-release --debug my-nginx/ --namespace helm-space` La marca opcional `debug` muestra todos los mensajes de depuración durante la instalación. La marca `namespace` especifica el espacio de nombres en el que se creará la parte de recursos de este gráfico.	DevOps ingeniero
Revisar los recursos del clúster de Amazon EKS.	Para revisar los recursos que se crearon como parte del gráfico de Helm en el espacio de nombres `helm-space` , utilice el siguiente comando. `kubectl get all -n helm-space`	DevOps ingeniero

Restaurar una versión anterior de una aplicación de Kubernetes

Tarea	Descripción	Habilidades requeridas
Modifique y actualice la versión.	Para modificar el gráfico, en `values.yaml` , cambie el valor `replicaCount` a 2. A continuación, ejecute el siguiente comando para actualizar la versión ya instalada. `helm upgrade my-nginx-release my-nginx/ --namespace helm-space`	DevOps ingeniero
Revisar el historial de la versión de Helm.	Para ver todas las revisiones de una versión específica instalada con Helm, ejecute el siguiente comando. `helm history my-nginx-release`	DevOps ingeniero
Comprobar los detalles de una revisión específica.	Antes de cambiar a o restaurar una versión operativa, y para obtener una capa adicional de validación antes de instalar una revisión, compruebe qué valores se han pasado a cada una de las revisiones mediante el siguiente comando. `helm get --revision=2 my-nginx-release`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Restaurar una versión anterior.	Para restaurar una revisión anterior, utilice el siguiente comando. `helm rollback my-nginx-release 1` Este ejemplo restaura la revisión número 1.	DevOps ingeniero

Inicializar un bucket de S3 como repositorio de Helm

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3 para gráficos de Helm.	Cree un bucket de S3 único. En el bucket, cree una carpeta llamada `charts`. El ejemplo de este patrón usa `s3://my-helm-charts/charts` como repositorio de gráficos de destino.	Administrador de la nube
Instalar el complemento de Helm para Amazon S3.	Para instalar el complemento helm-s3 en su máquina cliente, utilice el siguiente comando. `helm plugin install https://github.com/hypnoglow/helm-s3.git --version 0.10.0` Nota: El soporte de Helm V3 está disponible con la	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	versión 0.9.0 y superior del complemento.	
Inicializar el repositorio de Helm de Amazon S3.	Para inicializar la carpeta de destino como repositorio de Helm, utilice el siguiente comando. `helm S3 init s3://my-helm-charts/charts` El comando crea un archivo `index.yaml` en el destino para rastrear toda la información del gráfico almacenada en esa ubicación.	DevOps ingeniero
Añada el repositorio de Amazon S3 a Helm.	Para añadir el repositorio a la máquina cliente, utilice el siguiente comando. `helm repo add my-helm-charts s3://my-helm-charts/charts` Este comando añade un alias al repositorio de destino de la máquina cliente de Helm.	DevOps ingeniero
Revisar la lista de repositorios.	Para ver la lista de repositorios de la máquina cliente de Helm, ejecute `helm repo list`.	DevOps ingeniero

Empaquetar y almacenar gráficos en el repositorio de Helm de Amazon S3

Tarea	Descripción	Habilidades requeridas
Empaquetar el gráfico.	Para empaquetar el gráfico `my-nginx` que creó, ejecute `helm package ./my-nginx/` . El comando empaqueta todo el contenido de la carpeta de gráficos `my-nginx` en un archivo de almacenamiento que se nombra según el número de versión mencionado en el archivo `Chart.yaml` .	DevOps ingeniero
Almacenar el paquete en el repositorio de Helm de Amazon S3.	Para cargar el paquete en el repositorio de Helm de Amazon S3, ejecute el siguiente comando usando el nombre correcto del archivo `.tgz`. `helm s3 push ./my-nginx-0.1.0.tgz my-helm-charts`	DevOps ingeniero
Buscar el gráfico de Helm.	Para confirmar que el gráfico aparece tanto localmente como en el repositorio de Helm de Amazon S3, ejecute el siguiente comando. `helm search repo my-nginx`	DevOps ingeniero

Modificar, versionar y empaquetar un gráfico

Tarea	Descripción	Habilidades requeridas
Modifique y empaquete el gráfico.	En `values.yaml` , defina el valor de `replicaCount` en 1. A continuación, ejecute `helm package ./my-nginx/` para empaquetar el gráfico, esta vez cambiando la versión en `Chart.yaml` a `0.1.1`. Lo ideal es actualizar el control de versiones mediante la automatización mediante herramientas como GitVersion los números de compilación de Jenkins en una canalización de CI/CD. La automatización del número de versión está fuera del alcance de este patrón.	DevOps ingeniero
Enviar la nueva versión al repositorio de Helm de Amazon S3.	Para enviar el nuevo paquete, versión 0.1.1, al repositorio de Helm `my-helm-charts` de Amazon S3, ejecute el siguiente comando. `helm s3 push ./my-nginx-0.1.1.tgz my-helm-charts`	DevOps ingeniero

Buscar e instalar un gráfico en el repositorio de Helm de Amazon S3

Tarea	Descripción	Habilidades requeridas
Buscar todas las versiones del gráfico my-nginx.	Para ver todas las versiones disponibles de un gráfico, ejecute el siguiente comando con la marca `--versions` . `helm search repo my-nginx --versions` Sin la marca, Helm mostrará de forma predeterminada la última versión cargada de un gráfico.	DevOps ingeniero
Instalar un gráfico desde el repositorio de Helm de Amazon S3.	Los resultados de búsqueda de la tarea anterior mostrarán las múltiples versiones del gráfico `my-nginx`. Para instalar la nueva versión (0.1.1) desde el repositorio de Helm de Amazon S3, utilice el siguiente comando. `helm upgrade my-nginx-release my-helm-charts/my-nginx --version 0.1.1 --namespace helm-space`	DevOps ingeniero

Recursos relacionados

- Documentación de HELM
- Complemento helm-s3 (licencia MIT)

- Binario del cliente HELM
- Documentación de Amazon EKS

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Implementar funciones de Lambda con imágenes de contenedor

Creado por Ram Kandaswamy (AWS)

Entorno: producción	Tecnologías: contenedores y microservicios; nativo en la nube; desarrollo y pruebas de software; sin servidor	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon EC2 Container Registry; AWS Lambda		

Resumen

AWS Lambda admite imágenes de contenedores como modelo de implementación. Este patrón muestra cómo implementar funciones de Lambda a través de imágenes de contenedor.

Lambda es un servicio de computación controlado por eventos sin servidor que permite ejecutar código para prácticamente cualquier tipo de aplicación o servicio de backend, sin aprovisionar ni administrar servidores. La compatibilidad con imágenes de contenedores para las funciones de Lambda le otorga hasta 10 GB de almacenamiento para el artefacto de la aplicación y la posibilidad de utilizar herramientas de desarrollo de imágenes de contenedores conocidas.

El ejemplo de este patrón usa Python como lenguaje de programación subyacente, pero puede usar otros lenguajes, como Java, Node.js o Go. El patrón usa AWS CodeCommit como fuente, pero también puedes usar GitHub Bitbucket o Amazon Simple Storage Service (Amazon S3).

Requisitos previos y limitaciones

Requisitos previos

- Amazon Elastic Container Registry (Amazon ECR) activado
- Código de la aplicación
- Imágenes de Docker con el cliente de interfaz de tiempo de ejecución y la última versión de Python

Limitaciones

- El máximo tamaño de imagen soportado es de 10 GB.
- El tiempo de ejecución máximo para una implementación de contenedores basada en Lambda es de 15 minutos.

Arquitectura

Pila de tecnología de destino

- Lenguaje de programación Python
- AWS CodeBuild
- AWS CodeCommit
- Imagen de Docker
- Amazon ECR
- AWS Identity y Access Management (IAM)
- AWS Lambda
- Amazon CloudWatch Logs

Arquitectura de destino

1. Creas un repositorio y confirmas el código de la aplicación mediante CodeCommit.
2. El CodeBuild proyecto se inicia cuando se realiza un cambio en CodeCommit, que se utiliza como proveedor de código fuente.
3. El CodeBuild proyecto crea la imagen de Docker y la publica en Amazon ECR.
4. Crea una función de Lambda con la imagen de Amazon ECR.

Automatizar y escalar

Este patrón se puede automatizar mediante AWS CloudFormation, el AWS Cloud Development Kit (AWS CDK) o las operaciones de API desde un SDK. Lambda puede escalar automáticamente en función del número de solicitudes y se puede ajustar mediante los parámetros de simultaneidad. Para obtener más información, consulte la documentación de Lambda.

Herramientas

Servicios de AWS

- AWS CloudFormation Designer proporciona un editor JSON y YAML integrado que le ayuda a ver y editar CloudFormation plantillas.
- AWS CodeBuild es un servicio de compilación totalmente gestionado que le ayuda a compilar código fuente, ejecutar pruebas unitarias y producir artefactos listos para su implementación.
- AWS CodeCommit es un servicio de control de versiones que le ayuda a almacenar y gestionar repositorios de Git de forma privada, sin necesidad de gestionar su propio sistema de control de código fuente.
- AWS CodeStar es un servicio basado en la nube para crear, administrar y trabajar con proyectos de desarrollo de software en AWS. Para este patrón, puede usar AWS CodeStar u otro entorno de desarrollo.
- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable.
- AWS Lambda es un servicio de computación que le permite ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.

Otras herramientas

- Docker es un conjunto de productos de plataforma como servicio (PaaS) que utiliza la virtualización a nivel del sistema operativo para entregar software en contenedores.

Prácticas recomendadas

- Cree funciones lo más eficientes y pequeñas que sea posible para evitar la carga de archivos innecesarios.
- Trate de colocar las capas estáticas en la parte superior de la lista de archivos de Docker y coloque las capas que cambien con más frecuencia en la parte inferior. Esto mejora el almacenamiento en caché, lo que mejora el rendimiento.

- El propietario de la imagen es responsable de actualizar y parchear la imagen. Añada esa cadencia de actualización a sus procesos operativos. Para obtener más información, consulte la documentación de AWS Lambda.

Epics

Cree un proyecto en CodeBuild

Tarea	Descripción	Habilidades requeridas
Crea un CodeCommit repositorio.	Cree un CodeCommit repositorio que contenga el Dockerfile, el `buildspec .yaml` archivo y el código fuente de la aplicación. Para obtener más información, consulte la CodeCommit documentación de AWS.	Desarrollador
Cree un CodeBuild proyecto.	En la CodeBuild consola, crea un proyecto nuevo que utilice el CodeCommit repositorio y el `buildspec.yaml` archivo. Utilizará el CodeBuild proyecto para crear la imagen. Confirme que el modo con privilegios esté habilitad o. Esto es necesario para compilar imágenes de Docker. De lo contrario, la imagen no se compilará correctamente. Introduzca el nombre y la descripción del proyecto. Para el proveedor de origen, elija CodeCommit. Para obtener	Desarrollador

Tarea	Descripción	Habilidades requeridas
	más información, consulte la documentación de AWS.	
Edite el Dockerfile.	El Dockerfile debe estar ubicado en el directorio de nivel superior en el que se está desarrollando la aplicación. El código de Python debe estar en la carpeta `src`. Al crear la imagen, utilice las imágenes oficiales compatibles con Lambda. De lo contrario, se producirá un error de arranque que dificultará el proceso de empaquetado. Para obtener más información, consulte la sección Información adicional.	Desarrollador
Crear un repositorio en Amazon ECR.	Cree un repositorio de contenedores en Amazon ECR. En el siguiente comando de ejemplo, el nombre del repositorio creado es `cf-demo`. El repositorio se reutilizará en el archivo `buildspec.yaml` . `aws ecr create-repository --cf-demo`	Administrador de AWS, desarrollador

Tarea	Descripción	Habilidades requeridas
Enviar la imagen a Amazon ECR.	Se puede utilizar CodeBuild para realizar el proceso de creación de imágenes. CodeBuild necesita permiso para interactuar con Amazon ECR y trabajar con S3. Como parte del proceso, la imagen de Docker se compila y envía al registro de Amazon ECR. Para obtener información sobre la plantilla y el código, consulte la sección Información adicional.	Desarrollador
Verificar que la imagen está en el repositorio.	Para verificar que la imagen se encuentra en el repositorio, seleccione Repositorios en la consola de Amazon ECR. Si esa característica estaba activada en la configuración de Amazon ECR, la imagen debería aparecer en la lista, junto con etiquetas y los resultados de un informe de análisis de vulnerabilidades. Para obtener más información, consulte la documentación de AWS.	Desarrollador

Crear la función de Lambda para ejecutar la imagen

Tarea	Descripción	Habilidades requeridas
Crear la función de Lambda.	En la consola de Lambda, seleccione Crear función y, a continuación, seleccion e Imagen de contenedor. Introduzca el nombre de la función y el URI de la imagen que se encuentra en el repositorio de Amazon ECR y, a continuación, seleccione Crear función. Para obtener más información, consulte la documentación de AWS Lambda.	Desarrollador de aplicaciones
Probar la función de Lambda.	Seleccione Probar para invocar y probar la función. Para obtener más información, consulte la documentación de AWS Lambda.	Desarrollador de aplicaciones

Solución de problemas

Problema	Solución
La compilación no se está realizando correctam ente.	1. Compruebe si el modo privilegiado está activado para el CodeBuild proyecto. 2. Asegúrese de que los comandos relaciona dos con Docker tengan los permisos necesarios. Se intenta añadir `sudo` a los comandos. 3. Compruebe que la función de IAM asociada CodeBuild tenga una política con las

Problema	Solución
	acciones adecuadas para interactuar con Amazon ECR, Amazon S3 y CloudWatch los registros.

Recursos relacionados

- Imágenes base para Lambda
- Ejemplo de Docker para CodeBuild
- Credenciales de paso temporales

Información adicional

Editar el Dockerfile

El siguiente código muestra los comandos que usted edita en el Dockerfile.

```
FROM public.ecr.aws/lambda/python:3.11

# Copy function code
COPY app.py ${LAMBDA_TASK_ROOT}
COPY requirements.txt  ${LAMBDA_TASK_ROOT}

# install dependencies
RUN pip3 install --user -r requirements.txt

# Set the CMD to your handler (could also be done as a parameter override outside of
 the Dockerfile)
CMD [ "app.lambda_handler" ]
```

El valor del comando `FROM` corresponde a la imagen base de Python 3.11 que utiliza la función de Lambda en el repositorio público de imágenes de Amazon ECR.

El comando `COPY app.py ${LAMBDA_TASK_ROOT}` copia el código en el directorio raíz de la tarea, que la función de Lambda utilizará. Este comando usa la variable de entorno, por lo que no hay que preocuparse por la ruta real. La función que se va a ejecutar se pasa como argumento al comando `CMD [ "app.lambda_handler" ]`.

El comando `COPY requirements.txt` captura las dependencias necesarias para el código.

El comando `RUN pip install --user -r requirements.txt` instala las dependencias en el directorio de usuarios local.

Para compilar su imagen, ejecute el siguiente comando.

```
docker build -t <image name> .
```

Añadir la imagen en Amazon ECR

En el siguiente código, sustituya `aws_account_id` por el número de cuenta, y sustituya `us-east-1` si utiliza una región diferente. El `buildspec` archivo usa el número de CodeBuild compilación para identificar de forma exclusiva las versiones de las imágenes como un valor de etiqueta. Puede cambiarlo para adaptarlo a sus necesidades.

El código personalizado de buildspec

```
phases:
  install:
    runtime-versions:
       python: 3.11
  pre_build:
    commands:
      - python3 --version
      - pip3 install --upgrade pip
      - pip3 install --upgrade awscli
      - sudo docker info
  build:
    commands:
      - echo Build started on `date`
      - echo Building the Docker image...
      - ls
      - cd app
      - docker build -t cf-demo:$CODEBUILD_BUILD_NUMBER .
      - docker container ls
  post_build:
    commands:
      - echo Build completed on `date`
      - echo Pushing the Docker image...
      - aws ecr get-login-password --region us-east-1 | docker login --username AWS --
password-stdin aws_account_id.dkr.ecr.us-east-1.amazonaws.com
```

```
      - docker tag cf-demo:$CODEBUILD_BUILD_NUMBER aws_account_id.dkr.ecr.us-
east-1.amazonaws.com/cf-demo:$CODEBUILD_BUILD_NUMBER
      - docker push aws_account_id.dkr.ecr.us-east-1.amazonaws.com/cf-demo:
$CODEBUILD_BUILD_NUMBER
```

Implemente un microservicio Java de muestra en Amazon EKS y exponga el microservicio mediante un Equilibrador de carga de aplicación

Creado por Vijay Thompson (AWS) y Akkamahadevi Hiremath (AWS)

Entorno: PoC o piloto	Tecnologías: contenedores y microservicios	Carga de trabajo: código abierto
Servicios de AWS: Amazon EC2 Container Registry; Amazon EKS; Amazon ECR		

Resumen

Este patrón describe cómo implementar un microservicio Java de muestra como una aplicación en contenedores en Amazon Elastic Kubernetes Service (Amazon EKS) mediante la utilidad de línea de comandos `eksctl` y Amazon Elastic Container Registry (Amazon ECR). Puede usar un equilibrador de carga de aplicación para equilibrar la carga del tráfico de la aplicación.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- La Interfaz de la línea de comandos de AWS (AWS CLI) versión 1.7, instalada y configurada en Linux, macOS o Windows
- Un daemon de Docker en ejecución
- La utilidad de línea de comandos `eksctl`, instalada y configurada en macOS, Linux o Windows (para obtener más información, consulte Introducción a Amazon EKS — eksctl en la documentación de Amazon EKS).
- La utilidad de línea de comandos `kubectl`, instalada y configurada en macOS, Linux o Windows (para obtener más información, consulte Instalar o actualizar eksctl en la documentación de Amazon EKS).

Limitaciones

- Este patrón no cubre la instalación de un certificado SSL para el Equilibrador de carga de aplicación.

Arquitectura

Pila de tecnología de destino

- Amazon ECR
- Amazon EKS
- Elastic Load Balancing

Arquitectura de destino

El siguiente diagrama muestra una arquitectura para organizar en contenedores un microservicio Java en Amazon EKS.

Herramientas

- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable.
- Amazon Elastic Kubernetes Service (Amazon EKS) lo ayuda a ejecutar Kubernetes en AWS sin necesidad de instalar ni mantener su propio plano de control o nodos de Kubernetes.
- La Interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su shell de línea de comandos.
- Elastic Load Balancing distribuye automáticamente el tráfico entrante entre varios destinos, por ejemplo, instancias de Amazon Elastic Compute Cloud (Amazon EC2), contenedores y direcciones IP en una o varias zonas de disponibilidad.
- eksctl le ayuda a crear clústeres en Amazon EKS.
- kubectl permite ejecutar comandos en clústeres de Kubernetes.
- Docker le ayuda a crear, probar y entregar aplicaciones en paquetes llamados contenedores.

Epics

Crear un clúster de Amazon EKS mediante eksctl

Tarea	Descripción	Habilidades requeridas
Cree un clúster de Amazon EKS.	Para crear un clúster de Amazon EKS que utilice dos instancias t2.small de Amazon EC2 como nodos, ejecute el siguiente comando: `eksctl create cluster --name <your-cluster-name> --version <version-number> --nodes=1 --node-type=t2.small` Nota: el proceso puede tardar entre 15 y 20 minutos. Una vez creado el clúster, se añade la configuración de Kubernetes adecuada al archivo kubeconfig. Puede usar el archivo `kubeconfig` con `kubectl` para implement ar la aplicación en pasos posteriores.	Desarrollador, administrador del sistema
Verifique el clúster de Amazon EKS.	Para comprobar que se ha creado el clúster y que puede conectarse a él, ejecute el comando `kubectl get nodes`.	Desarrollador, administrador del sistema

Cree un repositorio de Amazon ECR y envíe la imagen de Docker.

Tarea	Descripción	Habilidades requeridas
Cree un repositorio de Amazon ECR.	Siga las instrucciones de Creación de un repositorio privado en la documentación de Amazon ECR.	Desarrollador, administrador del sistema
Cree un archivo XML POM.	Cree un archivo `pom.xml` basado en el ejemplo de código de archivo POM de la sección de información adicional de este patrón.	Desarrollador, administrador del sistema
Cree un archivo de origen.	Cree un archivo de origen llamado `HelloWorld.java` en la ruta `src/main/java/eksExample` según el siguiente ejemplo: `package eksExample;` `import static spark.Spark.get;` `public class HelloWorld {` `  public static void main(String[] args) {` `  get("/", (req, res) -> {` `  return "Hello World!";` `  });` `  }` `}` Asegúree de usar la siguiente estructura de directorios:	

Tarea	Descripción	Habilidades requeridas
	`` ### Dockerfile ### deployment.yaml ### ingress.yaml ### pom.xml ### service.yaml ### src ### main ### java ### eksExample ### HelloWorld.java ```	
Cree un Dockerfile.	Cree un archivo `Dockerfile` basado en el ejemplo de código de Dockerfile de la sección de información adicional de este patrón.	Desarrollador, administrador del sistema

Tarea	Descripción	Habilidades requeridas
Cree y envíe la imagen de Docker.	En el directorio en el que desee que su `Dockerfile` compile, etiquete y envie la imagen a Amazon ECR, ejecute los siguientes comandos: `aws ecr get-login -password --region <region>| docker login --username <username> --password-stdin <account_number>.dkr.ecr.<region>.amazonaws.com` `docker buildx build --platform linux/amd64 -t hello-world-java:v1 .` `docker tag hello-world-java:v1 <account_number>.dkr.ecr.<region>.amazonaws.com/<repository_name>:v1` `docker push <account_number>.dkr.ecr.<region>.amazonaws.com/<repository_name>:v1` Nota: modifique la región de AWS, el número de cuenta y los detalles del repositorio en los comandos anteriores. Asegúrese de anotar la URL de la imagen para usarla más adelante.	

Tarea	Descripción	Habilidades requeridas
	Importante: un sistema macOS con un chip M1 tiene problemas para crear una imagen compatible con Amazon EKS que se ejecuta en una plataforma AMD64. Para resolver este problema, utilice docker buildx para crear una imagen de Docker que funcione en Amazon EKS.	

Implemente los microservicios de Java

Tarea	Descripción	Habilidades requeridas
Cree un archivo implement ación.	Cree un archivo YAML llamado `deployment.yaml` basado en el ejemplo de código de archivo de implementación de la sección de información adicional de este patrón. Nota: utilice la URL de la imagen que copió anteriorm ente como ruta del archivo de imagen para el repositorio de Amazon ECR.	Desarrollador, administrador del sistema
Implemente los microserv icios de Java en el clúster de Amazon EKS.	Para crear una implement ación en su clúster de Amazon EKS, ejecute el comando `kubectl apply -f deployment.yaml` .	Desarrollador, administrador del sistema

Tarea	Descripción	Habilidades requeridas
Verifique el estado de los pods.	1. Para verificar el estado de los pods, ejecute el comando `kubectl get pods`. 2. Espere a que el estado cambie a Listo.	Desarrollador, administrador del sistema
Cree un servicio.	1. Cree un archivo llamado `service.yaml` basado en el ejemplo de código de archivo de servicio de la sección de información adicional de este patrón. 2. Ejecute el comando `kubectl apply -f service.yaml .`	Desarrollador, administrador del sistema
Instalación del complemento controlador del equilibrador de carga de AWS.	Siga las instrucciones de Instalación del complemento controlador del equilibrador de carga de AWS en la documentación de Amazon EKS. Nota: debe tener el complemento instalado para crear un Equilibrador de carga de aplicación o un Equilibrador de carga de red para un servicio de Kubernetes.	Desarrollador, administrador del sistema

Tarea	Descripción	Habilidades requeridas
Cree un recurso de ingreso.	Cree un archivo YAML llamado `ingress.yaml` basado en el ejemplo de código de archivo de recurso de la sección de información adicional de este patrón.	Desarrollador, administrador del sistema
Creación de un Equilibrador de carga de aplicación.	Para implementar el recurso de ingreso y crear un Equilibrador de carga de aplicación, ejecute el comando `kubectl apply -f ingress.yaml` .	Desarrollador, administrador del sistema

Pruebe la aplicación

Tarea	Descripción	Habilidades requeridas
Pruebe y verifique la aplicación.	1. Para obtener el nombre DNS del equilibrador de carga en el campo ADDRESS, ejecute el comando `kubectl get ingress.networking.k8s.io/java-microservice-ingress` . 2. En una instancia EC2 de la misma VPC que los nodos de Amazon EKS, ejecute el comando `curl -v <DNS address from previous command>`.	Desarrollador, administrador del sistema

Recursos relacionados

- Creación de un repositorio privado (documentación de Amazon ECR)
- Enviar una imagen de Docker (documentación de Amazon ECR)
- Controladores de ingreso (taller de Amazon EKS)
- Docker buildx (documentación de Docker)

Información adicional

Ejemplo de archivo POM

```
<?xml version="1.0" encoding="UTF-8"?>
<project xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/xsd/
maven-4.0.0.xsd">
  <modelVersion>4.0.0</modelVersion>


  <groupId>helloWorld</groupId>
  <artifactId>helloWorld</artifactId>
  <version>1.0-SNAPSHOT</version>


  <dependencies>
    <dependency>
      <groupId>com.sparkjava</groupId><artifactId>spark-core</
artifactId><version>2.0.0</version>
    </dependency>
  </dependencies>
  <build>
    <plugins>
      <plugin>
        <groupId>org.apache.maven.plugins</groupId><artifactId>maven-jar-plugin</
artifactId><version>2.4</version>
        <configuration><finalName>eksExample</finalName><archive><manifest>
              <addClasspath>true</addClasspath><mainClass>eksExample.HelloWorld</
mainClass><classpathPrefix>dependency-jars/</classpathPrefix>
            </manifest></archive>
        </configuration>
      </plugin>
```

```
      <plugin>
        <groupId>org.apache.maven.plugins</groupId><artifactId>maven-compiler-plugin</
artifactId><version>3.1</version>
        <configuration><source>1.8</source><target>1.8</target></configuration>
      </plugin>
      <plugin>
        <groupId>org.apache.maven.plugins</groupId><artifactId>maven-assembly-plugin</
artifactId>
        <executions>
          <execution>
            <goals><goal>attached</goal></goals><phase>package</phase>
            <configuration>
              <finalName>eksExample</finalName>
              <descriptorRefs><descriptorRef>jar-with-dependencies</descriptorRef></
descriptorRefs>
              <archive><manifest><mainClass>eksExample.HelloWorld</mainClass></
manifest></archive>
            </configuration>
          </execution>
        </executions>
      </plugin>
    </plugins>
  </build>
</project>
```

Ejemplo de Dockerfile

```
FROM bellsoft/liberica-openjdk-alpine-musl:17

RUN apk add maven
WORKDIR /code

# Prepare by downloading dependencies
ADD pom.xml /code/pom.xml
RUN ["mvn", "dependency:resolve"]
RUN ["mvn", "verify"]

# Adding source, compile and package into a fat jar
ADD src /code/src
RUN ["mvn", "package"]

EXPOSE 4567
CMD ["java", "-jar", "target/eksExample-jar-with-dependencies.jar"]
```

Ejemplo de archivo de implementación

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: microservice-deployment
spec:
  replicas: 2
  selector:
    matchLabels:
      app.kubernetes.io/name: java-microservice
  template:
    metadata:
      labels:
        app.kubernetes.io/name: java-microservice
    spec:
      containers:
      - name: java-microservice-container
        image: .dkr.ecr.amazonaws.com/:
        ports:
        - containerPort: 4567
```

Ejemplo de archivo de servicio

```
apiVersion: v1
kind: Service
metadata:
  name: "service-java-microservice"
spec:
  ports:
    - port: 80
      targetPort: 4567
      protocol: TCP
  type: NodePort
  selector:
    app.kubernetes.io/name: java-microservice
```

Ejemplo de archivo de recursos de ingreso

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
```

```
  name: "java-microservice-ingress"
  annotations:
    kubernetes.io/ingress.class: alb
    alb.ingress.kubernetes.io/load-balancer-name: apg2
    alb.ingress.kubernetes.io/target-type: ip
  labels:
    app: java-microservice
spec:
  rules:
    - http:
        paths:
          - path: /
            pathType: Prefix
            backend:
              service:
                name: "service-java-microservice"
                port:
                  number: 80
```

Implementar una aplicación agrupada en Amazon ECS con AWS Copilot

Creado por Jean-Baptiste Guillois (AWS), Mathew George (AWS) y Thomas Scott (AWS)

Repositorio de código: demostración de una aplicación de muestra agrupada	Entorno: producción	Tecnologías: contenedores y microservicios; productividad empresarial; nativo en la nube; desarrollo y pruebas de software
Servicios de AWS: Amazon ECS; AWS Fargate; Amazon ECR		

Resumen

Este patrón muestra cómo implementar contenedores en un clúster de Amazon Elastic Container Service (Amazon ECS) de dos maneras: mediante la consola de administración de Amazon Web Services (AWS) y mediante AWS Copilot, para demostrar cómo AWS Copilot simplifica las tareas de implementación.

Amazon ECS es un servicio de administración de contenedores altamente escalable y rápido que facilita la tarea de ejecutar, detener y administrar contenedores en un clúster. Los contenedores se definen en una definición de tareas que se utiliza para ejecutar tareas individuales o tareas dentro de un servicio. Puede ejecutar sus tareas y servicios en una infraestructura sin servidor administrada por AWS Fargate. Alternativamente, para obtener más control sobre su infraestructura, puede ejecutar sus tareas y servicios en un clúster de instancias de Amazon Elastic Compute Cloud (Amazon EC2) que administre.

Los comandos de la interfaz de la línea de comandos (CLI) de AWS Copilot simplifican la creación, el lanzamiento y el uso de aplicaciones en contenedores listas para producción en Amazon ECS desde un entorno de desarrollo local. La CLI de AWS Copilot se alinea con los flujos de trabajo de los desarrolladores que admiten prácticas recomendadas de aplicaciones modernas: desde la utilización de infraestructura como código hasta la creación de una canalización de integración y entrega continuas (CI/CD) aprovisionada en nombre de un usuario. Puede utilizar la CLI de AWS

Copilot como parte de su ciclo cotidiano de desarrollo y prueba o como alternativa a la Consola de administración de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada localmente para usar su cuenta de AWS (consulte las instrucciones de instalación y las instrucciones de configuración en la documentación de la CLI de AWS)
- AWS Copilot instalado localmente (consulte las instrucciones de instalación en la documentación de Amazon ECS)
- Docker instalado en su máquina local (consulte la documentación de Docker)

Limitaciones

- En el plan gratuito, Docker impone un límite de extracción de 100 imágenes de contenedor por cada 6 horas por dirección IP.

Arquitectura

Pila de tecnología de destino

- Entorno de AWS configurado con una nube privada virtual (VPC), subredes públicas y privadas y grupos de seguridad
- Clúster de Amazon ECS
- Definición de tareas y servicios de Amazon ECS
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon DynamoDB
- Equilibrador de carga de aplicación
- AWS Fargate
- Amazon Identity and Access Management (IAM)
- Amazon CloudWatch
- AWS CloudTrail

Arquitectura de destino

Al implementar la aplicación de muestra para este patrón, se crean e implementan varias tareas en zonas de disponibilidad independientes. Cada tarea almacena datos en Amazon DynamoDB. Al acceder a la página web de una tarea, puede ver los datos de todas las demás tareas.

Herramientas

Servicios de AWS

- Amazon ECR : Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado por AWS que es seguro, escalable y fiable. Amazon ECR admite repositorios privados con permisos basados en recursos mediante IAM.
- Amazon ECS: Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores altamente escalable y rápido que permite ejecutar, detener y administrar contenedores en un clúster. Puede ejecutar sus tareas y servicios en una infraestructura sin servidor administrada por AWS Fargate. Alternativamente, para obtener más control sobre su infraestructura, puede ejecutar sus tareas y servicios en un clúster de instancias de Amazon Elastic Compute Cloud (Amazon EC2) que administre.
- AWS Copilot: AWS Copilot proporciona una interfaz de la línea de comandos que le ayuda a lanzar y administrar aplicaciones en contenedores en AWS, incluyendo su envío a un registro, la creación de una definición de tarea y la creación de un clúster.
- AWS Fargate: AWS Fargate es un motor de pay-as-you-go cómputo sin servidor que le permite centrarse en crear aplicaciones sin tener que administrar servidores. AWS Fargate es compatible tanto con Amazon ECS como con Amazon Elastic Kubernetes Service (Amazon EKS). Al ejecutar las tareas y los servicios de Amazon ECS con el tipo de lanzamiento de Fargate o un proveedor de capacidad de Fargate, la aplicación se empaqueta en contenedores, se especifican los requisitos de CPU y de memoria, se definen las políticas de IAM y las redes, y se lanza la aplicación. Cada tarea de Fargate tiene su propio límite de aislamiento y no comparte el kernel subyacente, los recursos de CPU, los recursos de memoria ni la interfaz de red elástica con otra tarea.
- Amazon DynamoDB: Amazon DynamoDB es un servicio de base de datos NoSQL totalmente administrado que ofrece un rendimiento rápido y predecible, así como una perfecta escalabilidad.
- Elastic Load Balancing (ELB): Elastic Load Balancing distribuye automáticamente su tráfico entrante en varios destinos, por ejemplo, instancias de EC2, contenedores y direcciones IP en una o varias zonas de disponibilidad. Monitorea el estado de los destinos registrados y enruta el tráfico

solamente a destinos en buen estado. Elastic Load Balancing escala el equilibrador de carga a medida que el tráfico entrante va cambiando con el tiempo. Puede escalarse automáticamente para adaptarse a la mayoría de las cargas de trabajo.

Herramientas

- Interfaz de la línea de comandos de Docker
- Interfaz de la línea de comandos de AWS (AWS CLI)
- Interfaz de la línea de comandos de AWS Copilot

Código

El código de la aplicación de muestra utilizada en este patrón está disponible en el repositorio GitHub de aplicaciones de muestra en clúster. Siga las instrucciones de la siguiente sección para utilizar los archivos de muestra.

Epics

Implementar la pila de aplicaciones: opción 1 (Consola de administración de AWS)

Tarea	Descripción	Habilidades requeridas
Clona el GitHub repositorio.	Clone el repositorio de código de muestra mediante el comando: `git clone https://github.com/aws-samples/cluster-sample-app cluster-sample-app && cd cluster-sample-app`	Desarrollador de aplicaciones, AWS DevOps
Crear su repositorio de Amazon ECR.	1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon ECR en https://	Desarrollador de aplicaciones, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	console.aws.amazon.com/ecr/repositories. 2. Elija Create repository. 3. Para el nombre del repositorio, introduzca cluster-sample-app. 4. Mantenga los valores predeterminados para el resto de ajustes. 5. Elija Create repository. Para obtener más información, consulte Creación de un repositorio privado en la documentación de Amazon ECR.	

Tarea	Descripción	Habilidades requeridas
Crear, etiquetar y enviar una imagen de Docker a su repositorio de Amazon ECR.	1. Seleccione el repositorio que acaba de crear y seleccione Ver comandos push. 2. Copie los comandos que se muestran y ejecútelos localmente para crear, etiquetar y enviar su imagen de Docker. Estos comandos serán similares a lo siguiente. Para autenticar su cliente de Docker en el registro: `aws ecr get-login -password --region <YOUR_AWS_REGION> | docker login --username AWS --password-stdin <YOUR_AWS_ACCOUNT>.dkr.ecr.<YOUR_AWS_REGION>.amazonaws.com` Para compilar su imagen de Docker: `docker build -t cluster-sample-app .` Para etiquetar su imagen de Docker: `docker tag cluster-sample-app:latest`	Desarrollador de aplicaciones, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	<YOUR_AWS_ACCOUNT> .dkr.ecr.<YOUR_AWS _REGION>.amazonaws .com/cluster-sample- app:latest Para enviar su imagen de Docker a su repositorio: docker push <YOUR_AWS _ACCOUNT>.dkr.ecr. <YOUR_AWS_REGION>. amazonaws.com/clus ter-sample-app:latest	

Tarea	Descripción	Habilidades requeridas
Implementar la pila de aplicaciones.	1. Abra la CloudFormation consola de AWS en https://console.aws.amazon.com/cloudformation/. 2. Seleccione Crear pila. 3. En la sección Preparación de la plantilla, seleccione La plantilla está lista. 4. En la sección Especificar plantilla, elija Cargar un archivo de plantilla. 5. Elija el archivo local `cluster-sample-app-stack.yml` que ha clonado del GitHub repositorio como CloudFormation plantilla y, a continuación, elija Siguiente. 6. Escriba un nombre para la pila y después elija Next (Siguiente). 7. Mantenga todas las opciones predeterminadas y, a continuación, seleccione Siguiente. 8. Revise todas las opciones, confirme la creación de los recursos de IAM y, a continuación, seleccione Crear pila. 9. Cuando la pila de aplicaciones se haya implement	AWS DevOps, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	ado, seleccione la pestaña Salida, copie la URL y ábrala en su navegador para acceder a la aplicació n. Para obtener más informaci ón sobre la implementación de CloudFormation plantillas, consulte Crear una pila en la CloudFormation documenta ción de AWS.	

Implementar la pila de aplicaciones: opción 2 (CLI de AWS Copilot)

Tarea	Descripción	Habilidades requeridas
Clona el GitHub repositorio.	Clone el repositorio de código de muestra mediante el comando: `git clone https://g ithub.com/aws-samp les/cluster-sample- app cluster-sample-app && cd cluster-sample- app`	Desarrollador de aplicaciones, AWS DevOps
Implementar la imagen de contenedor en AWS mediante la CLI de AWS Copilot.	Implemente la aplicación en un solo paso mediante el siguiente comando en el directorio raíz de su proyecto: `copilot init --app cluster-sample-app --`	Desarrollador de aplicaciones, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`name demo --type "Load Balanced Web Service" --dockerfile ./Dockerfile --port 8080 --deploy` A continuación, debería poder acceder a la aplicación mediante el nombre de DNS obtenido como resultado.	

Eliminar los recursos creados

Tarea	Descripción	Habilidades requeridas
Eliminar los recursos creados a través de la consola de administración de AWS.	Si utilizó la opción 1 (la consola de administración de AWS) para implementar la pila de aplicaciones, siga estos pasos cuando esté listo para eliminar los recursos que creó: 1. Abra la CloudFormation consola en https://console.aws.amazon.com/cloudformation/. 2. Seleccione la pila que creó y, a continuación, seleccione Eliminar. 3. Abra la consola de Amazon ECR en https://console.aws.amazon.com/ecr/repositories.	Desarrollador de aplicaciones, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	4. Seleccione el repositorio que creó y, a continuación, seleccione Eliminar.	
Eliminar los recursos creados por AWS Copilot.	Si utilizó la opción 2 (la CLI de AWS Copilot) para implement ar la pila de aplicaciones, ejecute el siguiente comando desde el directorio raíz de su proyecto cuando esté listo para eliminar los recursos que creó: `copilot app delete`	Desarrollador de aplicaciones, AWS DevOps

Recursos relacionados

- Instalación o actualización de la versión más reciente de la CLI de AWS (documentación de la CLI de AWS)
- Uso de la interfaz de la línea de comandos de AWS Copilot (documentación de Amazon ECS)
- Amazon ECS en AWS Fargate (documentación de Amazon ECR)
- Documentación de Amazon ECS
- Documentación de ECR
- CloudFormation Documentación de Amazon
- Docker Desktop (documentación de Docker)

Implemente una aplicación basada en gRPC en un clúster de Amazon EKS y acceda a ella con un Equilibrador de carga de aplicación

Creado por Kirankumar Chandrashekar (AWS) y Huy Nguyen (AWS)

grpc-traffic-on-albRepositorio de código: -to-eks	Entorno: PoC o piloto	Tecnologías: contenedores y microservicios; entrega de contenido; aplicaciones web y móviles
Carga de trabajo: todas las demás cargas de trabajo	Servicios de AWS: Amazon EKS; Elastic Load Balancing (ELB)	

Resumen

Este patrón describe cómo alojar una aplicación basada en gRPC en un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) y cómo acceder a ella de forma segura a través de un Equilibrador de carga de aplicación.

gRPC es un marco de llamada a procedimientos remotos (RPC) de código abierto que se puede ejecutar en cualquier entorno. Puede usarlo para integraciones de microservicios y comunicaciones cliente-servidor. Para obtener más información sobre el gRPC, consulte la entrada del blog de AWS sobre el soporte del Application Load Balancer para end-to-end HTTP/2 y gRPC.

Este patrón muestra cómo alojar una aplicación basada en gRPC que se ejecute en pods de Kubernetes en Amazon EKS. El cliente gRPC se conecta a un Application Load Balancer a través del protocolo HTTP/2 con una conexión cifrada SSL/TLS. El Equilibrador de carga de aplicación reenvía el tráfico a la aplicación gRPC que se ejecuta en los pods de Amazon EKS. La cantidad de pods de gRPC se puede escalar automáticamente en función del tráfico mediante el escalador automático de pods horizontales de Kubernetes. El grupo objetivo del balanceador de carga de aplicaciones realiza comprobaciones de estado en los nodos de Amazon EKS, evalúa si el objetivo está en buen estado y reenvía el tráfico solo a los nodos en buen estado.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Docker, instalado y configurado en Linux, macOS o Windows.
- Interfaz de la línea de comandos de AWS (AWS CLI) versión 2, instalada y configurada en Linux, macOS o Windows.
- eksctl, instalado y configurado en Linux, macOS o Windows.
- `kubectl`, instalado y configurado para acceder a los recursos de su clúster de Amazon EKS. Para obtener más información, consulte Instalación o actualización de kubectl en la documentación de Amazon EKS.
- gRPCurl, instalado y configurado.
- Un clúster de Amazon EKS nuevo o existente. Para obtener más información, consulte Introducción a Amazon EKS.
- El terminal de su ordenador está configurado para acceder al clúster Amazon EKS. Para obtener más información, consulte Configurar el equipo para que se comunique con el clúster en la documentación de Amazon EKS.
- Controlador del equilibrador de carga de AWS, aprovisionado en el clúster de Amazon EKS.
- Un nombre de host DNS existente con un certificado SSL o SSL/TLS válido. Puede obtener un certificado para su dominio mediante AWS Certificate Manager (ACM) o cargando un certificado existente en ACM. Para obtener más información sobre estas dos opciones, consulte Solicitud de un certificado público e Importación de certificados a AWS Certificate Manager en la documentación de ACM.

Arquitectura

El siguiente diagrama muestra la arquitectura implementada por este patrón.

El siguiente diagrama muestra un flujo de trabajo en el que el tráfico SSL/TLS se recibe de un cliente gRPC que se descarga a un Equilibrador de carga de aplicación. El tráfico se reenvía en texto sin formato al servidor gPC porque proviene de una nube privada virtual (VPC).

Herramientas

Servicios de AWS

- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que permite interactuar con los servicios de AWS mediante comandos en el intérprete de comandos de línea de comandos.
- Elastic Load Balancing permite distribuir el tráfico entrante de las aplicaciones o de la red entre varios destinos. Así, por ejemplo, puede distribuir el tráfico a través de instancias de Amazon Elastic Compute Cloud (Amazon EC2), contenedores y direcciones IP de una o varias zonas de disponibilidad.
- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable.
- Amazon Elastic Kubernetes Service (Amazon EKS) le ayuda a ejecutar Kubernetes en AWS sin necesidad de instalar ni mantener su propio plano de control o nodos de Kubernetes.

Herramientas

- eksctl es una sencilla herramienta CLI para crear clústeres en Amazon EKS.
- kubectl: es una utilidad de línea de comandos para la ejecución de comandos en clústeres de Kubernetes.
- El controlador del equilibrador de carga de AWS le ayuda a administrar los Elastic Load Balancer de AWS para un clúster de Kubernetes.
- gRPCurl es una herramienta de línea de comandos que le ayuda a interactuar con los servicios de gRPC.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub grpc-traffic-on-alb-to-eks.

Epics

Cree y envíe la imagen de Docker del servidor gRPC a Amazon ECR

Tarea	Descripción	Habilidades requeridas
Cree un repositorio de Amazon ECR.	Inicie sesión en la consola de administración de AWS, abra la consola Amazon ECR y, a continuación, cree un repositorio de Amazon ECR. Para obtener más información, consulte Creación de un repositorio en la documentación de Amazon ECR. Asegúrese de registrar la URL del repositorio de Amazon ECR. También puede crear un repositorio de Amazon ECR con la CLI de AWS ejecutando el siguiente comando: `aws ecr create-repository --repository-name helloworld-grpc`	Administrador de la nube
Cree la imagen de Docker.	1. Clona el repositorio GitHub grpc-traffic-on-alb-to-eks. `git clone https://github.com/aws-samples/grpc-traffic-on-alb-to-eks.git` 2. Desde el directorio raíz del repositorio, asegúrese de	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	que el Dockerfile existe y, a continuación, ejecute el siguiente comando para crear la imagen de Docker: `docker build -t <amazon_ecr_repository_url>:<Tag> .` Importante: Asegúrese de `<amazon_ecr_repository_url>` reemplazarla por la URL del repositorio de Amazon ECR que creó anteriormente.	

Tarea	Descripción	Habilidades requeridas
Envíe la imagen de Docker a Amazon ECR.	1. Ejecute el siguiente comando para iniciar sesión en el repositorio de Amazon ECR: `aws ecr get-login -password --region us-east-1 --no-cli-auto-prompt | docker login --username AWS --password-stdin <your_aws_account_id>.dkr.ecr.us-east-1.amazonaws.com` 2. Envíe la imagen de Docker en el repositorio de Amazon ECR ejecutando el siguiente comando: `docker push <your_aws_account_id>.dkr.ecr.us-east-1.amazonaws.com/helloworld-grpc:1.0` Importante: asegúrese de sustituir `<your_aws_account_id>` por el ID de su cuenta de AWS.	DevOps ingeniero

Implemente los manifiestos de Kubernetes en el clúster de Amazon EKS

Tarea	Descripción	Habilidades requeridas
Modifique los valores del archivo de manifiesto de Kubernetes.	1. Modifique el archivo de manifiesto de `grpc-sample.yaml` Kubernetes en la carpeta de Kubernetes del repositorio según sus necesidades. Debe modificar las anotaciones y el nombre de host en el recurso de entrada. Para ver un ejemplo de recurso de entrada, consulte la sección Información adicional. Para obtener más información sobre anotaciones de entrada, consulte Anotaciones de ingreso en la documentación de Kubernetes. 2. En el recurso de implementación de Kubernetes, cambie el `image` de los recursos de despliegue por el identificador uniforme de recursos (URI) del repositorio de Amazon ECR al que insertó la imagen de Docker. Para ver un ejemplo de recurso de implementación, consulte la sección Información adicional.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Implemente el archivo de manifiesto de Kubernetes.	Implemente el `grpc-sample.yaml` archivo en el clúster de Amazon EKS ejecutando el siguiente `kubectl` comando: `kubectl apply -f ./kubernetes/grpc-sample.yaml`	DevOps ingeniero

Cree el registro de DNS para el FQDN del Equilibrador de carga de aplicación

Tarea	Descripción	Habilidades requeridas
Registre el FQDN para el Equilibrador de carga de aplicación.	1. Ejecute el siguiente comando `kubectl` para describir el recurso de entrada de Kubernetes que administra el Equilibrador de carga de aplicación: `kubectl get ingress -n grpcserver` Los resultados de muestra se proporcionan en la sección de información adicional. En el resultado , el campo `HOSTS` muestra el nombre de host DNS para el que se crearon los certificados SSL. 2. Registre el nombre de dominio completo (FQDN)	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	del balanceador de carga de aplicaciones en el `Address` campo de salida. 3. Cree un registro DNS que apunte al FQDN del balanceador de carga de aplicaciones. Si su proveedor de DNS es Amazon Route 53, puede crear un registro de alias que apunte al FQDN del Equilibrador de carga de aplicación. Para obtener más información sobre esta opción, consulte Elegir entre registros con alias y sin alias en la documentación de Route 53.	

Pruebe la solución

Tarea	Descripción	Habilidades requeridas
Pruebe el servidor gRPC.	Utilice gRPCurl para probar el punto de conexión al ejecutar el siguiente comando: `grpcurl grpc.example.com:443 list grpc.reflection.v1alpha.ServerReflection helloworld.helloworld`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Nota: Sustituya `grpc.example.com` por su nombre de DNS.	
Pruebe el servidor gRPC con un cliente gRPC.	En el cliente gRPC de `helloworld_client_ssl.py` ejemplo, sustituya el nombre de host de por el nombre de `grpc.example.com` host utilizado para el servidor gRPC. El siguiente ejemplo de código muestra la respuesta del servidor gRPC a la solicitud del cliente: `python ./app/helloworld_client_ssl.py` `message: "Hello to gRPC server from Client"` `message: "Thanks for talking to gRPC server!! Welcome to hello world. Received message is \"Hello to gRPC server from Client\""` `received: true` Esto demuestra que el cliente puede hablar con el servidor y que la conexión se ha realizado correctamente.	DevOps ingeniero

Limpieza

Tarea	Descripción	Habilidades requeridas
Elimine el registro DNS.	Elimine el registro DNS que apunta al FQDN del balanceador de carga de aplicaciones que creó anteriormente.	Administrador de la nube
Quite el balanceador de cargas.	En la consola Amazon EC2, elija Load Balancers y, a continuación, elimine el balanceador de carga que el controlador de Kubernetes creó para su recurso de entrada.	Administrador de la nube
Elimine el clúster de Amazon EKS.	Elimine el clúster de Amazon EKS mediante `eksctl`: `eksctl delete cluster -f ./eks.yaml`	AWS DevOps

Recursos relacionados

- Equilibrio de carga de red en Amazon EKS
- Grupos de destino para los Equilibradores de carga de aplicación

Información adicional

Ejemplo de recurso de ingreso:

```
---
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
```

```
  annotations:
    alb.ingress.kubernetes.io/healthcheck-protocol: HTTP
    alb.ingress.kubernetes.io/ssl-redirect: "443"
    alb.ingress.kubernetes.io/backend-protocol-version: "GRPC"
    alb.ingress.kubernetes.io/listen-ports: '[{"HTTP": 80}, {"HTTPS":443}]'
    alb.ingress.kubernetes.io/scheme: internet-facing
    alb.ingress.kubernetes.io/target-type: ip
    alb.ingress.kubernetes.io/certificate-arn: arn:aws:acm:<AWS-
Region>:<AccountId>:certificate/<certificate_ID>
    alb.ingress.kubernetes.io/healthcheck-protocol: HTTP
  labels:
    app: grpcserver
    environment: dev
  name: grpcserver
  namespace: grpcserver
spec:
  ingressClassName: alb
  rules:
  - host: grpc.example.com # <----- replace this as per your host name for which the
 SSL certtficate is available in ACM
    http:
      paths:
      - backend:
          service:
            name: grpcserver
            port:
              number: 9000
        path: /
        pathType: Prefix
```

Ejemplo de recurso de implementación:

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: grpcserver
  namespace: grpcserver
spec:
  selector:
    matchLabels:
      app: grpcserver
  replicas: 1
  template:
```

```
    metadata:
      labels:
        app: grpcserver
    spec:
      containers:
      - name: grpc-demo
        image: <your_aws_account_id>.dkr.ecr.us-east-1.amazonaws.com/helloworld-
grpc:1.0   #<------- Change to the URI that the Docker image is pushed to
        imagePullPolicy: Always
        ports:
        - name: grpc-api
          containerPort: 9000
        env:
        - name: POD_IP
          valueFrom:
            fieldRef:
              fieldPath: status.podIP
      restartPolicy: Always
```

Resultado de ejemplo:

```
NAME             CLASS           HOSTS                          Address
 PORTS          AGE
 grpcserver      <none>      <DNS-HostName>                 <ELB-address>
 80            27d
```

Implementar y depurar clústeres de Amazon EKS

Creado por Svenja Raether (AWS) y Mathew George (AWS)

Entorno: PoC o piloto	Tecnologías: Contenedores y microservicios; infraestructura; modernización; sin servidor; nativo en la nube	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon EKS; AWS Fargate		

Resumen

Los contenedores se están convirtiendo en una parte esencial del desarrollo de aplicaciones nativas en la nube. Kubernetes proporciona una forma eficiente de administrar y orquestar contenedores. Amazon Elastic Kubernetes Service (Amazon EKS) es un servicio completamente administrado y certificado que cumple con Kubernetes para crear, proteger, operar y mantener clústeres de Kubernetes en Amazon Web Services (AWS). Es compatible con la ejecución de pods en AWS Fargate para proporcionar capacidad informática bajo demanda correctamente dimensionada.

Es importante que los desarrolladores y administradores conozcan las opciones de depuración al ejecutar cargas de trabajo en contenedores. Este patrón lo guía a través de la implementación y la depuración de contenedores en Amazon EKS con AWS Fargate. Incluye la creación, la implementación, el acceso, la depuración y la limpieza de las cargas de trabajo de Amazon EKS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Rol de AWS Identity and Access Management (IAM) configurado con permisos suficientes para crear e interactuar con roles de Amazon EKS, roles de IAM y roles vinculados a servicios
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada en su máquina local
- eksctl

- kubectl
- Helm

Limitaciones

- Este patrón proporciona a los desarrolladores prácticas de depuración útiles para los entornos de desarrollo. No establece las prácticas recomendadas para los entornos de producción.
- Si ejecuta Windows, utilice los comandos específicos del sistema operativo para configurar las variables de entorno.

Versiones de producto utilizadas

- CLI de AWS versión 2
- La versión de kubectl dentro de una versión menor diferente al plano de control de Amazon EKS que está utilizando
- eksctl última versión
- Helm v3

Arquitectura

Pila de tecnología

- Equilibrador de carga de aplicación
- Amazon EKS
- AWS Fargate

Arquitectura de destino

Todos los recursos que se muestran en el diagrama los aprovisionan los comandos `eksctl` y `kubectl` emitidos desde una máquina local. Los clústeres privados deben ejecutarse desde una instancia que está dentro de la VPC privada.

La arquitectura de destino consiste en un clúster EKS que utiliza el tipo de lanzamiento de Fargate. Esto proporciona capacidad informática bajo demanda correctamente dimensionada sin necesidad de especificar tipos de servidor. El clúster EKS tiene un plano de control que se utiliza para gestionar

los nodos y las cargas de trabajo del clúster. Los pods se aprovisionan en subredes de VPC privadas que abarcan varias zonas de disponibilidad. Se hace referencia a la galería pública de Amazon ECR para recuperar e implementar una imagen del servidor web NGINX en los pods del clúster.

El diagrama muestra cómo acceder al plano de control de Amazon EKS mediante comandos `kubectl` y cómo acceder a la aplicación mediante el equilibrador de carga de aplicación.

.

1. Una máquina local fuera de la nube de AWS envía comandos al plano de control de Kubernetes dentro de una VPC administrada por Amazon EKS.
2. Amazon EKS programa los pods en función de los selectores del perfil de Fargate.
3. La máquina local abre la URL de equilibrador de carga de aplicación en el navegador.
4. El equilibrador de carga de aplicación divide el tráfico entre los pods de Kubernetes en los nodos del clúster de Fargate implementados en subredes privadas que abarcan varias zonas de disponibilidad.

Herramientas

Servicios de AWS

- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable.
- Amazon Elastic Kubernetes Service (Amazon EKS) le ayuda a ejecutar Kubernetes en AWS sin necesidad de instalar ni mantener su propio plano de control o nodos de Kubernetes. Este patrón también utiliza la herramienta de línea de comandos eksctl para trabajar con los clústeres de Kubernetes en Amazon EKS.
- AWS Fargate le permite ejecutar contenedores sin necesidad de administrar servidores o instancias de Amazon Elastic Compute Cloud (Amazon EC2). Se utiliza en conjunto con Amazon Elastic Container Service (Amazon ECS).
- Elastic Load Balancing (ELB) distribuye el tráfico entrante de aplicaciones o redes entre varios destinos. Así, por ejemplo, puede distribuir el tráfico a través de instancias de Amazon Elastic Compute Cloud (Amazon EC2), contenedores y direcciones IP de una o varias zonas de disponibilidad. Este patrón usa el componente de control del Controlador del equilibrador de carga de AWS para crear el equilibrador de carga de aplicación cuando se aprovisiona una entrada

de Kubernetes. El equilibrador de carga de aplicación distribuye el tráfico entrante entre varios destinos.

Otras herramientas

- Helm es un administrador de paquetes de código abierto para Kubernetes. En este patrón, Helm se utiliza para instalar el controlador del equilibrador de carga de AWS.
- Kubernetes es un sistema de código abierto para automatizar la implementación, escalado y administración de las aplicaciones en contenedores.
- NGINX es un servidor proxy inverso y web de alto rendimiento.

Epics

Crear un clúster de EKS

Tarea	Descripción	Habilidades requeridas
Cree los archivos.	Con el código de la sección de Información adicional, cree los siguientes archivos: • `clusterconfig-fargate.yaml` • `nginx-deployment.yaml` • `nginx-service.yaml` • `nginx-ingress.yaml` • `index.html`	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps
Configure las variables de entorno.	Nota: Si se produce un error en un comando debido a tareas pendientes anteriores, espere unos segundos y vuelva a ejecutar el comando.	Desarrollador de aplicaciones, AWS DevOps, administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	Este patrón utiliza la región de AWS y el nombre del clúster que se definen en el archivo `clusterconfig-fargate.yaml` . Establezca los mismos valores que las variables de entorno para hacer referencia a ellos en otros comandos. `export AWS_REGION="us-east-1"` `export CLUSTER_NAME="my-fargate"`	

Tarea	Descripción	Habilidades requeridas
Crear un clúster de EKS.	Para crear un clúster de EKS que utilice las especificaciones del archivo `clusterconfig-fargate.yaml` , ejecute el siguiente comando. `eksctl create cluster -f clusterconfig-fargate.yaml` El archivo contiene el `ClusterConfig` , que proporciona un nuevo clúster de EKS denominado `my-fargate-cluster` en la región `us-east-1` y un perfil de Fargate predeterminado (`fp-default`). El perfil Fargate predeterminado está configurado con dos selectores (`default` y `kube-system`).	Desarrollador de aplicaciones, AWS DevOps, administrador de AWS

Tarea	Descripción	Habilidades requeridas
Compruebe el clúster creado.	Ejecute el siguiente comando para comprobar el clúster creado. `eksctl get cluster --output yaml` La salida debería ser la siguiente. `- Name: my-fargate` `  Owned: "True"` `  Region: us-east-1` Compruebe el perfil de Fargate creado utilizando el `CLUSTER_NAME` . `eksctl get fargatepr ofile --cluster  $CLUSTER_NAME --output  yaml` Este comando muestra información sobre los recursos. Puede usar la información para verificar el clúster creado. La salida debería ser la siguiente. `- name: fp-default` `  podExecutionRoleAR N: arn:aws:iam::<YOUR -ACCOUNT-ID>:role/ eksctl-my-fargate- cluster-FargatePod ExecutionRole-xxx`	Desarrollador de aplicaciones, AWS DevOps, administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	<pre> selectors: - namespace: default - namespace: kube-system status: ACTIVE subnets: - subnet-aaa - subnet-bbb - subnet-ccc</pre>	

Implementar un contenedor

Tarea	Descripción	Habilidades requeridas
Implementar el servidor web NGINX.	Para aplicar la implementación del servidor web de NGINX en el clúster, ejecute el siguiente comando. <pre>kubectl apply -f ./nginx-deployment.yaml</pre> La salida debería ser la siguiente. <pre>deployment.apps/nginx-deployment created</pre> La implementación incluye tres réplicas de la imagen de NGINX tomada de la galería pública de Amazon ECR. La imagen se implementa en el espacio de nombres predeterminado y se expone	Desarrollador de aplicaciones, AWS DevOps, administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	en el puerto 80 de los pods en ejecución.	

Tarea	Descripción	Habilidades requeridas
Compruebe la implementación y los pods.	(Opcional) Compruebe la implementación. Puede verificar el estado de la implementación con el comando siguiente. `kubectl get deployment` La salida debería ser la siguiente. `NAME  READY  UP-TO-DATE  AVAILABLE  AGE nginx-deployment  3/3  3  3  7m14s` Un pod es un objeto implementable en Kubernetes que contiene uno o más contenedores. Para enumerar todos los pods, ejecute el siguiente comando. `kubectl get pods` La salida debería ser la siguiente. `NAME  READY  STATUS  RESTARTS  AGE`	Desarrollador de aplicaciones, AWS DevOps, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	`nginx-deployment-xxxx-aaa 1/1 Running 0 94s` `nginx-deployment-xxxx-bbb 1/1 Running 0 94s` `nginx-deployment-xxxx-ccc 1/1 Running 0 94s`	
Escale la implementación.	Para escalar la implement ación de las tres réplicas especificadas en `deploymen t.yaml` a cuatro réplicas, utilice el siguiente comando. `kubectl scale deploymen t nginx-deployment -- replicas 4` La salida debería ser la siguiente. `deployment.apps/nginx-deployment scaled`	Desarrollador de aplicaciones, AWS DevOps, administrador de sistemas de AWS

Implementar un controlador del equilibrador de carga de AWS

Tarea	Descripción	Habilidades requeridas
Configure las variables de entorno.	Describa la CloudFormation pila del clúster para recuperar información sobre su VPC. `aws cloudformation describe-stacks --`	Desarrollador de aplicaciones, AWS DevOps, administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	`stack-name eksctl-$CLUSTER_NAME-cluster --query "Stacks[0].Outputs[?OutputKey==\`VPC\`].OutputValue"` La salida debería ser la siguiente. `[ "vpc-<YOUR-VPC-ID>" ]` Copie el ID de VPC y expórtelo como una variable de entorno. `export VPC_ID="vpc-<YOUR-VPC-ID>"`	
Configurar el IAM de una cuenta de servicio del clúster.	Utilice `AWS_REGION` y `CLUSTER_NAME` de la épica anterior para crear un proveedor de IAM Open ID Connect para el clúster. `eksctl utils associate-iam-oidc-provider \ --region $AWS_REGION \ --cluster $CLUSTER_NAME \ --approve`	Desarrollador de aplicaciones, AWS DevOps, administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
Descargue y cree la política de IAM.	Descargue una política de IAM para el controlador del equilibrador de carga de AWS que le permita realizar llamadas a las API de AWS en su nombre. `curl -o iam-policy.json https://raw.githubusercontent.com/kubernetes-sigs/aws-load-balancer-controller/main/docs/install/iam_policy.json` Cree la política en su cuenta de AWS mediante la CLI de AWS. `aws iam create-policy \ --policy-name AWSLoadBalancerControllerIAMPolicy \ --policy-document file://iam-policy.json` Debería ver la siguiente salida. `{ "Policy": { "PolicyName": "AWSLoadBalancerControllerIAMPolicy", "PolicyId": "<YOUR_POLICY_ID>",`	Desarrollador de aplicaciones, AWS DevOps, administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	<pre>"Arn": "arn:aws:iam::<YOUR-ACCOUNT-ID>:policy/AWSLoadBalancerControllerIAMPolicy", "Path": "/", "DefaultVersionId": "v1", "AttachmentCount": 0, "PermissionsBoundaryUsageCount": 0, "IsAttachable": true, "CreateDate": "<YOUR-DATE>", "UpdateDate": "<YOUR-DATE>" } }</pre> Guarde el Nombre de recurso de Amazon (ARN) de la política como `$POLICY_ARN` . <pre>export POLICY_ARN=”arn:aws:iam::<YOUR-ACCOUNT-ID>:policy/AWSLoadBalancerControllerIAMPolicy”</pre>	

Tarea	Descripción	Habilidades requeridas
Cree una cuenta de servicio de IAM.	Cree una cuenta de servicio denominada `aws-load-balancer-controller` en el espacio de nombres `kube-system`. Utilice el `CLUSTER_NAME`, `AWS_REGION` y `POLICY_ARN` que configuró previamente. `eksctl create iamserviceaccount \` `--cluster=$CLUSTER_NAME \` `--region=$AWS_REGION \` `--attach-policy-arn=$POLICY_ARN \` `--namespace=kube-system \` `--name=aws-load-balancer-controller \` `--override-existing-serviceaccounts \` `--approve` Verifique la creación. `eksctl get iamserviceaccount \` `--cluster $CLUSTER_NAME \` `--name aws-load-balancer-controller \` `--namespace kube-system \` `--output yaml` La salida debería ser la siguiente.	Desarrollador de aplicaciones, AWS DevOps, administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	`- metadata:` `    name: aws-load-balancer-controller` `    namespace: kube-system` `  status:` `    roleARN: arn:aws:iam::<YOUR-ACCOUNT-ID>:role/eksctl-my-fargate-addon-iam serviceaccount-ku-Role1-<YOUR-ROLE-ID>` `  wellKnownPolicies:` `    autoScaler: false` `    awsLoadBalancerController: false` `    certManager: false` `    ebsCSIController: false` `    efsCSIController: false` `    externalDNS: false` `    imageBuilder: false`	

Tarea	Descripción	Habilidades requeridas
Instalación del complemento controlador del equilibrador de carga de AWS.	Actualizar el repositorio de Helm. `helm repo update` Añada el repositorio de gráficos de Amazon EKS al repositorio de Helm. `helm repo add eks https://aws.github.io/eks-charts` Aplique las definiciones de recursos personalizados (CRD) de Kubernetes que utiliza el Controlador del equilibrador de carga AWS eks-chart en segundo plano. `kubectl apply -k "github.com/aws/eks-charts/stable/aws-load-balancer-controller//crds?ref=master"` La salida debería ser la siguiente. `customresourcedefinition.apiextensions.k8s.io/ingressclassparams.elbv2.k8s.aws created customresourcedefinition.apiextension`	Desarrollador de aplicaciones, AWS DevOps, administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	`s.k8s.io/targetgro upbindings.elbv2.k 8s.aws created` Instale el gráfico de Helm con las variables de entorno que configuró anteriormente. `helm install aws-load- balancer-controlle r eks/aws-load-balan cer-controller \ --set clusterName= $CLUSTER_NAME \ --set serviceAc count.create=false \ --set region=$A WS_REGION \ --set vpcId=$VPC_ID \ --set serviceAc count.name=aws-load- balancer-controller \ -n kube-system` La salida debería ser la siguiente. `NAME: aws-load- balancer-controller LAST DEPLOYED: <YOUR-DAT E> NAMESPACE: kube-system STATUS: deployed REVISION: 1 TEST SUITE: None NOTES: AWS Load Balancer controller installed!`	

Tarea	Descripción	Habilidades requeridas
Crear un servicio NGINX.	Cree un servicio para exponer los pods de NGINX mediante el archivo `nginx-service.yaml` . `kubectl apply -f nginx-service.yaml` La salida debería ser la siguiente. `service/nginx-service created`	Desarrollador de aplicaciones, AWS DevOps, administrador de sistemas de AWS
Cree el recurso de entrada de Kubernetes.	Cree un servicio para exponer los pods de NGINX mediante el archivo `nginx-ingress.yaml` . `kubectl apply -f nginx-ingress.yaml` La salida debería ser la siguiente. `ingress.networking.k8s.io/nginx-ingress created`	Desarrollador de aplicaciones, AWS DevOps, administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
Obtenga la URL del equilibrador de carga.	Para recuperar la información de entrada, utilice el siguiente comando. `kubectl get ingress nginx-ingress` La salida debería ser la siguiente. `NAME CLASS HOSTS ADDRESS PORTS AGE` `nginx-ingress <none> * k8s-default-nginxing-xxx.us-east-1.elb.amazonaws.com 80 80s` Copie la ADDRESS (por ejemplo, `k8s-default-nginxing-xxx.us-east-1.elb.amazonaws.com`) del resultado y péguela en su navegador para acceder al archivo `index.html`.	Desarrollador de aplicaciones, AWS DevOps, administrador de sistemas de AWS

Depurar contenedores en ejecución

Tarea	Descripción	Habilidades requeridas
Seleccione un pod.	Enumere todos los pods y copie el nombre del pod deseado. `kubectl get pods` La salida debería ser la siguiente. `NAME READY STATUS RESTARTS AGE` `nginx-deployment-xxxx-aaa 1/1 Running 0 55m` `nginx-deployment-xxxx-bbb 1/1 Running 0 55m` `nginx-deployment-xxxx-ccc 1/1 Running 0 55m` `nginx-deployment-xxxx-ddd 1/1 Running 0 42m` Este comando muestra los pods existentes e información adicional. Si está interesado en un pod específico, introduzc	Desarrollador de aplicaciones, AWS DevOps, administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	a el nombre del pod que le interese para la variable `POD_NAME` o configúrelo como una variable de entorno. De lo contrario, omita este parámetro para buscar todos los recursos. `export POD_NAME="nginx-deployment-<YOUR-POD-NAME>"`	
Acceder a los registros.	Obtenga los registros del pod que desee depurar. `kubectl logs $POD_NAME`	Desarrollador de aplicaciones, administrador de sistemas de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
Reenvíe el puerto NGINX.	Utilice el reenvío de puertos para asignar el puerto del pod para acceder al servidor web NGINX a un puerto de su máquina local. `kubectl port-forward deployment/nginx-deployment 8080:80` En su navegador, abra la siguiente URL. `http://localhost:8080` El comando `port-forward` proporciona acceso al archivo `index.html` sin ponerlo a disposición del público a través de un equilibrador de carga. Esto resulta útil para acceder a la aplicación en ejecución mientras la depura. Puede detener el reenvío de puertos pulsando el comando del teclado Ctrl+C.	Desarrollador de aplicaciones, AWS DevOps, administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
Ejecute comandos dentro del pod.	Para ver el archivo `index.html` actual, utilice el siguiente comando. `kubectl exec $POD_NAME -- cat /usr/share/nginx/html/index.html` Puede usar el comando `exec` para ejecutar cualquier comando directamente en el pod. Esto resulta útil para depurar las aplicaciones en ejecución.	Desarrollador de aplicaciones, AWS DevOps, administrador de sistemas de AWS
Copie los archivos a un pod.	Elimine el archivo `index.html` predeterminado de este pod. `kubectl exec $POD_NAME -- rm /usr/share/nginx/html/index.html` Cargue el archivo `index.html` local personalizado en el pod. `kubectl cp index.html $POD_NAME:/usr/share/nginx/html/` Puede usar el comando `cp` para cambiar o añadir archivos directamente a cualquiera de los pods.	Desarrollador de aplicaciones, AWS DevOps, administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
Utilice el reenvío de puertos para mostrar el cambio.	Utilice el reenvío de puertos para verificar los cambios que realizó en este pod. `kubectl port-forward pod/$POD_NAME 8080:80` Abra la siguiente URL en su navegador. `http://localhost:8080` Los cambios aplicados al archivo `index.html` deberían estar visibles en el navegador.	Desarrollador de aplicaciones, AWS DevOps, administrador de sistemas de AWS

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Eliminar el equilibrador de carga.	Elimine la entrada. `kubectl delete ingress/nginx-ingress` La salida debería ser la siguiente. `ingress.networking.k8s.io "nginx-ingress" deleted` Elimine el servicio.	Desarrollador de aplicaciones, AWS DevOps, administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	`kubectl delete service/nginx-service` La salida debería ser la siguiente. `service "nginx-service" deleted` Elimine el controlador del equilibrador de carga. `helm delete aws-load-balancer-controller -n kube-system` La salida debería ser la siguiente. `release "aws-load-balancer-controller" uninstalled` Elimine la cuenta de servicio. `eksctl delete iamserviceaccount --cluster $CLUSTER_NAME --namespace kube-system --name aws-load-balancer-controller`	

Tarea	Descripción	Habilidades requeridas
Eliminar la implementación.	Use el siguiente comando para eliminar los recursos de implementación. `kubectl delete deploy/nginx-deployment` La salida debería ser la siguiente. `deployment.apps "nginx-deployment" deleted`	Desarrollador de aplicaciones, AWS DevOps, administrador de sistemas de AWS
Eliminar el clúster.	Elimine el clúster de EKS mediante el siguiente comando, donde `my-fargate` es el nombre del clúster. `eksctl delete cluster --name $CLUSTER_NAME` Este comando elimina todo el clúster, incluidos todos los recursos asociados.	Desarrollador de aplicaciones, AWS DevOps, administrador de sistemas de AWS
Eliminar la política de IAM.	Elimine la política creada anteriormente mediante la CLI de AWS. `aws iam delete-policy --policy-arn $POLICY_ARN`	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps

Solución de problemas

Problema	Solución
Recibe un mensaje de error al crear un clúster, indicando que la zona de disponibilidad de destino no tiene capacidad suficiente para admitir el clúster. Debería ver un mensaje similar al siguiente. `Cannot create cluster 'my-fargate' because us-east-1e, the targeted availability zone, does not currently have sufficient capacity to support the cluster. Retry and choose from these availability zones: us-east-1a, us-east-1b, us-east-1c, us-east-1d, us-east-1f`	Vuelva a crear el clúster con las zonas de disponibilidad recomendadas en el mensaje de error. Especifique una lista de zonas de disponibilidad en la última línea de su archivo `clusterconfig-fargate.yaml` (por ejemplo, `availabilityZones: ["us-east-1a", "us-east-1b", "us-east-1c"]`).

Recursos relacionados

- Documentación de Amazon EKS
- Equilibrador de carga de aplicaciones en Amazon EKS
- Guías de prácticas recomendadas de EKS
- Documentación del controlador del equilibrador de carga de AWS
- Documentación de eksctl
- Imagen de NGINX de la Galería pública de Amazon ECR
- Documentación de Helm
- Depurar pods en ejecución (documentación de Kubernetes)
- Taller de Amazon EKS
- Errores de creación del clúster de EKS

Información adicional

clusterconfig-fargate.yaml

```
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
  name: my-fargate
  region: us-east-1

fargateProfiles:
  - name: fp-default
    selectors:
      - namespace: default
      - namespace: kube-system
```

nginx-deployment.yaml

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: "nginx-deployment"
  namespace: "default"
spec:
  replicas: 3
  selector:
    matchLabels:
      app: "nginx"
  template:
    metadata:
      labels:
        app: "nginx"
    spec:
      containers:
      - name: nginx
        image: public.ecr.aws/nginx/nginx:latest
        ports:
        - containerPort: 80
```

nginx-service.yaml

```
apiVersion: v1
kind: Service
metadata:
  annotations:
    alb.ingress.kubernetes.io/target-type: ip
  name: "nginx-service"
  namespace: "default"
spec:
  ports:
  - port: 80
    targetPort: 80
    protocol: TCP
  type: NodePort
  selector:
    app: "nginx"
```

nginx-ingress.yaml

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  namespace: "default"
  name:  "nginx-ingress"
  annotations:
    kubernetes.io/ingress.class: alb
    alb.ingress.kubernetes.io/scheme: internet-facing
spec:
  rules:
    - http:
        paths:
        - path: /
          pathType: Prefix
          backend:
            service:
              name: "nginx-service"
              port:
                number: 80
```

index.html

```
<!DOCTYPE html>
<html>
```

```
<body>
    <h1>Welcome to your customized nginx!</h1>
    <p>You modified the file on this running pod</p>
</body>

</html>
```

Implementar contenedores mediante Elastic Beanstalk

Creado por Thomas Scott (AWS) y Jean-Baptiste Guillois (AWS)

Repositorio de código: aplicación Cluster Sample	Entorno: producción	Tecnologías: contenedores y microservicios; nativo en la nube; modernización
Servicios de AWS: AWS Elastic Beanstalk		

Resumen

En la nube de Amazon Web Services (AWS), AWS Elastic Beanstalk admite Docker como plataforma disponible, de forma que los contenedores pueden ejecutarse en el entorno creado. Este patrón muestra cómo implementar contenedores mediante el servicio Elastic Beanstalk. La implementación de este patrón utilizará el entorno de servidor web basado en la plataforma Docker.

Para usar Elastic Beanstalk para implementar y escalar aplicaciones y servicios web, debe cargar el código y la implementación se gestiona automáticamente. También se incluyen el aprovisionamiento de capacidad, el equilibrio de carga, el escalado automático y la supervisión del estado de las aplicaciones. Cuando usa Elastic Beanstalk, puede tomar el control total de los recursos de AWS que crea en su nombre. No se aplican cargos adicionales por utilizar Elastic Beanstalk. Solo tiene que pagar por los recursos de AWS que se utilizan para almacenar y ejecutar sus aplicaciones.

Este patrón incluye instrucciones de implementación utilizando la interfaz de la línea de comandos de AWS Elastic Beanstalk (CLI de EB) y la consola de administración de AWS.

Casos de uso

Los casos de uso de Elastic Beanstalk incluyen los siguientes:

- Implementar un entorno prototipo para hacer una demostración de una aplicación frontend. (Este patrón usa un Dockerfile como ejemplo).
- Implemente una API para gestionar las solicitudes de API de un dominio determinado.
- Implemente una solución de orquestación mediante Docker-Compose (`docker-compose.yml` no se utiliza como ejemplo práctico en este patrón).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS
- AWS EB CLI instalada localmente
- Instalación de Docker en un equipo local

Limitaciones

- En el plan gratuito, hay un límite de 100 extracciones de Docker cada 6 horas por dirección IP.

Arquitectura

Pila de tecnología de destino

- Instancias de Amazon Elastic Compute Cloud (Amazon EC2)
- Grupo de seguridad
- Equilibrador de carga de aplicación
- Grupo de escalado automático

Arquitectura de destino

Automatizar y escalar

AWS Elastic Beanstalk puede escalarse automáticamente en función del número de solicitudes realizadas. Entre los recursos que AWS crea para un entorno se incluye un equilibrador de carga de aplicación, un grupo de escalado automático y una o varias instancias de Amazon EC2.

El equilibrador de carga se encuentra delante de las instancias de Amazon EC2, que forman parte de un grupo de escalado automático. Amazon EC2 Auto Scaling inicia automáticamente más instancias de Amazon EC2 para acomodar el aumento de la carga que registra la aplicación. Si la carga de la aplicación se reduce, Amazon EC2 Auto Scaling detiene las instancias, aunque siempre deja en ejecución al menos una.

Activadores de escalado automáticos

El grupo Auto Scaling del entorno de Elastic Beanstalk utiliza CloudWatch dos alarmas de Amazon para iniciar las operaciones de escalado. Los desencadenadores predeterminados adaptan su capacidad cuando el tráfico de la red saliente promedio de cada instancia es superior a 6 MB o inferior a 2 MB durante un periodo de cinco minutos. Para utilizar Amazon EC2 Auto Scaling de forma eficaz, configure desencadenadores adecuados para su aplicación, tipo de instancia y requisitos de servicio. Puede optar por el escala en función de varias estadísticas, como la latencia, E/S de disco, la utilización de la CPU y el recuento de solicitudes. Para obtener más información, consulte Límites de escalado automático.

Herramientas

Servicios de AWS

- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.
- La interfaz de la línea de comandos de AWS EB (CLI de EB) es un cliente de línea de comandos que puede utilizar para crear, configurar y administrar entornos de Elastic Beanstalk.
- Elastic Load Balancing permite distribuir el tráfico entrante de las aplicaciones o de la red entre varios destinos. Así, por ejemplo, puede distribuir el tráfico a través de instancias de Amazon Elastic Compute Cloud (Amazon EC2), contenedores y direcciones IP de una o varias zonas de disponibilidad.

Otros servicios

- Docker agrupa el software en unidades estandarizadas denominadas contenedores que incluyen bibliotecas, herramientas del sistema, código y tiempo de ejecución.

Código

El código de este patrón está disponible en el repositorio de aplicaciones de muestra de GitHub clúster.

Epics

Creación con un Dockerfile

Tarea	Descripción	Habilidades requeridas
Clone el repositorio remoto.	• Para clonar el repositorio, ejecute el comando `git clone https://github.com/aws-samples/cluster-sample-app.git . < /p>`	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps
Inicialice el proyecto Docker de Elastic Beanstalk.	1. Cree un archivo llamado `aws.json` en la raíz. 2. Añada el siguiente código al archivo `aws.json`: `{ "AWSEBDockerrunVersion":"1", "Image":{ "Name":"cluster-sample-app" }, "Ports":[ { "ContainerPort":80 , "HostPort":8080 } ] }` 3. Ejecute el comando `eb init -p docker` en la raíz del proyecto.	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
Ejecute el proyecto localmente.	1. Ejecute el comando `eb local run` en la raíz del proyecto. 2. Pruebe la aplicación navegando hasta `http://localhost` .	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps

Implemente utilizando la CLI de EB

Tarea	Descripción	Habilidades requeridas
Ejecute el comando de implementación	1. Ejecute el comando `eb create docker-sample-cluster-app` en la raíz del proyecto.	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps
Acceda a la versión implementada.	Una vez finalizado el comando de implementación, acceda al proyecto mediante el comando `eb open`.	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps

Implementación con la consola

Tarea	Descripción	Habilidades requeridas
Implemente la aplicación mediante el navegador.	1. Abra la consola de . 2. Vuelva a la consola de Elastic Beanstalk. 3. Elija Create application (Crear aplicación). 4. Para el Application Name (Nombre de la aplicación),	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	introduzca Cluster-Sample-App. 5. Elija Docker como plataforma. 6. Seleccione Upload your code (Sube código). 7. Elija su archivo .zip local (en la raíz del proyecto clonado) o una URL pública de Amazon Simple Storage Service (Amazon S3).	
Acceda a la versión implementada.	Tras la implementación, acceda a la aplicación implementada y elija la URL proporcionada.	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps

Recursos relacionados

- Entornos del servidor web
- Instalación de la CLI de EB en macOS
- Instalación manual de la CLI de EB

Información adicional

Ventajas de utilizar Elastic Beanstalk

- Aprovisionamiento automático de infraestructura
- Administración automática de la plataforma subyacente
- Parches y actualizaciones automáticos para dar soporte a la aplicación
- Escalado automático de la aplicación
- Posibilidad de personalizar el número de nodos
- Posibilidad de acceder a los componentes de la infraestructura si es necesario

- Facilidad de implementación en comparación con otras soluciones de implementación de contenedores

Genere una dirección IP saliente estática mediante una función de Lambda, Amazon VPC y una arquitectura sin servidor

Creado por Thomas Scott (AWS)

Entorno: producción	Tecnologías: contenedores y microservicios; desarrollo y pruebas de software	Servicios de AWS: AWS Lambda

Resumen

En este patrón se describe la forma de generar una dirección IP saliente estática en la nube de Amazon Web Services (AWS) mediante una arquitectura sin servidor. Su organización puede beneficiarse de este enfoque si quiere enviar archivos a una entidad empresarial independiente mediante el protocolo seguro File Transfer (SFTP). Esto significa que la entidad empresarial debe tener acceso a una dirección IP que permita que los archivos pasen por su firewall.

El enfoque del patrón le ayuda a crear una función de AWS Lambda que utilice una dirección IP elástica como dirección IP de salida. Si sigue los pasos de este patrón, puede crear una función de Lambda y una nube privada virtual (VPC) que enrute el tráfico saliente a través de una puerta de enlace de Internet con una dirección IP estática. Para usar la dirección IP estática, debe adjuntar la función de Lambda a la VPC y sus subredes.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Permisos de AWS Identity and Access Management (IAM) para crear e implementar una función de Lambda y para crear una VPC y sus subredes. Para obtener más información, consulte Rol de ejecución y permisos de usuario en la documentación de AWS Lambda.
- Si planea usar la infraestructura como código (IaC) para implementar el enfoque de este patrón, necesitará un entorno de desarrollo integrado (IDE) como AWS Cloud9. Para obtener más información, consulte ¿Qué es AWS Cloud9? en la documentación de AWS Cloud9.

Arquitectura

El siguiente diagrama muestra la arquitectura sin servidor para este patrón.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El tráfico saliente deja `NAT gateway 1` en `Public subnet 1`.
2. El tráfico saliente deja `NAT gateway 2` en `Public subnet 2`.
3. La función de Lambda se puede ejecutar en `Private subnet 1` o `Private subnet 2`.
4. `Private subnet 1` y `Private subnet 2` enrutan el tráfico a las puertas de enlace NAT de las subredes públicas.
5. Las puertas de enlace NAT envían tráfico saliente a la puerta de enlace de Internet desde las subredes públicas.
6. Los datos salientes se transfieren desde la puerta de enlace de Internet al servidor externo.

Pila de tecnología

- Lambda
- Amazon Virtual Private Cloud (Amazon VPC)

Automatizar y escalar

Puede garantizar la alta disponibilidad (HA) mediante el uso de dos subredes públicas y dos privadas en distintas zonas de disponibilidad. Incluso si una zona de disponibilidad deja de estar disponible, la solución del patrón sigue funcionando.

Herramientas

- AWS Lambda: AWS Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo. Solo pagará por el tiempo de computación que consuma, no se aplican cargos cuando el código no se está ejecutando.

- Amazon VPC: Amazon Virtual Private Cloud (Amazon VPC) le permite aprovisionar una sección aislada de forma lógica de la nube de AWS donde puede lanzar recursos de AWS en una red virtual que haya definido. Dicha red virtual es prácticamente idéntica a las redes tradicionales que se utilizan en sus propios centros de datos, con los beneficios que supone utilizar la infraestructura escalable de AWS.

Epics

Cree una nueva VPC

Tarea	Descripción	Habilidades requeridas
Cree una nueva VPC.	Inicie sesión en la consola de administración de AWS, abra la consola de Amazon VPC y, a continuación, cree una VPC llamada `Lambda VPC` que tenga `10.0.0.0/25` como rango CIDR IPv4. Para obtener más información, consulte Introducción a Amazon VPC en la documentación de Amazon VPC.	Administrador de AWS

Crear dos subredes públicas

Tarea	Descripción	Habilidades requeridas
Cree la primera subred pública.	1. En la consola de Amazon VPC, elija Subredes y, a continuación, elija Crear subred. 2. En Etiqueta de nombre, ingrese `public-one` . 3. En VPC, elija `Lambda VPC`.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	4. Elija una zona de disponibilidad y regístrela. 5. Para el bloque CIDR de IPv4, introduzca `10.0.0.0/28` y, a continuación, seleccione Create subnet (Crear subred).	
Cree la segunda subred pública.	1. En la consola de Amazon VPC, elija Subredes y, a continuación, elija Crear subred. 2. En Etiqueta de nombre, ingrese `public-two` . 3. En VPC, elija `Lambda VPC`. 4. Elija una zona de disponibilidad y regístrela. Importante: no puede utilizar la zona de disponibilidad que contenga la subred `public-one` . 5. Para el bloque CIDR de IPv4, introduzca `10.0.0.16/28` y, a continuación, seleccione Crear subred.	Administrador de AWS

Crear dos subredes privadas

Tarea	Descripción	Habilidades requeridas
Cree la primera subred privada.	1. En la consola de Amazon VPC, elija Subredes y, a	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	continuación, elija Crear subred. 2. En Etiqueta de nombre, ingrese `private-one` . 3. En VPC, elija `Lambda VPC`. 4. Elija la zona de disponibilidad que contiene la subred `public-one` que creó anteriormente. 5. Para el bloque CIDR de IPv4, introduzca `10.0.0.32/28` y, a continuación, seleccione Create subnet (Crear subred).	
Cree la segunda subred privada.	1. En la consola de Amazon VPC, elija Subredes y, a continuación, elija Crear subred. 2. En Etiqueta de nombre, ingrese `private-two` . 3. En VPC, elija `Lambda VPC`. 4. Elija la misma zona de disponibilidad que contiene la subred `public-two` que creó anteriormente. 5. Para el bloque CIDR de IPv4, introduzca `10.0.0.64/28` y, a continuación, seleccione Create subnet (Crear subred).	Administrador de AWS

Crear dos direcciones IP elásticas para su gateway NAT

Tarea	Descripción	Habilidades requeridas
Cree la primera dirección IP elástica.	1. En la consola de Amazon VPC, elija IP elásticas y, a continuación, elija Asignar nueva dirección. 2. Elija Asignar y registre el ID de asignación de la dirección IP elástica recién creada. Nota: Esta dirección IP elástica se utiliza para su primera puerta de enlace NAT.	Administrador de AWS
Cree la segunda dirección IP elástica.	1. En la consola de Amazon VPC, elija IP elásticas y, a continuación, elija Asignar nueva dirección. 2. Elija Allocate (Asignar) y registre el Allocation ID (ID de asignación) de la dirección IP elástica recién creada. Nota: Esta dirección IP elástica se utiliza para su segunda puerta de enlace NAT.	Administrador de AWS

Cree un puerta de enlace de Internet

Tarea	Descripción	Habilidades requeridas
Cree una puerta de enlace de Internet.	1. En la consola de Amazon VPC, elija Internet Gateways (Puertas de enlace de Internet) y, luego, elija Create internet gateway (Crear puerta de enlace de Internet). 2. Introduzca `Lambda internet gateway` como nombre y, a continuación, seleccione Crear puerta de enlace de Internet. Asegúrese de registrar el ID de la puerta de enlace de Internet.	Administrador de AWS
Adjunte la puerta de enlace de Internet a la VPC.	Seleccione el puerta de enlace de Internet que acaba de crear y, a continuación, elija Actions, Attach to VPC (Acciones, Adjuntar a la VPC).	Administrador de AWS

Cree dos puertas de enlace NAT

Tarea	Descripción	Habilidades requeridas
Cree la primera puerta de enlace NAT.	1. En la consola de Amazon VPC, elija NAT Gateways (Puertas de enlace NAT) y, luego, elija Create NAT Gateway (Crear puerta de enlace NAT).	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	2. Introduzca `nat-one` como nombre de la puerta de enlace NAT. 3. Seleccione `public-one` como la subred en la que crear la puerta de enlace NAT. 4. En el tipo de conectividad, elija Pública. 5. En Elastic IP Allocation ID (ID de asignación de IP elástica), elija el primer ID de la dirección IP elástica que creó anteriormente y asoció con la puerta de enlace NAT. 6. Elija Crear una puerta de enlace de NAT.	

Tarea	Descripción	Habilidades requeridas
Cree la segunda puerta de enlace NAT.	1. En la consola de Amazon VPC, elija NAT Gateways (Puertas de enlace NAT) y, luego, elija Create NAT Gateway (Crear puerta de enlace NAT). 2. Introduzca `nat-two` como nombre de la puerta de enlace NAT. 3. Seleccione `public-two` como la subred en la que crear la puerta de enlace NAT. 4. En el tipo de conectividad, elija Pública. 5. En Elastic IP Allocation ID (ID de asignación de IP elástica), elija el segundo ID de la dirección IP elástica que creó anteriormente y asoció con la puerta de enlace NAT. 6. Elija Crear una puerta de enlace de NAT.	Administrador de AWS

Cree tablas de enrutamiento para sus subredes públicas y privadas

Tarea	Descripción	Habilidades requeridas
Crear la tabla de enrutamiento de la subred pública.	1. En la consola de Amazon VPC, elija Route Tables (Tablas de enrutamiento) y, a continuación, elija Create	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	route table (Crear tabla de enrutamiento). 2. Introduzca `public-one-subnet` el nombre de tabla de enrutamiento y, a continuación, elija Crear tabla de enrutamiento. 3. Seleccione la tabla de enrutamiento `public-one-subnet` , elija Edit routes (Editar rutas), y luego elija Add route (Agregar ruta). 4. Especifique `0.0.0.0` en el cuadro Destination (Destino) y seleccione el ID del puerta de enlace de Internet en la lista Target (Objetivo). 5. En la pestaña Subnet associations (Asociaciones de subred), elija Edit subnet associations (Editar asociaciones de subred), seleccione la subred `public-one` con el rango CIDR `10.0.0.0/28` y, a continuación, elija Save associations (Guardar asociaciones). 6. Seleccione Guardar cambios.	

Tarea	Descripción	Habilidades requeridas
Crear la tabla de enrutamiento de la segunda subred pública.	1. En la consola de Amazon VPC, elija Route Tables (Tablas de enrutamiento) y, a continuación, elija Create route table (Crear tabla de enrutamiento). 2. Introduzca `public-two-subnet` el nombre de tabla de enrutamiento y, a continuación, elija Crear tabla de enrutamiento. 3. Elija la `public-two-subnet`route table (tabla de enrutamiento), elija Edit routes (Editar rutas) y luego elija Add route (Agregar ruta). 4. Especifique `0.0.0.0` en el cuadro Destination (Destino) y seleccione el ID del puerta de enlace de Internet en la lista Target (Objetivo). 5. En la pestaña Subnet associations (Asociaciones de subred), elija Edit subnet associations (Editar asociaciones de subred), seleccione la subred `public-two` con el rango CIDR `10.0.0.16/28` y, a continuación, elija Save associations (Guardar asociaciones).	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	6. Seleccione Guardar cambios.	

Tarea	Descripción	Habilidades requeridas
Crear la tabla de enrutamiento de la subred privada.	1. En la consola de Amazon VPC, elija Route Tables (Tablas de enrutamiento) y, a continuación, elija Create route table (Crear tabla de enrutamiento). 2. Introduzca `private-one-subnet` el nombre de tabla de enrutamiento y, a continuación, elija Crear tabla de enrutamiento. 3. Elija la `private-one-subnet` route table (tabla de enrutamiento), elija Edit routes (Editar rutas) y luego elija Add route (Agregar ruta). 4. Especifique `0.0.0.0` en el cuadro Destination (Destino) y seleccione la puerta de enlace de NAT en la subred `public-one` de la lista Target (Objetivo). 5. En la pestaña Subnet associations (Asociaciones de subred), elija Edit subnet associations (Editar asociaciones de subred), seleccione la subred `private-one` `10.0.0.32/28` con el rango CIDR y, a continuación, elija Save	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	associations (Guardar asociaciones). 6. Seleccione Guardar cambios.	

Tarea	Descripción	Habilidades requeridas
Crear la tabla de enrutamiento de la segunda subred privada.	1. En la consola de Amazon VPC, elija Route Tables (Tablas de enrutamiento) y, a continuación, elija Create route table (Crear tabla de enrutamiento). 2. Introduzca `private-two-subnet` el nombre de tabla de enrutamiento y, a continuación, elija Crear tabla de enrutamiento. 3. Elija la `private-two-subnet` route table (tabla de enrutamiento), elija Edit routes (Editar rutas) y luego elija Add route (Agregar ruta). 4. Especifique `0.0.0.0` en el cuadro Destination (Destino) y seleccione la puerta de enlace de NAT en la subred `public-two` de la lista Target (Objetivo). 5. En la pestaña Subnet associations (Asociaciones de subred), elija Edit subnet associations (Editar asociaciones de subred), seleccione la subred `private-two` con el rango CIDR `10.0.0.64/28` y, a continuación, elija Save associations (Guardar asociaciones).	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	6. Seleccione Guardar cambios.	

Cree la función de Lambda, agréguela a la VPC y pruebe la solución

Tarea	Descripción	Habilidades requeridas
Crear una nueva función de Lambda.	1. Abra la consola AWS Lambda y, a continuación, elija Create a function (Crear una función) 2. En Información básica, inserte `Lambda test` en Nombre de la función y, a continuación, elija el idioma que prefiera en Tiempo de ejecución. 3. Elija Crear función.	Administrador de AWS
Agregue la función de Lambda a su VPC.	1. En la consola de AWS Lambda, seleccione Funciones y, a continuación, elija la función que creó anteriormente. 2. Elija Configuración y, a continuación, elija VPC. 3. Elija Editar y, a continuación, elija `Lambda VPC` y ambas subredes privadas. 4. Elija el Grupo de seguridad predeterminado para realizar las pruebas y, a	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	continuación, seleccione Guardar.	
Escriba el código para llamar a un servicio externo.	1. En el lenguaje de programación que prefiera, escriba el código para llamar a un servicio externo que devuelva su dirección IP. 2. Compruebe que la dirección IP devuelta coincide con una de sus direcciones IP elásticas.	Administrador de AWS

Recursos relacionados

- Configuración de una función Lambda para obtener acceso a los recursos en una PC

Instalación del agente SSM en los nodos de trabajo de Amazon EKS mediante Kubernetes DaemonSet

Creado por Mahendra Siddappa (AWS)

Entorno: PoC o piloto	Tecnologías: contenedores y microservicios; Infraestructura DevOps	Servicios de AWS: Amazon EKS; AWS Systems Manager

Resumen

Nota, septiembre de 2021: Las últimas AMI optimizadas para Amazon EKS instalan SSM Agent automáticamente. Para obtener más información, consulte las notas de la versión de las AMI de junio de 2021.

En Amazon Elastic Kubernetes Service (Amazon EKS), debido a las directrices de seguridad, los nodos de trabajo no tienen pares de claves de Secure Shell (SSH) adjuntos. Este patrón muestra cómo puede usar el tipo de DaemonSet recurso Kubernetes para instalar AWS Systems Manager Agent (SSM Agent) en todos los nodos de trabajo, en lugar de instalarlo manualmente o reemplazar la Amazon Machine Image (AMI) de los nodos. DaemonSet utiliza una tarea automática en el nodo de trabajo para programar la instalación del agente SSM. También puede usar este patrón para instalar otros paquetes en los nodos de trabajo.

Al solucionar problemas en el clúster, instalar el agente SSM bajo demanda le permite establecer una sesión de SSH con el nodo de trabajo, recopilar registros o analizar la configuración de la instancia, sin pares de claves SSH.

Requisitos previos y limitaciones

Requisitos previos

- Un clúster de Amazon EKS existente con nodos de trabajo de Amazon Elastic Compute Cloud (Amazon EC2).
- Las instancias contenedoras deben tener los permisos necesarios para comunicarse con el servicio SSM. AmazonSSM, la función gestionada por AWS Identity and Access Management (IAM), ManagedInstanceCore proporciona los permisos necesarios para que el agente SSM se

ejecute en instancias EC2. Para obtener más información, consulte la documentación de AWS Systems Manager.

Limitaciones

- Este patrón no se aplica a AWS Fargate porque DaemonSets no es compatible con la plataforma Fargate.
- Este patrón solo se aplica a los nodos de trabajo basados en Linux.
- Los DaemonSet pods se ejecutan en modo privilegiado. Si el clúster de Amazon EKS tiene un webhook que bloquea los pods en modo privilegiado, el agente SSM no se instalará.

Arquitectura

El siguiente diagrama ilustra la arquitectura de este patrón.

Herramientas

Herramientas

- kubectl es una utilidad de línea de comandos que se utiliza para interactuar con un clúster de Amazon EKS. Este patrón se utiliza `kubectl` para implementar un DaemonSet en el clúster de Amazon EKS, que instalará el agente SSM en todos los nodos de trabajo.
- Amazon EKS facilita la ejecución de Kubernetes en AWS sin tener que instalar, operar y mantener su propio plano o nodos de control de Kubernetes. Kubernetes es un sistema de código abierto para automatizar la implementación, escalado y administración de las aplicaciones en contenedores.
- El administrador de sesiones de AWS Systems Manager le permite administrar instancias EC2, instancias locales y máquinas virtuales (VM) mediante una intérprete de comandos interactiva con un solo clic basada en navegador o mediante la Interfaz de la línea de comandos de AWS (AWS CLI).

Código

Utilice el siguiente código para crear un archivo de DaemonSet configuración que instalará el agente SSM en el clúster de Amazon EKS. Siga las instrucciones en la sección Epics.

```
cat << EOF > ssm_daemonset.yaml
apiVersion: apps/v1
kind: DaemonSet
metadata:
  labels:
    k8s-app: ssm-installer
  name: ssm-installer
  namespace: kube-system
spec:
  selector:
    matchLabels:
      k8s-app: ssm-installer
  template:
    metadata:
      labels:
        k8s-app: ssm-installer
    spec:
      containers:
      - name: sleeper
        image: busybox
        command: ['sh', '-c', 'echo I keep things running! && sleep 3600']
      initContainers:
      - image: amazonlinux
        imagePullPolicy: Always
        name: ssm
        command: ["/bin/bash"]
        args: ["-c","echo '* * * * * root yum install -y https://s3.amazonaws.com/
ec2-downloads-windows/SSMAgent/latest/linux_amd64/amazon-ssm-agent.rpm & rm -rf /etc/
cron.d/ssmstart' > /etc/cron.d/ssmstart"]
        securityContext:
          allowPrivilegeEscalation: true
        volumeMounts:
        - mountPath: /etc/cron.d
          name: cronfile
        terminationMessagePath: /dev/termination-log
        terminationMessagePolicy: File
      volumes:
      - name: cronfile
        hostPath:
          path: /etc/cron.d
          type: Directory
      dnsPolicy: ClusterFirst
      restartPolicy: Always
```

```
      schedulerName: default-scheduler
      terminationGracePeriodSeconds: 30
EOF
```

Epics

Configurar kubectl

Tarea	Descripción	Habilidades requeridas
Instale y configure kubectl para acceder al clúster de EKS.	Si `kubectl` aún no está instalado y configurado para acceder al clúster de Amazon EKS, consulte Instalación de kubectl en la documentación de Amazon EKS.	DevOps

Implemente el DaemonSet

Tarea	Descripción	Habilidades requeridas
Cree el archivo DaemonSet de configuración.	Utilice el código de la sección Código que aparece anteriormente en este patrón para crear un archivo de DaemonSet configuración denominado `ossm_daemonset.yaml` , que se implementará en el clúster de Amazon EKS. El pod lanzado por DaemonSet tiene un contenedor principal y un `init` contenedor. El contenedor principal tiene un comando `sleep`. El contenedor `init` incluye una	DevOps

Tarea	Descripción	Habilidades requeridas
	sección `command` que crea un archivo cron para instalar el agente SSM en la ruta `/etc/cron.d/` . El trabajo cron se ejecuta solo una vez y el archivo que crea se elimina automáticamente una vez finalizado el trabajo. Cuando el contenedor de inicio ha terminado, el contenedor principal espera 60 minutos antes de salir. Después de 60 minutos, se lanza una nueva cápsula. Este módulo instala el Agente SSM, si falta, o actualiza el Agente SSM a la versión más reciente. Si es necesario, puede modificar el comando `sleep` para que se reinicie el pod una vez al día o para que se ejecute con más frecuencia.	

Tarea	Descripción	Habilidades requeridas
DaemonSet Despliéguelo en el clúster de Amazon EKS.	Para implementar el archivo de DaemonSet configuración que creó en el paso anterior en el clúster de Amazon EKS, utilice el siguiente comando: `kubectl apply -f ssm_daemonset.yaml` Este comando crea un DaemonSet para ejecutar los pods en los nodos de trabajo e instalar el agente SSM.	DevOps

Recursos relacionados

- Instalación de kubectl (documentación de Amazon EKS)
- Configuración del administrador de sesiones (documentación de AWS Systems Manager)

Instale el agente SSM y el CloudWatch agente en los nodos de trabajo de Amazon EKS mediante preBootstrapCommands

Creado por Akkamahadevi Hiremath (AWS)

Entorno: producción	Tecnologías: contenedores y microservicios; infraestructura; operaciones	Servicios de AWS: Amazon EKS; AWS Systems Manager; Amazon CloudWatch

Resumen

Este patrón proporciona ejemplos de código y pasos para instalar el agente de AWS Systems Manager (SSM Agent) y el agente de Amazon CloudWatch en los nodos de trabajo de Amazon Elastic Kubernetes Service (Amazon EKS) en la nube de Amazon Web Services (AWS) durante la creación del clúster de Amazon EKS. Puede instalar el agente SSM y el CloudWatch agente mediante la `preBootstrapCommands` propiedad del esquema del archivo de `eksctl` configuración (documentación de Weaveworks). A continuación, puede utilizar SSM Agent para conectarse a los nodos de trabajo sin utilizar un par de claves de Amazon Elastic Compute Cloud (Amazon EC2). Además, puede utilizar el CloudWatch agente para supervisar la utilización de la memoria y el disco en los nodos de trabajo de Amazon EKS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- La utilidad de línea de comandos eksctl, instalada y configurada en macOS, Linux o Windows
- La utilidad de línea de comandos kubectl, instalada y configurada en macOS, Linux o Windows

Limitaciones

- Le recomendamos que evite añadir scripts de ejecución prolongada a la propiedad `preBootstrapCommands`, ya que esto retrasa la incorporación del nodo al clúster de Amazon EKS durante las actividades de escalado. En su lugar, le recomendamos que cree una imagen de máquina de Amazon Machine (AMI) personalizada.

- Este patrón se aplica únicamente a instancias Linux de Amazon EC2.

Arquitectura

Pila de tecnología

- Amazon CloudWatch
- Amazon Elastic Kubernetes Service (Amazon EKS)
- Almacén de parámetros de AWS Systems Manager

Arquitectura de destino

El siguiente diagrama muestra un ejemplo de un usuario que se conecta a los nodos de trabajo de Amazon EKS mediante el agente SSM, que se instaló mediante elv`preBootstrapCommands`.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El usuario crea un clúster de Amazon EKS mediante el archivo de `eksctl` configuración con la `preBootstrapCommands` propiedad, que instala el agente y CloudWatch el agente de SSM.
2. Todas las instancias nuevas que se unan al clúster más adelante debido a actividades de escalado se crean con el agente y el agente SSM preinstalados. CloudWatch
3. El usuario se conecta a Amazon EC2 mediante el agente SSM y, a continuación, supervisa el uso de la memoria y el disco mediante el agente. CloudWatch

Herramientas

- Amazon le CloudWatch ayuda a monitorizar las métricas de sus recursos de AWS y las aplicaciones que ejecuta en AWS en tiempo real.
- Amazon Elastic Kubernetes Service (Amazon EKS) lo ayuda a ejecutar Kubernetes en sin necesidad de instalar ni mantener su propio plano de control o nodos de Kubernetes.
- Almacén de parámetros de AWS Systems Manager proporciona un almacenamiento seguro y jerárquico para administrar los datos de configuración y administrar los secretos.
- El administrador de sesiones de AWS Systems Manager lo ayuda a administrar las instancias de EC2, las instancias en las instalaciones y las máquinas virtuales a través de un intérprete de

comandos interactivo basado en navegador con un solo clic o a través de la Interfaz de la línea de comandos de AWS (AWS CLI).

- eksctl: es una utilidad sencilla de línea de comandos para crear y administrar clústeres de Kubernetes en Amazon EKS.
- kubectl: es una utilidad de línea de comandos para comunicarse con el servidor de la API del clúster.

Epics

Crear un clúster de Amazon EKS

Tarea	Descripción	Habilidades requeridas
Guarde el archivo de configuración del CloudWatch agente.	Guarde el archivo de configuración del CloudWatch agente en el almacén de parámetros de AWS Systems Manager, en la región de AWS en la que desee crear su clúster de Amazon EKS. Para ello, cree un parámetro en el Almacén de parámetros de AWS Systems Manager y anote el nombre del parámetro (por ejemplo, `AmazonCloudwatch-linux`). Para obtener más información, consulte el ejemplo de código del archivo de configuración del CloudWatch agente en la sección de información adicional de este patrón.	DevOps ingeniero
Cree el archivo de configuración y el clúster de eksctl.	1. Cree un archivo `eksctl` de configuración que incluya los pasos de instalación del	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	CloudWatch agente y del agente SSM. Para obtener más información, consulte el ejemplo de código del archivo de configuración eksctl en la sección de información adicional de este patrón. 2. Crear un clúster ejecutando el comando `eksctl create cluster -f cluster.yaml .`	

Compruebe que el agente y el agente de SSM CloudWatch funcionan

Tarea	Descripción	Habilidades requeridas
Pruebe el agente de SSM.	Utilice SSH para conectarse a los nodos de su clúster de Amazon EKS mediante cualquiera de los métodos descritos en Iniciar una sesión en la documentación de AWS Systems Manager.	AWS DevOps
Pon a prueba el CloudWatch agente.	Utilice la CloudWatch consola para validar el CloudWatch agente: 1. Inicie sesión en la consola de administración de AWS y abra la consola de CloudWatch .	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	2. En el panel de navegación, expanda Métricas y seleccione Todas las étricas. 3. En el cuadro de búsqueda de la pestaña Examinar, introduzca y, a continuación, seleccione las métricas de CWAgent para ver las métricas de memoria y disco.	

Recursos relacionados

- Instalación y ejecución del CloudWatch agente en sus servidores (CloudWatch documentación de Amazon)
- Creación de un parámetro de Systems Manager (consola) (documentación de AWS Systems Manager)
- Crear el archivo de configuración del CloudWatch agente (CloudWatch documentación de Amazon)
- Iniciar una sesión (AWS CLI) (documentación de AWS Systems Manager)
- Inicio de una sesión (consola de Amazon EC2) (documentación de AWS Systems Manager)

Información adicional

Ejemplo de archivo de configuración del CloudWatch agente

En el siguiente ejemplo, el CloudWatch agente está configurado para supervisar el uso del disco y la memoria en las instancias de Amazon Linux:

```
{
    "agent": {
        "metrics_collection_interval": 60,
        "run_as_user": "cwagent"
```

```
    },
    "metrics": {
        "append_dimensions": {
            "AutoScalingGroupName": "${aws:AutoScalingGroupName}",
            "ImageId": "${aws:ImageId}",
            "InstanceId": "${aws:InstanceId}",
            "InstanceType": "${aws:InstanceType}"
        },
        "metrics_collected": {
            "disk": {
                "measurement": [
                    "used_percent"
                ],
                "metrics_collection_interval": 60,
                "resources": [
                    "*"
                ]
            },
            "mem": {
                "measurement": [
                    "mem_used_percent"
                ],
                "metrics_collection_interval": 60
            }
        }
    }
}
```

Ejemplo de archivo de configuración eksctl

```
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig
metadata:
  name: test
  region: us-east-2
  version: "1.24"
managedNodeGroups:
  - name: test
    minSize: 2
    maxSize: 4
    desiredCapacity: 2
    volumeSize: 20
    instanceType: t3.medium
```

```
    preBootstrapCommands:
    - sudo yum install amazon-ssm-agent -y
    - sudo systemctl enable amazon-ssm-agent
    - sudo systemctl start amazon-ssm-agent
    - sudo yum install amazon-cloudwatch-agent -y
    - sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-
config -m ec2 -s -c ssm:AmazonCloudwatch-linux
    iam:
      attachPolicyARNs:
        - arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy
        - arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy
        - arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly
        - arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy
        - arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore
```

Detalles de código adicionales

- En la última línea de la propiedad `preBootstrapCommands`, `AmazonCloudwatch-linux` es el nombre del parámetro creado en el almacén de parámetros del Almacén de parámetros de AWS Systems Manager. Debe incluir `AmazonCloudwatch-linux` en el Almacén de parámetros de la misma región de AWS en la que creó el clúster de Amazon EKS. También puede especificar una ruta de archivo, pero le recomendamos que utilice Systems Manager para facilitar la automatización y la reutilización.
- Si las utiliza `preBootstrapCommands` en el archivo `eksctl` de configuración, verá dos plantillas de lanzamiento en la consola de administración de AWS. La primera plantilla de lanzamiento incluye los comandos especificados en `preBootstrapCommands`. La segunda plantilla incluye los comandos especificados `preBootstrapCommands` y los datos de usuario predeterminados de Amazon EKS. Estos datos son necesarios para que los nodos se unan al clúster. El grupo Auto Scaling del grupo de nodos utiliza estos datos de usuario para generar nuevas instancias.
- Si usa el atributo `iam` en el archivo de configuración `eksctl`, debe enumerar las políticas predeterminadas de Amazon EKS junto con cualquier política adicional requerida en las políticas de AWS Identity and Access Management (IAM) adjuntas. En el fragmento de código del paso Crear el clúster y el archivo de configuración eksctl, `AmazonSSMMangedInstanceCore` se añaden políticas adicionales para garantizar que el CloudWatch agente `CloudWatchAgentServerPolicy` y el agente SSM funcionen según lo previsto. Las políticas`AmazonEKSWorkerNodePolicy`, `AmazonEKS_CNI_Policy` y `AmazonEC2ContainerRegistryReadOnly` son políticas obligatorias necesarias para que el clúster de Amazon EKS funcione correctamente.

Optimizar imágenes de Docker generadas por AWS App2Container

Creado por Varun Sharma (AWS)

Entorno: PoC o piloto	Tecnologías: contenedores y microservicios; Modernización; DevOps	Servicios de AWS: Amazon ECS

Resumen

AWS App2Container es una herramienta de línea de comandos que le ayuda a transformar en contenedores las aplicaciones existentes en las instalaciones que se ejecutan en máquinas virtuales sin necesidad de cambiar el código.

En función del tipo de aplicación, App2Container adopta un enfoque conservador para identificar las dependencias. En el modo de proceso, todos los archivos que no son del sistema en el servidor de aplicaciones se incluyen en la imagen del contenedor. En esos casos, se puede generar una imagen de gran tamaño.

Este patrón proporciona un enfoque para optimizar las imágenes del contenedor generadas por App2Container. Es aplicable a todas las aplicaciones Java detectadas por App2Container en modo de proceso. El flujo de trabajo definido en el patrón ha sido diseñado para ejecutarse en el servidor de aplicaciones.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un servidor de aplicaciones con una aplicación Java que se ejecuta en un servidor Linux
- App2Container instalado y configurado, con todos los requisitos previos satisfechos, en el servidor Linux

Arquitectura

Pila de tecnología de origen

- Aplicaciones Java que se ejecutan en un servidor Linux

Pila de tecnología de destino

- Una imagen de Docker generada por App2Container

Arquitectura de destino

1. Descubra las aplicaciones que se ejecutan en el servidor de aplicaciones y analice las aplicaciones.
2. Contenerización de aplicaciones.
3. Evalúe el tamaño de la imagen de Docker. Si la imagen es demasiado grande, continúe con el paso 4.
4. Utilice el script de intérprete de comandos (adjunto) para identificar los archivos de gran tamaño.
5. Actualice las listas `appExcludedFiles` y `appSpecificFiles` del archivo `analysis.json`.

Herramientas

Herramientas

- AWS App2Container (A2C): AWS App2Container (A2C) es una herramienta de la línea de comandos que le ayuda a migrar mediante lift-and-shift las aplicaciones que se ejecutan en centros de datos en las instalaciones o en máquinas virtuales, de modo que se ejecuten en contenedores administrados por Amazon Elastic Container Service (Amazon ECS) o Amazon Elastic Kubernetes Service (Amazon EKS).

Código

Se adjuntan el script de intérprete de comandos `optimizeImage.sh` y un archivo `analysis.json` de ejemplo.

El archivo `optimizeImage.sh` es un script de utilidad para revisar el contenido del archivo generado por App2Container, `ContainerFiles.tar`. La revisión identifica los archivos o subdirectorios grandes que se pueden excluir. El script es un contenedor para el siguiente comando tar.

```
tar -Ptvf <path>|tr -s ' '|cut -d ' ' -f3,6| awk '$2 ~/<filetype>$/'| awk '$2 ~/
^<toplevel>/'| cut -f1-<depth> -d'/'|awk '{ if ($1>= <size>) arr[$2]+=$1 } END { for
 (key in arr) { if(<verbose>) printf("%-50s\t%-50s\n", key, arr[key]) else printf("%s,
\n", key) } } '|sort -k2 -nr
```

En el comando tar, el script usa los siguientes valores:

`path`	La ruta a `ContainerFiles.tar`
`filetype`	Tipo de archivo a comparar
`toplevel`	Directorio de nivel superior a comparar
`depth`	Profundidad de la ruta absoluta
`size`	Tamaño de cada archivo

El script hace lo siguiente:

1. Emplea `tar -Ptvf` para enumerar los archivos sin extraerlos.
2. Filtra los archivos por tipo de archivo, empezando por el directorio de nivel superior.
3. En función de la profundidad, genera la ruta absoluta como un índice.
4. Según el índice y el almacenamiento, indica el tamaño total del subdirectorio.
5. Imprime el tamaño del subdirectorio.

También puede sustituir los valores manualmente en el comando tar.

Epics

Descubra, analice y coloque las aplicaciones en contenedores

Tarea	Descripción	Habilidades requeridas
Descubra las aplicaciones Java en las instalaciones.	Para descubrir todas las aplicaciones en ejecución en el servidor de aplicaciones, ejecute el siguiente comando.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`sudo app2container inventory`	
Analice las aplicaciones descubiertas.	Para analizar cada aplicación mediante el `application-id` obtenido en la fase de inventario, ejecute el siguiente comando. `sudo app2container analyze --application-id <java-app-id>`	AWS DevOps
Coloque las aplicaciones analizadas en contenedores.	Ejecute el siguiente comando para la contenerización de una aplicación. `sudo app2container containerize --application-id <application-id>` El comando genera la imagen de Docker junto con un paquete tar en la ubicación del espacio de trabajo. Si la imagen de Docker es demasiado grande, continúe al siguiente paso.	AWS DevOps

Identifique appExcludedFiles y appSpecificFiles desde el archivo tar extraído de App2Container

Tarea	Descripción	Habilidades requeridas
Identifique el tamaño del archivo tar de artefactos.	Identifique el archivo `ContainerFiles.tar` en `{workspace}/{java-app-id}/Artifacts` . `workspace` es el espacio de trabajo de App2Container, y `java-app-id` es la ID de la aplicación. `./optimizeImage.sh -p /{workspace}/{java-app-id}/Artifacts/ContainerFiles.tar -d 0 -t / -v` Este es el tamaño total del archivo tar tras la optimización.	AWS DevOps
Enumere los subdirectorios del directorio / y sus tamaños.	Para identificar los tamaños de los subdirectorios principales en el directorio de nivel superior `/`, ejecute el siguiente comando. `./optimizeImage.sh -p /{workspace}/{java-app-id}/Artifacts/ContainerFiles.tar -d 1 -t / -s 1000000 -v` `/var` `554144711` `/usr` `2097300819`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`/tmp 18579660` `/root 43645397` `/opt 222320534` `/home 65212518` `/etc 11357677`	

Tarea	Descripción	Habilidades requeridas
Identifique los subdirectorios grandes en el directorio /.	En cada subdirectorio principal enumerado en el comando anterior, identifique los tamaños de sus subdirectorios. Use `-d` para aumentar la profundidad y `-t` para indicar el directorio de nivel superior. Por ejemplo, use `/var` como directorio de nivel superior. En `/var`, identifique todos los subdirectorios grandes y sus tamaños. `./optimizeImage.sh -p /{workspace}/{java-app-id}/Artifacts/ContainerFiles.tar -d 2 -t /var -s 1000000 -v` Repita este proceso en cada subdirectorio de la lista del paso anterior (por ejemplo, `/usr`, `/tmp`, `/opt` y `/home`).	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Analice la carpeta grande de cada subdirectorio en el directorio /.	En cada subdirectorio enumerado en el paso anterior, identifique las carpetas necesarias para ejecutar la aplicación. Por ejemplo, en los subdirectorios del paso anterior, enumere todos los subdirectorios del directorio `/var` y sus tamaños. Identifique los subdirectorios necesarios para la aplicación. `/var/tmp 237285851` `/var/lib 24489984` `/var/cache 237285851` Para excluir los subdirectorios que la aplicación no necesita, en el archivo `analysis.json` , añada dichos subdirectorios a la sección `appExcludedFiles` , en `containerParameters` . Se adjunta un archivo `analysis.json` de ejemplo.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Identifique los archivos necesarios en la lista appExcludes.	En cada subdirectorio agregado a la lista appExcludes, identifique los archivos de dicho subdirectorio necesarios para la aplicación. En el archivo analysis.json, añada los archivos o subdirectorios específicos en la sección `appSpecificFiles` , en `containerParameters` . Por ejemplo, si el directorio `/usr/lib` se añade a la lista de exclusiones, pero `/usr/lib/jvm` es necesario para la aplicación, añada `/usr/lib/jvm` a la sección `appSpecificFiles` .	AWS DevOps

Extraiga la aplicación y vuelva a colocarla en un contenedor

Tarea	Descripción	Habilidades requeridas
Coloque la aplicación analizada en un contenedor.	Ejecute el siguiente comando para la contenerización de la aplicación. `sudo app2container containerize --application-id <application-id>` El comando genera la imagen de Docker junto con un	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	paquete tar en la ubicación del espacio de trabajo.	
Identifique el tamaño del archivo tar de artefactos.	Identifique el archivo `ContainerFiles.tar` en `{workspace}/{java-app-id}/Artifacts` , donde `workspace` es el espacio de trabajo de App2Container, y `java-app-id` es la ID de la aplicación. `./optimizeImage.sh -p /{workspace}/{java-app-id}/Artifacts/ContainerFiles.tar -d 0 -t / -v` Este es el tamaño total del archivo tar tras la optimización.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Ejecutar la imagen de Docker.	Para comprobar que la imagen se inicia sin errores, ejecute la imagen de Docker de forma local mediante los siguientes comandos. Para identificar el `imageId` del contenedor, use `docker images |grep java-app-id .` Para ejecutar el contenedor, use `docker run -d <image id>`.	AWS DevOps

Recursos relacionados

- ¿Qué es App2Container?
- AWS App2Container: una nueva herramienta de colocación en contenedor para aplicaciones Java y .NET (publicación del blog)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Coloque los pods de Kubernetes en Amazon EKS mediante la afinidad, las taints y las tolerancias de nodos

Documento creado por Hitesh Parikh (AWS) y Raghu Bhamidimarri (AWS)

Entorno: PoC o piloto	Tecnologías: contenedores y microservicios	Carga de trabajo: código abierto
Servicios de AWS: Amazon EKS		

Resumen

Este patrón muestra el uso de la afinidad de nodos de Kubernetes, las taints de nodos y las tolerancias de los pods para programar intencionalmente los pods de aplicaciones en nodos de trabajo específicos de un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) en la nube de Amazon Web Services (AWS).

Una taint es una propiedad de un nodo que permite a los nodos rechazar un conjunto de pods. Una tolerancia es una propiedad de los pods que permite al programador de Kubernetes programar los pods en los nodos que tengan las mismas taints.

Sin embargo, las tolerancias por sí solas no pueden impedir que un programador coloque un pod en un nodo de trabajo que no contenga taints. Por ejemplo, un pod de procesamiento intensivo con una tolerancia puede programarse involuntariamente en un nodo no contaminado de uso general. En ese escenario, la propiedad de afinidad de nodos de un pod indica al planificador que coloque el pod en un nodo que cumpla con los criterios de selección de nodos especificados en la afinidad de nodos.

La combinación de taint, tolerancia y la afinidad de nodos indica al programador que programe los pods de forma coherente en los nodos, con las taints coincidentes y las etiquetas de nodo que coincidan con los criterios de selección de nodos de afinidad de nodos especificados en el pod.

Este patrón proporciona un ejemplo de un archivo de manifiesto de implementación de Kubernetes y los pasos para crear un clúster de EKS, implementar una aplicación y validar la ubicación del pod.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS con credenciales configuradas para crear recursos en su cuenta de AWS
- Interfaz de la línea de comandos de AWS (AWS CLI)
- eksctl
- kubectl
- Se instaló Docker (para el sistema operativo que se estaba utilizando) y se puso en marcha el motor (para obtener información sobre los requisitos de licencia de Docker, consulte el sitio de Docker)
- Java, versión 11 o posterior
- Un microservicio de Java que se ejecute en su entorno de desarrollo integrado (IDE) favorito; por ejemplo, AWS Cloud9, IntelliJ IDEA Community Edition o Eclipse (si no tiene un microservicio de Java, consulte el patrón Implementar un ejemplo de microservicio de Java en Amazon EKS y Microservicios con Spring para obtener ayuda con la creación del microservicio)

Limitaciones

- Este patrón no proporciona el código Java y supone que ya está familiarizado con Java. Para crear un microservicio Java básico, consulte Implementación de un microservicio Java de muestra en Amazon EKS.
- Los pasos de este artículo crean recursos de AWS que pueden acumular costos. Asegúrese de limpiar los recursos de AWS una vez que haya completado los pasos para implementar y validar el patrón.

Arquitectura

Pila de tecnología de destino

- Amazon EKS
- Java
- Docker
- Amazon Elastic Container Registry (Amazon ECR)

Arquitectura de destino

El diagrama de arquitectura de la solución muestra Amazon EKS con dos pods (implementación 1 y implementación 2) y dos grupos de nodos (ng1 y ng2) con dos nodos cada uno. Los pods y los nodos tienen las siguientes propiedades.

	Pod de implementación 1	Pod de implementación 2	Grupo de nodos 1 (ng1)	Grupo de nodos 2 (ng2)
Tolerancia	clave: classified_load, valor: verdadero, efecto: NoSchedule clave: machine_learning_workload, valor: verdadero, efecto: NoSchedule	Ninguna		
Afinidad de nodos	clave: alpha.eksctl.io/nodegroup-name = ng1;	Ninguna	NodeGroups.name = ng1	
Taint			clave: classified_load, valor: verdadero, efecto: NoSchedule clave: machine_learning_workload, valor: verdadero	Ninguna

, efecto:
NoSchedule

1. El pod de implementación 1 tiene definidas las tolerancias y la afinidad de nodos, lo que indica al programador de Kubernetes que coloque los pods de despliegue en los nodos del grupo de nodos 1 (ng1).
2. El grupo de nodos 2 (ng2) no tiene una etiqueta de nodo que coincida con la expresión del selector de nodos de afinidad de nodos de la implementación 1, por lo que los pods no se programarán en los nodos ng2.
3. El pod de la implementación 2 no tiene tolerancias ni afinidades de nodos definidas en el manifiesto de implementación. El programador rechazará la programación de pods de implementación 2 en el grupo de nodos 1 debido a las taint de los nodos.
4. En su lugar, los pods de implementación 2 se colocarán en el grupo de nodos 2, ya que los nodos no tienen ningún taint.

Este patrón muestra que, si se utilizan las taints y las tolerancias, combinadas con la afinidad de nodos, se puede controlar la colocación de los pods en conjuntos específicos de nodos de trabajo.

Herramientas

Servicios de AWS

- La Interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su shell de línea de comandos.
- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable.
- Amazon Elastic Kubernetes Service (Amazon EKS) lo ayuda a ejecutar Kubernetes en sin necesidad de instalar ni mantener su propio plano de control o nodos de Kubernetes.
- eksctl es el equivalente de kubectl en AWS y ayuda a crear EKS.

Otras herramientas

- Docker es un conjunto de productos de plataforma como servicio (PaaS) que utiliza la virtualización en el nivel del sistema operativo para entregar software en contenedores.
- kubectl: una interfaz de línea de comandos que le ayuda en la ejecución de comandos en clústeres de Kubernetes.

Epics

Cree el clúster EKS

Tarea	Descripción	Habilidades requeridas
Cree el archivo cluster.yaml.	Cree un archivo denominado `cluster.yaml` con el siguiente código. `apiVersion: eksctl.io/v1alpha5` `kind: ClusterConfig` `metadata:` `  name: eks-taint-demo` `  region: us-west-1` `# Unmanaged nodegroups with and without taints.` `nodeGroups:` `  - name: ng1` `  instanceType: m5.xlarge` `  minSize: 2` `  maxSize: 3` `  taints:` `  - key: classified_workload` `  value: "true"` `  effect: NoSchedule` `  - key: machine_learning_workload` `  value: "true"`	Propietario de la aplicación, AWS DevOps, administrador de la nube, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	<pre>effect: NoSchedule - name: ng2 instanceType: m5.xlarge minSize: 2 maxSize: 3</pre>	
Cree el clúster mediante eksctl.	Ejecute el archivo `cluster.yaml` para crear el clúster EKS. La creación del clúster puede tardar unos minutos. `eksctl create cluster -f cluster.yaml`	AWS DevOps, administrador de sistemas de AWS, desarrollador de aplicaciones

Cree una imagen y cárguela en Amazon ECR

Tarea	Descripción	Habilidades requeridas
Crear un repositorio privado de Amazon ECR.	Para crear un repositorio de Amazon ECR, consulte Creación de un repositorio privado. Anote el URI del repositorio.	AWS DevOps, DevOps ingeniero, desarrollador de aplicaciones
Cree el archivo Dockerfile.	Si tiene una imagen de contenedor de Docker existente que desea usar para probar el patrón, puede omitir este paso. Para crear un archivo Dockerfile, use el siguiente fragmento como referencia.	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Si encuentra errores, consulte la sección Resolución de problemas. `FROM adoptopenjdk/openjdk11:jdk-11.0.14.1_1-alpine` `RUN apk add maven` `WORKDIR /code` `# Prepare by downloading dependencies` `ADD pom.xml /code/pom.xml` `RUN ["mvn", "dependency:resolve"]` `RUN ["mvn", "verify"]` `# Adding source, compile and package into a fat jar` `ADD src /code/src` `RUN ["mvn", "package"]` `EXPOSE 4567` `CMD ["java", "-jar", "target/eksExample-jar-with-dependencies.jar"]`	

Tarea	Descripción	Habilidades requeridas
Cree el archivo pom.xml y los archivos fuente, y cree y envíe la imagen de Docker.	Para crear el archivo `pom.xml` y el archivo fuente de Java, consulte Implementar un ejemplo de microservicio Java en el patrón Amazon EKS. Siga las instrucciones de ese patrón para crear y enviar la imagen de Docker.	AWS DevOps, DevOps ingeniero, desarrollador de aplicaciones

Implemente en Amazon EKS

Tarea	Descripción	Habilidades requeridas
Cree el archivo deploymen t.yaml.	Para crear el archivo `deployment.yaml` , use el código que aparece en la sección Información adicional. En el código, la clave de la afinidad de nodos es cualquier etiqueta que se cree al crear grupos de nodos. Este patrón usa la etiqueta predeterm inada creada por eksctl. Para obtener información sobre cómo personalizar las etiquetas, consulte Asignar pods a nodos en la documenta ción de Kubernetes. El valor de la clave de afinidad de nodos es el nombre del grupo de nodos creado por `cluster.yaml` .	AWS DevOps, DevOps ingeniero, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	Para obtener la clave y el valor de la taint, ejecute el siguiente comando. `kubectl get nodes -o json | jq '.items[].spec.taints'` La imagen es el URI del repositorio de Amazon ECR que creó en un paso anterior.	
Implemente el archivo.	Para implementar en Amazon EKS, ejecute el siguiente comando. `kubectl apply -f deployment.yaml`	Desarrollador de aplicaciones, DevOps ingeniero, AWS DevOps

Tarea	Descripción	Habilidades requeridas
Compruebe la implement ación.	1. Para verificar si los pods están LISTOS, ejecute el siguiente comando. `kubectl get pods -o wide` Si el POD está listo, la salida tendrá un aspecto semejante al siguiente, con el STATUS como En ejecución. `NAME READY STATUS RESTARTS AGE IP NODE NOMINATED NODE READINESS GATES` `<pod_name> 1/1 Running 0 12d 192.168.18.50 ip-192-168-20-110.us-west-1.compute.internal <none> <none>` Anote el nombre del pod y el nombre del nodo. Puede saltar el siguiente paso. 2. (Opcional) Para obtener detalles adicionales sobre el Pod y verificar las tolerancias en el Pod, ejecute el siguiente comando.	Desarrollador de aplicaciones, DevOps ingeniero, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`kubectl describe pod <pod_name>` Un ejemplo de la salida se encuentra en la sección de Información adicional. 3. Para validar que la ubicación del pod en el nodo es correcta, ejecute el siguiente comando. `kubectl describe node <node name> | grep -A 1 "Taints"` Confirme que la taint del nodo coincide con la tolerancia y que la etiqueta del nodo coincide con la afinidad de nodos definida en `deployment.yaml` . El pod con tolerancias y afinidad de nodos debe colocarse en un nodo con las taint y las etiquetas de afinidad de nodos coinciden tes. El comando anterior muestra las taint del nodo. El siguiente es un ejemplo de salida. `kubectl describe node ip-192-168-29-181. us-west-1.compute.`	

Tarea	Descripción	Habilidades requeridas
	`internal | grep -A 1 "Taints"` `Taints:` `classifled_workload=true:NoSchedule` `machine_learning_workload=true:NoSchedule` Además, ejecute el siguiente comando para comprobar que el nodo en el que está colocado el pod tiene una etiqueta que coincida con la etiqueta del nodo de afinidad de nodos. `kubectl get node <node name> --show-labels` 4. Para comprobar que la aplicación está haciendo lo que debe hacer, compruebe los registros del Pod ejecutando el siguiente comando. `kubectl logs -f <name-of-the-pod>`	

Tarea	Descripción	Habilidades requeridas
Cree un segundo archivo.yaml de implementación sin tolerancias ni afinidad entre nodos.	Este paso adicional sirve para validar que, si no se especifica ninguna afinidad o tolerancia de nodos en el archivo de manifiesto de implementación, el pod resultante no esté programado en un nodo contaminado. (Debe programarse en un nodo que no tenga ninguna taint). Use el siguiente código para crear un nuevo archivo de implementación llamado `deploy_no_taint.yaml` . `apiVersion: apps/v1` `kind: Deployment` `metadata:` `  name: microservice-deployment-non-tainted` `spec:` `  replicas: 1` `  selector:` `  matchLabels:` `  app.kubernetes.io/name: java-microservice-no-taint` `  template:` `  metadata:` `  labels:` `  app.kubernetes.io/name: java-microservice-no-taint` `  spec:` `  containers:` `  - name: java-microservice-container-2`	Desarrollador de aplicaciones, AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`image: <account_number>.dkr.ecr<region>.amazonaws.com/<repository_name>:latest` `ports:` `- containerPort: 4567`	
Implemente el segundo archivo de implementación (.yaml) y valide la colocación del pod	1. Ejecute el siguiente comando de la . `kubectl apply -f deploy_no_taint.yaml` 2. Una vez que la implementación se haya realizado correctamente, ejecute los mismos comandos que ejecutó anteriormente para comprobar la ubicación del pod en un grupo de nodos sin ningún problema. `kubectl describe node <node_name> | grep "Taints"` La salida debería ser la siguiente. `Taints: <none>` Esto completa la prueba.	Desarrollador de aplicaciones, AWS DevOps, DevOps ingeniero

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Limpie los recursos.	Para evitar incurrir en cargos de AWS por los recursos que quedan en ejecución, utilice el siguiente comando. `eksctl delete cluster --name <Name of the cluster> --region <region-code>`	AWS DevOps, desarrollador de aplicaciones

Solución de problemas

Problema	Solución
Es posible que algunos de estos comandos no se ejecuten si su sistema utiliza la arquitectura arm64 (especialmente si la ejecuta en un Mac M1). La siguiente línea puede generar un error. `FROM adoptopenjdk/openjdk11:jdk-11.0.14.1_1-alpine`	Si tiene errores al ejecutar el Dockerfile, sustituya la línea `FROM` por la siguiente. `FROM bellsoft/liberica-openjdk-alpine-musl:17`

Recursos relacionados

- Implemente un ejemplo de microservicio Java en Amazon EKS
- Crear un repositorio privado de Amazon ECR
- Asignación de pods a nodos (documentación de Kubernetes)
- Taints y tolerancias (documentación de Kubernetes)
- Amazon EKS
- Amazon ECR

- CLI de AWS
- Docker
- IntelliJ IDEA CE
- Eclipse

Información adicional

deployment.yaml

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: microservice-deployment
spec:
  replicas: 1
  selector:
    matchLabels:
      app.kubernetes.io/name: java-microservice
  template:
    metadata:
      labels:
        app.kubernetes.io/name: java-microservice
    spec:
      affinity:
        nodeAffinity:
          requiredDuringSchedulingIgnoredDuringExecution:
            nodeSelectorTerms:
              - matchExpressions:
                  - key: alpha.eksctl.io/nodegroup-name
                    operator: In
                    values:
                      - <node-group-name-from-cluster.yaml>
      tolerations: #only this pod has toleration and is viable to go to ng with taint
        - key: "<Taint key>" #classified_workload in our case
          operator: Equal
          value: "<Taint value>" #true
          effect: "NoSchedule"
        - key: "<Taint key>" #machine_learning_workload in our case
          operator: Equal
          value: "<Taint value>" #true
          effect: "NoSchedule"
```

```
      containers:
        - name: java-microservice-container
          image: <account_number>.dkr.ecr<region>.amazonaws.com/
<repository_name>:latest
          ports:
            - containerPort: 4567
```

describe el ejemplo de salida del pod

```
Name:         microservice-deployment-in-tainted-nodes-5684cc495b-vpcfx
Namespace:    default
Priority:     0
Node:         ip-192-168-29-181.us-west-1.compute.internal/192.168.29.181
Start Time:   Wed, 14 Sep 2022 11:06:47 -0400
Labels:       app.kubernetes.io/name=java-microservice-taint
              pod-template-hash=5684cc495b
Annotations:  kubernetes.io/psp: eks.privileged
Status:       Running
IP:           192.168.13.44
IPs:
  IP:           192.168.13.44
Controlled By:  ReplicaSet/microservice-deployment-in-tainted-nodes-5684cc495b
Containers:
  java-microservice-container-1:
    Container ID:
 docker://5c158df8cc160de8f57f62f3ee16b12725a87510a809d90a1fb9e5d873c320a4
    Image:          934188034500.dkr.ecr.us-east-1.amazonaws.com/java-eks-apg
    Image ID:       docker-pullable://934188034500.dkr.ecr.us-east-1.amazonaws.com/
java-eks-apg@sha256:d223924aca8315aab20d54eddf3443929eba511b6433017474d01b63a4114835
    Port:           4567/TCP
    Host Port:      0/TCP
    State:          Running
      Started:      Wed, 14 Sep 2022 11:07:02 -0400
    Ready:          True
    Restart Count:  0
    Environment:    <none>
    Mounts:
      /var/run/secrets/kubernetes.io/serviceaccount from kube-api-access-ddvvw (ro)
Conditions:
  Type              Status
  Initialized       True
  Ready             True
  ContainersReady   True
```

```
  PodScheduled      True
Volumes:
  kube-api-access-ddvvw:
    Type:                    Projected (a volume that contains injected data from
 multiple sources)
    TokenExpirationSeconds:  3607
    ConfigMapName:           kube-root-ca.crt
    ConfigMapOptional:       <nil>
    DownwardAPI:             true
QoS Class:                   BestEffort
Node-Selectors:              <none>
Tolerations:                 classifled_workload=true:NoSchedule
                             machine_learning_workload=true:NoSchedule
                             node.kubernetes.io/not-ready:NoExecute op=Exists for 300s
                             node.kubernetes.io/unreachable:NoExecute op=Exists for
 300s
Events:                      <none>
```

Replicar imágenes filtradas de contenedores de Amazon ECR en todas las cuentas o regiones

Creado por Abdal Garuba (AWS)

Entorno: producción	Tecnologías: contenedores y microservicios; DevOps	Servicios de AWS: Amazon EC2 Container Registry; Amazon; CloudWatch AWS CodeBuild; AWS Identity and Access Management; AWS CLI

Resumen

Amazon Elastic Container Registry (Amazon ECR) puede replicar todas las imágenes de contenedores de un repositorio de imágenes en las regiones de Amazon Web Services (AWS) y en las cuentas de AWS de forma nativa, mediante las características de replicación cross-Region (entre regiones) y cross-account (entre cuentas). (Para obtener más información, consulte la publicación del blog de AWS Cross region replication in Amazon ECR has landed [La replicación entre regiones en Amazon ECR ya está aquí]). Sin embargo, no hay forma de filtrar bajo ningún criterio las imágenes que se copian en las cuentas o Regiones de AWS.

Este patrón describe cómo replicar las imágenes de contenedores almacenadas en Amazon ECR en todas las cuentas y regiones de AWS, en función de los patrones de etiquetas de imagen. El patrón utiliza Amazon CloudWatch Events para detectar eventos push en las imágenes que tienen una etiqueta personalizada predefinida. Un evento push inicia un CodeBuild proyecto de AWS y le pasa los detalles de la imagen. El CodeBuild proyecto copia las imágenes del registro Amazon ECR de origen al registro de destino en función de los detalles proporcionados.

Este patrón copia las imágenes que tienen etiquetas específicas en todas las cuentas. Así, por ejemplo, puede usar este patrón para copiar solo imágenes seguras y listas para producción en la cuenta de AWS de producción. En la cuenta de desarrollo, una vez probadas exhaustivamente las imágenes, puede añadir una etiqueta predefinida a las imágenes seguras y seguir los pasos de este patrón para copiar las imágenes marcadas en la cuenta de producción.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa para los registros de Amazon ECR de origen y destino
- Permisos administrativos para las herramientas utilizadas en este patrón
- Docker instalado en su equipo local para realizar pruebas
- Interfaz de la línea de comandos de AWS (AWS CLI), para autenticarse en Amazon ECR

Limitaciones

- Este patrón observa los eventos push del registro de origen en una sola región de AWS. Puede implementar este patrón en otras regiones para observar los registros de esas regiones.
- En este patrón, una regla de Amazon CloudWatch Events escucha un patrón de etiqueta de imagen único. Si desea comprobar si hay varios patrones, puede añadir eventos para detectar otros patrones de etiquetas de imagen.

Arquitectura

Arquitectura de destino

Automatizar y escalar

Este patrón se puede automatizar con un script de infraestructura como código (IaC) y se puede implementar a gran escala. Para usar las CloudFormation plantillas de AWS para implementar este patrón, descargue el adjunto y siga las instrucciones de la sección Información adicional.

Puede apuntar varios CloudWatch eventos de Amazon Events (con diferentes patrones de eventos personalizados) al mismo CodeBuild proyecto de AWS para replicar varios patrones de etiquetas de imagen, pero tendrá que actualizar la validación secundaria del `buildspec.yaml` archivo (que se incluye en el archivo adjunto y en la sección Herramientas) de la siguiente manera para admitir varios patrones.

```
...
if [[ ${IMAGE_TAG} != release-* ]]; then
...
```

Herramientas

Servicios de Amazon

- IAM: AWS Identity and Access Management (IAM) es un servicio web que ayuda a controlar de forma segura el acceso a los recursos de AWS. En este patrón, tendría que crear la función de IAM multicuenta que AWS CodeBuild asumirá al enviar las imágenes de los contenedores al registro de destino.
- Amazon ECR: Amazon Elastic Container Registry (Amazon ECR) es un registro de contenedores totalmente administrado que facilita almacenar, administrar, compartir e implementar imágenes y artefactos de contenedores en cualquier lugar. Las acciones de inserción de imágenes en el registro de origen envían los detalles de los eventos del sistema al bus de eventos que recoge Amazon CloudWatch Events.
- AWS CodeBuild: AWS CodeBuild es un servicio de integración continua totalmente gestionado que proporciona potencia informática para realizar tareas como la compilación del código fuente, la ejecución de pruebas y la producción de artefactos listos para su implementación. Este patrón utiliza AWS CodeBuild para realizar la acción de copia del registro Amazon ECR de origen al registro de destino.
- CloudWatch Eventos: Amazon CloudWatch Events ofrece una secuencia de eventos del sistema que describen los cambios en los recursos de AWS. Este patrón utiliza reglas para hacer coincidir las acciones push de Amazon ECR con un patrón de etiqueta de imagen específico.

Herramientas

- Docker CLI: Docker es una herramienta que facilita la creación y administración de contenedores. Los contenedores empaquetan una aplicación y todas sus dependencias en una sola unidad o paquete que se puede implementar fácilmente en cualquier plataforma que admita el tiempo de ejecución del contenedor.

Código

Se puede implementar este patrón de dos maneras:

- Configuración automatizada: Implemente las dos CloudFormation plantillas de AWS que se proporcionan en el archivo adjunto. Para obtener instrucciones, consulte la sección Información adicional.
- Configuración manual: Siga los pasos de la sección Epics.

Ejemplo de buildspec.yaml

Si utiliza las CloudFormation plantillas que se proporcionan con este patrón, el `buildspec.yaml` archivo se incluye en los CodeBuild recursos.

```
  version: 0.2
  env:
    shell: bash
  phases:
    install:
      commands:
        - export CURRENT_ACCOUNT=$(echo ${CODEBUILD_BUILD_ARN} | cut -d':' -f5)
        - export CURRENT_ECR_REGISTRY=${CURRENT_ACCOUNT}.dkr.ecr.
${AWS_REGION}.amazonaws.com
        - export DESTINATION_ECR_REGISTRY=${DESTINATION_ACCOUNT}.dkr.ecr.
${DESTINATION_REGION}.amazonaws.com
    pre_build:
      on-failure: ABORT
      commands:
        - echo "Validating Image Tag ${IMAGE_TAG}"
        - |
          if [[ ${IMAGE_TAG} != release-* ]]; then
            aws codebuild stop-build --id ${CODEBUILD_BUILD_ID}
            sleep 60
            exit 1
          fi
        - aws ecr get-login-password --region ${AWS_REGION} | docker login -u AWS --
password-stdin ${CURRENT_ECR_REGISTRY}
        - docker pull ${CURRENT_ECR_REGISTRY}/${REPO_NAME}:${IMAGE_TAG}
    build:
      commands:
        - echo "Assume cross-account role"
        - CREDENTIALS=$(aws sts assume-role --role-arn ${CROSS_ACCOUNT_ROLE_ARN} --
role-session-name Rolesession)
        - export AWS_DEFAULT_REGION=${DESTINATON_REGION}
        - export AWS_ACCESS_KEY_ID=$(echo ${CREDENTIALS} | jq -r
 '.Credentials.AccessKeyId')
        - export AWS_SECRET_ACCESS_KEY=$(echo ${CREDENTIALS} | jq -r
 '.Credentials.SecretAccessKey')
        - export AWS_SESSION_TOKEN=$(echo ${CREDENTIALS} | jq -r
 '.Credentials.SessionToken')
        - echo "Logging into cross-account registry"
        - aws ecr get-login-password --region ${DESTINATION_REGION} | docker login -u
 AWS --password-stdin ${DESTINATION_ECR_REGISTRY}
```

```
        - echo "Check if Destination Repository exists, else create"
        - |
          aws ecr describe-repositories --repository-names ${REPO_NAME} --region
${DESTINATION_REGION} \
          || aws ecr create-repository --repository-name ${REPO_NAME} --region
${DESTINATION_REGION}
        - echo "retag image and push to destination"
        - docker tag ${CURRENT_ECR_REGISTRY}/${REPO_NAME}:${IMAGE_TAG}
${DESTINATION_ECR_REGISTRY}/${REPO_NAME}:${IMAGE_TAG}
        - docker push ${DESTINATION_ECR_REGISTRY}/${REPO_NAME}:${IMAGE_TAG}
```

Epics

Cree roles de IAM

Tarea	Descripción	Habilidades requeridas
Crea un rol de CloudWatch eventos.	En la cuenta de AWS de origen, cree un rol de IAM para que lo asuma Amazon CloudWatch Events. El rol debe tener permisos para iniciar un CodeBuild proyecto de AWS. Para crear el rol mediante la AWS CLI, siga las instrucciones de la documentación de IAM. Ejemplo de política de confianza (`trustpolicy.json`): `{ "Version": "2012-10-17", "Statement": { "Effect": "Allow",`	Administrador de AWS DevOps, administrador de sistemas de AWS, administrador de nube, arquitecto de nube, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	<pre> "Principal": {"Service": "events.a mazonaws.com"}, "Action": "sts:Assu meRole" } }</pre> Ejemplo de política de permisos (`permissionpolicy.json`): <pre>{ "Version": "2012-10- 17", "Statement": { "Effect": "Allow", "Action": "codebuil d:StartBuild", "Resource": "<CodeBuild Project ARN>" } }</pre>	

Tarea	Descripción	Habilidades requeridas
Cree un CodeBuild rol.	Cree una función de IAM para CodeBuild que AWS la asuma siguiendo las instrucciones de la documentación de IAM. El rol debe tener los siguientes permisos: • Permiso para asumir el rol de multicuenta de destino • Permiso para crear grupos de registros y flujos de registros, y para enviar eventos de registro • Permisos de solo lectura para todos los repositorios de Amazon ECR, mediante la adición de la política gestionada de AmazonEC2 Container Registry ReadOnly al rol • Permiso para detener CodeBuild Ejemplo de política de confianza (`trustpolicy.json`): `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": {`	Administrador de AWS DevOps, administrador de sistemas de AWS, administrador de nube, arquitecto de nube, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	<pre>"Service": "codebuild.amazonaws.com" }, "Action": "sts:AssumeRole" }] }</pre> Ejemplo de política de permisos (`permissionpolicy.json`): <pre>{ "Version": "2012-10-17", "Statement": [{ "Action": ["codebuild:StartBuild", "codebuild:StopBuild", "codebuild:Get*", "codebuild:List*", "codebuild:BatchGet*"], "Resource": "*", "Effect": "Allow" }, { "Action": [</pre>	

Tarea	Descripción	Habilidades requeridas
	<pre>"logs:CreateLogGroup", "logs:CreateLogStream", "logs:PutLogEvents"], "Resource": "*", "Effect": "Allow" }, { "Action": "sts:AssumeRole", "Resource": "<ARN of destination role>", "Effect": "Allow", "Sid": "AssumeCrossAccountArn" }] }</pre> Adjunte la política administrada `AmazonEC2ContainerRegistryReadOnly` al comando de CLI de la siguiente manera: <pre>~$ aws iam attach-role-policy \ --policy-arn arn:aws:iam::aws:policy/Ama</pre>	

Tarea	Descripción	Habilidades requeridas
	`zonEC2ContainerRegistryReadOnly \` `--role-name <name of CodeBuild Role>`	

Tarea	Descripción	Habilidades requeridas
Cree un rol multicuenta.	En la cuenta de AWS de destino, cree una función de IAM para la CodeBuild función de AWS que asuma la cuenta de origen. El rol multicuenta debería permitir a las imágenes de contenedores crear un nuevo repositorio y cargar imágenes de contenedores a Amazon ECR. Para crear el rol de IAM mediante la AWS CLI, siga las instrucciones de la documentación de IAM. Para permitir el CodeBuild proyecto de AWS del paso anterior, utilice la siguiente política de confianza: `{ "Version": "2012-10-17", "Statement": { "Effect": "Allow", "Principal": { "AWS": "<ARN of source codebuild role>" }, "Action": "sts:AssumeRole" } }` Para permitir que el CodeBuild proyecto de AWS del paso	Administrador de AWS, administrador de la nube DevOps, arquitecto de la nube, DevOps ingeniero, administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	anterior guarde imágenes en el registro de destino, utilice la siguiente política de permisos: `{ "Version": "2012-10-17", "Statement": [{ "Action": ["ecr:GetDownloadUrlForLayer", "ecr:BatchCheckLayerAvailability", "ecr:PutImage", "ecr:InitiateLayerUpload", "ecr:UploadLayerPart", "ecr:CompleteLayerUpload", "ecr:GetRepositoryPolicy", "ecr:DescribeRepositories", "ecr:GetAuthorizationToken", "ecr:CreateRepository"],`	

Tarea	Descripción	Habilidades requeridas
	"Resource": "*", "Effect": "Allow" }] }	

Crea el CodeBuild proyecto

Tarea	Descripción	Habilidades requeridas
Crea un CodeBuild proyecto.	Cree un CodeBuild proyecto de AWS en la cuenta de origen siguiendo las instrucciones de la CodeBuild documentación de AWS. El proyecto debe estar en la misma región que el registro de origen. Configure el proyecto de la siguiente manera: • Tipo de entorno: `LINUX CONTAINER` • Rol de servicio: `CodeBuild Role` • Modo privilegiado: `true` • Imagen del entorno: `aws/codebuild/standard:x.x` (utilice la última imagen disponible) • Variables de entorno:	Administrador de AWS DevOps, administrador de sistemas de AWS, administrador de nube, arquitecto de nube, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	• `CROSS_ACCOUNT_ROLE_ARN` : el nombre de recurso de Amazon (ARN) del rol multicuenta • `DESTINATION_REGION` : el nombre de la región multicuenta • `DESTINATION_ACCOUNT` : el número de la cuenta de destino • Especificaciones de construcción: utilice el archivo `buildspec.yaml` que aparece en la sección Herramientas.	

Creación del evento

Tarea	Descripción	Habilidades requeridas
Cree una regla de eventos.	Como el patrón usa la función de filtrado de contenido, debes crear el evento con Amazon EventBridge. Crea el evento y el destino siguiendo las instrucciones de la EventBridge documentación, con algunas modificaciones: • En Define pattern (Definir patrón), seleccione Event pattern (Patrón de eventos) y, a continuación, Custom	Administrador de AWS DevOps, administrador de sistemas de AWS, administrador de nube, arquitecto de nube, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	pattern (Patrón personalizado). • Copie el siguiente código de ejemplo de patrón de eventos personalizados en el cuadro de texto proporcionado: `{ "source": ["aws.ecr"], "detail-type": ["ECR Image Action"], "detail": { "action-type": ["PUSH"], "result": ["SUCCESS"], "image-tag": [{ "prefix": "release-"}] } }` • En Select targets, elige el CodeBuild proyecto de AWS y pega el ARN del CodeBuild proyecto de AWS que creaste en la epopeya anterior. • En Configure input (Configurar entrada), seleccione Input Transformer (Transformador de entrada).	

Tarea	Descripción	Habilidades requeridas
	• En el cuadro de texto Input Path (Ruta de entrada), pegue: `{"IMAGE_TAG":"$.detail.image-tag","REPO_NAME":"$.detail.repository-name"}` • En el cuadro de texto Input Template (Plantilla de entrada), pegue: `{"environmentVariablesOverride": [ {"name": "IMAGE_TAG", "value":<IMAGE_TAG>},{"name":"REPO_NAME","value":<REPO_NAME>}]}` • Elija Usar el rol existente y elija el nombre del rol de CloudWatch Eventos que creó anteriormente en la epopeya Crear roles de IAM.	

Valide

Tarea	Descripción	Habilidades requeridas
Autenticación con Amazon ECR.	Realice la autenticación en los registros de origen y destino siguiendo los pasos de la	Administrador de AWS DevOps, administrador de sistemas de AWS, administr

Tarea	Descripción	Habilidades requeridas
	documentación de Amazon ECR.	ador de nube, DevOps ingeniero, arquitecto de nube
Pruebe la replicación de imágenes.	En su cuenta de origen, envíe una imagen de contenedor a un repositorio de origen de Amazon ECR nuevo o existente con una etiqueta de imagen con el prefijo `release-`. Para enviar la imagen, siga los pasos de la documentación de Amazon ECR. Puede supervisar el progreso del CodeBuild proyecto en la CodeBuild consola. Cuando el CodeBuild proyecto se haya completado correctamente, inicie sesión en la cuenta de AWS de destino, abra la consola Amazon ECR y confirme que la imagen existe en el registro de Amazon ECR de destino.	Administrador de AWS DevOps, administrador de sistemas de AWS, administrador de nube, arquitecto de nube, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Pruebe la exclusión de imágenes.	En su cuenta de origen, envíe una imagen de contenedo r a un repositorio de origen de Amazon ECR nuevo o existente con una etiqueta de imagen que no tenga el prefijo personalizado. Confirme que el CodeBuild proyecto no se haya iniciado y que no aparezca ninguna imagen de contenedor en el registro de destino.	Administrador de AWS DevOps, administrador de sistemas de AWS, administr ador de nube, arquitecto de nube, DevOps ingeniero

Recursos relacionados

- ¿Cómo empezar con CodeBuild
- Cómo empezar con Amazon EventBridge
- Filtrado basado en contenido en los patrones de EventBridge eventos de Amazon
- Delegate access across AWS accounts using IAM roles (Delegar el acceso entre cuentas de AWS mediante roles de IAM)
- Private image replication (Replicación de imágenes privadas)

Información adicional

Para implementar automáticamente los recursos de este patrón, siga estos pasos:

1. Descarga el archivo adjunto y extrae las dos CloudFormation plantillas: `part-1-copy-tagged-images.yaml` y`part-2-destination-account-role.yaml`.
2. Inicie sesión en la CloudFormation consola de AWS e impleméntelo `part-1-copy-tagged-images.yaml` en la misma cuenta y región de AWS que los registros de Amazon ECR de origen. Actualice los parámetros según sea necesario. La plantilla implementa los recursos siguientes:
   - Función de IAM en Amazon CloudWatch Events

- Función de IAM en CodeBuild proyectos de AWS
- CodeBuild Proyecto AWS
- Regla de CloudWatch eventos de AWS

3. Tome nota del valor de `SourceRoleName` en la pestaña Outputs (Salidas). Lo necesitará para el siguiente paso.
4. Implemente la segunda CloudFormation plantilla en la cuenta de AWS en la que desee copiar las imágenes del contenedor de Amazon ECR. `part-2-destination-account-role.yaml` Actualice los parámetros según sea necesario. En el parámetro `SourceRoleName`, especifique el valor del paso 3. Esta plantilla implementa el rol de IAM multicuenta.
5. Valide la replicación y exclusión de imágenes, tal y como se describe en el último paso de la sección de Epics.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Rotar las credenciales de la base de datos sin reiniciar los contenedores

Documento creado por Josh Joy (AWS)

Entorno: Producción	Tecnologías: contenedores y microservicios; bases de datos; infraestructura DevOps; seguridad, identidad y cumplimiento; gestión y gobierno	Servicios de AWS: Amazon ECS; Amazon Aurora; AWS Fargate; AWS Secrets Manager; Amazon VPC

Resumen

En la nube de Amazon Web Services (AWS), puede usar AWS Secrets Manager para rotar, administrar y recuperar credenciales de bases de datos durante todo su ciclo de vida. Los usuarios y las aplicaciones recuperan secretos mediante una llamada a las API de Secrets Manager, la cual elimina la necesidad de codificar información confidencial en texto sin formato.

Si utiliza contenedores para cargas de trabajo de microservicios, puede almacenar las credenciales de forma segura en AWS Secrets Manager. Para separar la configuración y el código, estas credenciales suelen insertarse en el contenedor. Sin embargo, es importante rotar sus credenciales de forma periódica y automática. También es importante respaldar la posibilidad de actualizar las credenciales después de revocarlas. Al mismo tiempo, las aplicaciones requieren la capacidad de rotar las credenciales y reducir a la vez cualquier posible impacto en las fases posteriores.

Este patrón describe cómo rotar los secretos que están protegidos con AWS Secrets Manager dentro de sus contenedores sin necesidad de reiniciarlos. Además, este patrón reduce el número de búsquedas de credenciales en Secrets Manager mediante el componente de almacenamiento en caché alojado en el cliente de Secrets Manager. Cuando se utiliza el componente de almacenamiento en caché alojado en el cliente para actualizar las credenciales de la aplicación, no es necesario reiniciar el contenedor para recuperar una credencial rotada.

Este enfoque funciona para Amazon Elastic Kubernetes Service (Amazon EKS) y Amazon Elastic Container Service (Amazon ECS).

Se describen dos escenarios. En el escenario de un solo usuario, la credencial de la base de datos se actualiza cuando se produce una rotación secreta al detectar la credencial caducada. La caché del credencial recibe instrucciones para actualizar el secreto y, a continuación, la aplicación restablece la conexión a la base de datos. El componente de almacenamiento en caché alojado en el cliente almacena en caché la credencial dentro de la aplicación y ayuda a evitar el uso de Secrets Manager para cada búsqueda de credenciales. La credencial se rota dentro de la aplicación sin necesidad de forzar la actualización de la credencial reiniciando el contenedor.

El segundo escenario rota el secreto alternando entre dos usuarios. Tener dos usuarios activos reduce la posibilidad de que se produzca un tiempo de inactividad, ya que las credenciales de un usuario están siempre activas. La rotación de credenciales de dos usuarios resulta útil cuando se tiene una implementación grande con clústeres en los que puede haber un pequeño retraso en la propagación de las actualizaciones de credenciales.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una aplicación que se ejecuta en un contenedor de Amazon EKS o Amazon ECS.
- Las credenciales se almacenan en Secrets Manager, con la rotación habilitada.
- Un segundo conjunto de credenciales almacenado en Secrets Manager, si se implementa la solución para dos usuarios. Se pueden encontrar ejemplos de código en el GitHub repositorio aws-secrets-manager-rotation -lambdas.
- Una base de datos de Amazon Aurora.

Limitaciones

- Este ejemplo está dirigido a aplicaciones de Python. Para las aplicaciones Java, puede utilizar el componente de almacenamiento en caché alojado en el cliente de Java o la biblioteca de almacenamiento en caché en el cliente de JDBC para Secrets Manager.

Arquitectura

Arquitectura de destino

Escenario 1: rotación de una credencial para un solo usuario

En el primer escenario, Secrets Manager rota periódicamente una única credencial de base de datos. El contenedor de aplicaciones se ejecuta en Fargate. Cuando se establece la primera conexión a la base de datos, el contenedor de la aplicación obtiene la credencial de base de datos de Aurora. A continuación, el componente de almacenamiento en caché de Secrets Manager almacena en caché la credencial para el futuro establecimiento de la conexión. Una vez transcurrido el período de rotación, la credencial caduca y la base de datos devuelve un error de autenticación. A continuación, la aplicación recupera la credencial rotada, invalida la caché y actualiza la caché de credenciales mediante el componente de almacenamiento en caché alojado en el cliente de Secrets Manager.

En este escenario, es posible que se produzca una interrupción mínima mientras se está rotando la credencial y las conexiones obsoletas están utilizando la credencial obsoleta. Este problema se puede solucionar utilizando el escenario de dos usuarios.

Escenario 2: rotación de una credencial para dos usuarios

En el segundo escenario, Secrets Manager rota periódicamente dos credenciales de usuario (la de Alice y la de Bob) de la base de datos. El contenedor de aplicaciones se ejecuta en el clúster de Fargate. Cuando se establece la primera conexión a la base de datos, el contenedor de la aplicación obtiene la credencial de la base de datos de Aurora para el primer usuario (Alice). A continuación, el componente de almacenamiento en caché de Secrets Manager almacena en caché la credencial para el futuro establecimiento de la conexión.

Aunque hay dos usuarios y credenciales, Secrets Manager solo administra una credencial activa. En este caso, el componente de almacenamiento en caché caduca periódicamente y obtiene la credencial más reciente. Si el período de rotación de Secrets Manager es superior al tiempo de espera de la caché, el componente de almacenamiento en caché recoge la credencial rotada del segundo usuario (Bob). Por ejemplo, si la caducidad de la caché se mide en minutos y el período de rotación se mide en días, el componente de almacenamiento en caché obtiene la nueva credencial como parte de la actualización periódica de la caché. De esta forma, se minimiza el tiempo de inactividad porque la credencial de cada usuario está activa durante una rotación de Secrets Manager.

Automatizar y escalar

Puede usar AWS CloudFormation para implementar este patrón mediante el uso de la infraestructura como código. Esto compila y crea el contenedor de aplicaciones, crea la tarea de Fargate,

implementa el contenedor en Fargate y configura Secrets Manager con Aurora. Para obtener instrucciones de step-by-step implementación, consulte el archivo readme.

Herramientas

Herramientas

- AWS Secrets Manager le permite reemplazar las credenciales codificadas, incluidas las contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto. Dado que Secrets Manager puede rotar automáticamente el secreto según una programación, se pueden reemplazar los secretos a largo plazo por otros a corto plazo, lo que reduce el riesgo de que se filtren.
- Docker: facilita a los desarrolladores empaquetar, enviar y ejecutar cualquier aplicación como un contenedor ligero, portátil y autosuficiente.

Código

Ejemplos de código Python

Este patrón utiliza el componente de almacenamiento en caché alojado en el cliente de Python para que Secrets Manager recupere las credenciales de autenticación al establecer la conexión a la base de datos. El componente de almacenamiento en caché alojado en el cliente ayuda a evitar tener que recurrir a Secrets Manager todas las veces.

Ahora, cuando finalice el período de rotación, la credencial almacenada en caché caducará y, al conectarse a la base de datos, se producirá un error de autenticación. Para MySQL, el código de error de autenticación es 1045. En este ejemplo, se utiliza Amazon Aurora para MySQL, aunque podría utilizarse otro motor, como PostgreSQL. Cuando se produce un error de autenticación, el código de gestión de excepciones de conexión a la base de datos lo detecta. A continuación, informa al componente de almacenamiento en caché alojado en el cliente de Secrets Manager para que actualice el secreto y, a continuación, vuelve a autenticarse y restablecer la conexión con la base de datos. Si se utiliza PostgreSQL u otro motor, se debe buscar el código de error de autenticación correspondiente.

La aplicación del contenedor puede ahora actualizar la contraseña de la base de datos con la contraseña rotada sin necesidad de reiniciar el contenedor.

Colocar el siguiente código en su código de aplicación que gestiona las conexiones a la base de datos. Este ejemplo utiliza Django y subclasifica el backend de la base de datos con un encapsulador

de bases de datos para las conexiones. Si está utilizando un lenguaje de programación o una biblioteca de conexiones de bases de datos diferentes, consulte la biblioteca de conexiones de base de datos para ver cómo subclasificar la recuperación de conexiones de bases de datos.

```
    def get_new_connection(self, conn_params):
        try:
            logger.info("get connection")
            databasecredentials.get_conn_params_from_secrets_manager(conn_params)
            conn =super(DatabaseWrapper,self).get_new_connection(conn_params)
            return conn
        except MySQLdb.OperationalError as e:
            error_code=e.args[0]
            if error_code!=1045:
                raise e

            logger.info("Authentication error. Going to refresh secret and try again.")
            databasecredentials.refresh_now()
            databasecredentials.get_conn_params_from_secrets_manager(conn_params)
            conn=super(DatabaseWrapper,self).get_new_connection(conn_params)
            logger.info("Successfully refreshed secret and established new database
connection.")
            return conn
```

Código de AWS CloudFormation y Python

- https://github.com/aws-samples/ aws-secrets-manager-credential - rotation-without-container-restart

Epics

Mantener la disponibilidad de las aplicaciones durante la rotación de credenciales

Tarea	Descripción	Habilidades requeridas
Instalar el componente de almacenamiento en caché.	Descargue e instale el componente de almacenamiento en caché alojado en el cliente de Secrets Manager para Python. Para ver el enlace de descarga, consulte	Desarrollador

Tarea	Descripción	Habilidades requeridas
	la sección Recursos relaciona dos.	
Guarde en caché la credencia l de trabajo.	Utilice el componente de almacenamiento en caché alojado en el cliente de Secrets Manager para almacenar en caché la credencial de trabajo de forma local.	Desarrollador
Actualice el código de la aplicación para actualizar la credencial en caso de que se produzca un error no autorizad o en la conexión a la base de datos.	Actualice el código de la aplicación para utilizar Secrets Manager con el fin de obtener y actualizar las credenciales de la base de datos. Añada la lógica para gestionar los códigos de error no autorizad os y, a continuación, obtenga la credencial recién rotada. Consulte la sección Ejemplo de código Python.	Desarrollador

Recursos relacionados

Crear un secreto en Secrets Manager

- Crear claves en AWS KMS
- Crear y administrar secretos con AWS Secrets Manager

Crear un clúster de base de datos de Amazon Aurora

- Creación de una instancia de base de datos de Amazon RDS

Crear los componentes de Amazon ECS

- Crear un clúster mediante la consola clásica
- Crear una imagen de Docker
- Creación de un repositorio privado
- Registro privado de Amazon ECR
- Inserción de una imagen de Docker
- Definiciones de tareas de Amazon ECS
- Creación de un servicio de Amazon ECS en la consola clásica

Descargar e instalar el componente de almacenamiento en caché alojado en el cliente de Secrets Manager

- Cliente de almacenamiento en caché de Python

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Ejecute tareas de Amazon ECS en Amazon WorkSpaces con Amazon ECS Anywhere

Documento creado por Akash Kumar (AWS)

Entorno: producción	Tecnologías: contenedores y microservicios; modernización	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon ECS; Amazon WorkSpaces; AWS Directory Service		

Resumen

Amazon Elastic Container Service (Amazon ECS) Anywhere permite la implementación de tareas de Amazon ECS en cualquier entorno, incluida la infraestructura administrada por Amazon Web Services (AWS) y la infraestructura administrada por el cliente. Esto se puede hacer al tiempo que se utiliza un plano de control totalmente administrado por AWS que se ejecuta en la nube y que está siempre actualizado.

Las empresas suelen utilizar Amazon WorkSpaces para desarrollar aplicaciones basadas en contenedores. Para ello era necesario utilizar Amazon Elastic Compute Cloud (Amazon EC2) o AWS Fargate con un clúster de Amazon ECS para probar y ejecutar tareas de ECS. Ahora, con Amazon ECS Anywhere, puede añadir Amazon WorkSpaces como instancias externas directamente a un clúster de ECS y ejecutar sus tareas directamente. Esto reduce el tiempo de desarrollo, ya que puede probar su contenedor con un clúster de ECS localmente en Amazon WorkSpaces. También puede ahorrar el costo de utilizar instancias EC2 o Fargate para probar sus aplicaciones de contenedores.

Este patrón muestra cómo implementar tareas de ECS en Amazon WorkSpaces con Amazon ECS Anywhere. Configura el clúster de ECS y utiliza AWS Directory Service Simple AD para lanzar el WorkSpaces. A continuación, la tarea ECS de ejemplo lanza NGINX en. WorkSpaces

Requisitos previos y limitaciones

- Una cuenta de AWS activa

- Interfaz de la línea de comandos de AWS (AWS CLI)
- Credenciales de AWS configuradas en su máquina

Arquitectura

Pila de tecnología de destino

- Una nube privada virtual (VPC)
- Clúster de Amazon ECS
- Amazon WorkSpaces
- AWS Directory Service con AD Connector

Arquitectura de destino

La arquitectura incluye los siguientes servicios y recursos:

- Un clúster de ECS con subredes públicas y privadas en una VPC personalizada
- Simple AD en la VPC para proporcionar a los usuarios acceso a Amazon WorkSpaces
- Amazon WorkSpaces aprovisionó en la VPC mediante Simple AD
- AWS Systems Manager activado para añadir Amazon WorkSpaces como instancias gestionadas
- Con Amazon ECS y AWS Systems Manager Agent (SSM Agent), Amazon WorkSpaces agregó a Systems Manager y al clúster de ECS
- Un ejemplo de tarea de ECS para ejecutar WorkSpaces en el clúster de ECS

Herramientas

- AWS Directory Service Simple Active Directory (Simple AD) es un directorio administrado de manera autónoma que utiliza tecnología de un servidor compatible con Active Directory de Samba 4. Simple AD ofrece un subconjunto de las características que ofrece AWS Managed Microsoft AD, incluida la capacidad de gestionar los usuarios y conectarse de forma segura a las instancias de Amazon EC2.

- Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores escalable y rápido que ayuda a ejecutar, detener y administrar contenedores en un clúster.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Systems Manager le permite administrar las aplicaciones y la infraestructura que se ejecutan en la nube de AWS. Systems Manager simplifica la administración de aplicaciones y recursos, reduce el tiempo requerido para detectar y resolver problemas operativos y ayuda a utilizar y administrar los recursos de a escala de manera segura.
- Amazon le WorkSpaces ayuda a aprovisionar escritorios Microsoft Windows o Amazon Linux virtuales basados en la nube para sus usuarios, conocidos como WorkSpaces. WorkSpaces elimina la necesidad de adquirir e implementar hardware o instalar software complejo.

Epics

Configurar el clúster de ECS

Tarea	Descripción	Habilidades requeridas
Crear y configurar el clúster de ECS.	Para crear el clúster de ECS, siga las instrucciones que figuran en la Documentación de AWS, que incluyen los siguientes pasos: • En Seleccione la compatibi lidad de clústeres, elija Solo redes, que admitirá Amazon WorkSpace como instancia externa al clúster de ECS. • Elija crear una nueva VPC.	Arquitecto de la nube

Lanza Amazon WorkSpaces

Tarea	Descripción	Habilidades requeridas
Configura Simple AD y lanza Amazon WorkSpaces.	Para aprovisionar un directorio de Simple AD para su VPC recién creada e iniciar Amazon WorkSpaces, siga las instrucciones de la documentación de AWS.	Arquitecto de la nube

Configuración de AWS Systems Manager para entornos híbridos

Tarea	Descripción	Habilidades requeridas
Descargar los scripts adjuntos.	En su máquina local, descargue los archivos `ssm-trust-policy.json` y `ssm-activation.json` que se encuentran en la sección Archivos adjuntos.	Arquitecto de la nube
Agregar el rol de IAM.	Añadir variables de entorno en función de los requisitos de su empresa. `export AWS_DEFAULT_REGION=${AWS_REGION_ID}` `export ROLE_NAME=${ECS_TASK_ROLE}` `export CLUSTER_NAME=${ECS_CLUSTER_NAME}` `export SERVICE_NAME=${ECS_CLUSTER_SERVICE_NAME}` Ejecutar el siguiente comando.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	`aws iam create-role --role-name $ROLE_NAME --assume-role-policy-document file://ssm-trust-policy.json`	
Añada la ManagedInstanceCore política de AmazonSSM a la función de IAM.	Ejecutar el siguiente comando. `aws iam attach-role-policy --role-name $ROLE_NAME --policy-arn arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore`	Arquitecto de la nube
Agregue la política EC2Role de ContainerServicefor AmazonEC2 a la función de IAM.	Ejecutar el siguiente comando. `aws iam attach-role-policy --role-name $ROLE_NAME --policy-arn arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role`	Arquitecto de la nube
Comprobar el rol de IAM.	Para verificar el rol de IAM, ejecute el siguiente comando. `aws iam list-attached-role-policies --role-name $ROLE_NAME`	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Activar Systems Manager.	Ejecutar el siguiente comando. `aws ssm create-activation --iam-role $ROLE_NAME | tee ssm-activation.json`	Arquitecto de la nube

Añádala al clúster de ECS WorkSpaces

Tarea	Descripción	Habilidades requeridas
Conéctese a su WorkSpaces.	Para conectarse a sus Workspaces y configurarlos, siga las instrucciones que figuran en la Documentación de AWS.	Desarrollador de aplicaciones
Descargar el script de instalación ecs-anywhere.	En el símbolo del sistema, ejecute el siguiente comando. `curl -o "ecs-anywhere-install.sh" "https://amazon-ecs-agent-packages-preview.s3.us-east-1.amazonaws.com/ecs-anywhere-install.sh" && sudo chmod +x ecs-anywhere-install.sh`	Desarrollador de aplicaciones
Comprobar la integridad del script del intérprete de comandos.	Ejecutar el siguiente comando (opcional). `curl -o "ecs-anywhere-install.sh.sha256" "https://amazon-ec`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`s-agent-packages-preview.s3.us-east-1.amazonaws.com/ecs-anywhere-install.sh.sha256" && sha256sum -c ecs-anywhere-install.sh.sha256`	
Agregar un repositorio EPEL en Amazon Linux.	Para agregar un repositorio Extra Packages for Enterprise Linux (EPEL), ejecute el comando `sudo amazon-linux-extras install epel -y`.	Desarrollador de aplicaciones
Instalar Amazon ECS Anywhere.	Para ejecutar el script de instalación, utilice el siguiente comando. `sudo ./ecs-anywhere-install.sh --cluster $CLUSTER_NAME --activation-id $ACTIVATION_ID --activation-code $ACTIVATION_CODE --region $AWS_REGION`	

Tarea	Descripción	Habilidades requeridas
Comprobar la información de la instancia desde el clúster de ECS.	Para comprobar la información de las instancias del clúster de Systems Manager y ECS y validar las que WorkSpaces se agregaron al clúster, ejecute el siguiente comando desde su máquina local. `aws ssm describe-instance-information" && "aws ecs list-container-instances --cluster $CLUSTER_NAME`	Desarrollador de aplicaciones

Agregue una tarea de ECS para el WorkSpaces

Tarea	Descripción	Habilidades requeridas
Para crear un rol de IAM de ejecución de tareas.	Descargue `task-execution-assume-role.json` y `external-task-definition.json` desde la sección Archivos adjuntos. Ejecute el siguiente comando en su equipo local. `aws iam --region $AWS_DEFAULT_REGION create-role --role-name $ECS_TASK_EXECUTION_ROLE --assume-role-policy-document file://ta`	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	`sk-execution-assume-role.json`	
Agregue la política al rol de ejecución.	Ejecutar el siguiente comando. `aws iam --region $AWS_DEFAULT_REGION attach-role-policy --role-name $ECS_TASK_EXECUTION_ROLE --policy-arn arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy`	Arquitecto de la nube
Crear un rol de tarea.	Ejecutar el siguiente comando. `aws iam --region $AWS_DEFAULT_REGION create-role --role-name $ECS_TASK_EXECUTION_ROLE --assume-role-policy-document file://task-execution-assume-role.json`	Arquitecto de la nube
Registrar la definición de tareas en el clúster.	Ejecute el siguiente comando en su equipo local. `aws ecs register-task-definition --cli-input-json file://external-task-definition.json`	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Ejecutar la tarea.	Ejecute el siguiente comando en su equipo local. `aws ecs run-task --cluster $CLUSTER_NAME --launch-type EXTERNAL --task-definition nginx`	Arquitecto de la nube
Validar el estado de ejecución de la tarea.	Para obtener el ID de la tarea, ejecute el siguiente comando. `export TEST_TASKID=$(aws ecs list-tasks --cluster $CLUSTER_NAME | jq -r '.taskArns[0]')` Ejecute el siguiente comando con el ID de la tarea. `aws ecs describe-tasks --cluster $CLUSTER_NAME --tasks ${TEST_TASKID}`	Arquitecto de la nube
Compruebe la tarea en WorkSpace.	Para comprobar que NGINX se está ejecutando en WorkSpace, ejecute el comando. `curl http://localhost:8080`	Desarrollador de aplicaciones

Recursos relacionados

- Clúster de ECS
- Configurar un entorno híbrido

- Amazon WorkSpaces
- AD sencillo

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Ejecute un contenedor de Docker de la API web de ASP.NET Core en una instancia Linux de Amazon EC2

Creado por Vijai Anand Ramalingam (AWS) y Sreelaxmi Pai (AWS)

Entorno: PoC o piloto	Tecnologías: contenedores y microservicios; desarrollo y pruebas de software; aplicaciones web y móviles	Carga de trabajo: Microsoft
Servicios de AWS: Amazon EC2; Elastic Load Balancing (ELB)		

Resumen

Este patrón es para personas que están empezando a colocar en contenedores sus aplicaciones en la nube de Amazon Web Services (AWS). Cuando empiezaa a colocar aplicaciones en contenedores en la nube, normalmente no hay ninguna plataforma de orquestación de contenedores configurada. Este patrón le ayuda a configurar rápidamente la infraestructura en AWS para probar sus aplicaciones en contenedores sin necesidad de una infraestructura compleja de orquestación de contenedores.

El primer paso en el proceso de modernización es transformar la aplicación. Si se trata de una aplicación antigua de .NET Framework, primero debe cambiar el tiempo de ejecución a ASP.NET Core. A continuación, proceda del modo siguiente:

- Cree la imagen del contenedor de Docker
- Ejecute el contenedor de Docker con la imagen compilada
- Valide la aplicación antes de implementarla en cualquier plataforma de orquestación de contenedores, como Amazon Elastic Container Service (Amazon ECS) o Amazon Elastic Kubernetes Service (Amazon EKS).

Este patrón cubre los aspectos de compilación, ejecución y validación del desarrollo de aplicaciones modernas en una instancia Linux de Amazon Elastic Compute Cloud (Amazon EC2).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de Amazon Web Services (AWS) activa
- Un rol de AWS Identity and Access Management (IAM) con acceso suficiente para crear recursos de AWS para este patrón
- Se descargó e instaló Visual Studio Community 2022 o posterior
- Un proyecto de .NET Framework modernizado a ASP.NET Core
- Un repositorio GitHub

Versiones de producto

- Visual Studio Community 2022 o posterior

Arquitectura

Arquitectura de destino

Este patrón utiliza una CloudFormation plantilla de AWS para crear la arquitectura de alta disponibilidad que se muestra en el siguiente diagrama. Se lanza una instancia Linux Amazon EC2 en una subred privada. El administrador de sesiones de AWS Systems Manager se utiliza para acceder a la instancia privada de Amazon EC2 Linux y con el objetivo de probar la API que se ejecuta en el contenedor de Docker.

1. Acceso a la instancia de Linux a través de Session Manager

Herramientas

Servicios de AWS

- Interfaz de la línea de comandos de AWS: la Interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su shell de línea de comandos. Con una configuración mínima, puede

utilizar comandos de CLI de AWS que implementen una funcionalidad equivalente a la que ofrece la consola de administración de AWS basada en navegador.

- Consola de administración de AWS: la consola de administración de AWS es una aplicación web que engloba y hace referencia a un amplio conjunto de consolas de servicios para la administración de recursos de AWS. La primera vez que inicie sesión, verá la página de inicio de la consola. La página de inicio proporciona acceso a la consola de cada servicio y ofrece un único lugar para acceder a la información que necesita para realizar sus tareas relacionadas con AWS.
- Administrador de sesiones de AWS Systems Manager: el administrador de sesiones es una funcionalidad de AWS Systems Manager totalmente gestionada. Con el administrador de sesiones, puede gestionar las instancias de Amazon Elastic Compute Cloud (Amazon EC2). El administrador de sesiones proporciona una administración de nodos segura y auditable sin necesidad de abrir puertos de entrada, mantener los hosts bastiones ni administrar las claves SSH.

Otras herramientas

- Visual Studio 2022: Visual Studio 2022 es un entorno de desarrollo integrado (IDE).
- Docker: Docker es un conjunto de productos de plataforma como servicio (PaaS) que utiliza la virtualización a nivel del sistema operativo para entregar software en contenedores.

Código

```
FROM mcr.microsoft.com/dotnet/aspnet:5.0 AS base
 WORKDIR /app
EXPOSE 80
EXPOSE 443

FROM mcr.microsoft.com/dotnet/sdk:5.0 AS build
WORKDIR /src
COPY ["DemoNetCoreWebAPI/DemoNetCoreWebAPI.csproj", "DemoNetCoreWebAPI/"]
RUN dotnet restore "DemoNetCoreWebAPI/DemoNetCoreWebAPI.csproj"
COPY . .
WORKDIR "/src/DemoNetCoreWebAPI"
RUN dotnet build "DemoNetCoreWebAPI.csproj" -c Release -o /app/build

FROM build AS publish
RUN dotnet publish "DemoNetCoreWebAPI.csproj" -c Release -o /app/publish

FROM base AS final
WORKDIR /app
```

```
COPY --from=publish /app/publish .
ENTRYPOINT ["dotnet", "DemoNetCoreWebAPI.dll"]
```

Epics

Desarrollar la API web de ASP.NET Core

Tarea	Descripción	Habilidades requeridas
Cree un ejemplo de API web de ASP.NET Core con Visual Studio.	Para crear una API web de ASP.NET Core de ejemplo, haga lo siguiente: 1. Open Visual Studio 2022. 2. Elija Crear un proyecto nuevo. 3. Seleccione la plantilla de proyecto de la API web de ASP.NET Core y elija Siguiente. 4. Para el nombre del proyecto, introduzca DemoNetCoreWebAPI y elija Siguiente. 5. Seleccione Crear. 6. Para ejecutar el proyecto localmente, presione F5. 7. Compruebe que el punto final de la WeatherFo recastAPI predeterminado devuelva los resultados mediante Swagger. 8. Abra la línea de comandos, vaya a la carpeta del proyecto .csproj y ejecute los siguientes comandos	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	para enviar la nueva API web a su repositorio. GitHub `git add --all` `git commit -m “Initial Version”` `git push`	

Tarea	Descripción	Habilidades requeridas
Cree un Dockerfile.	Para crear un archivo Dockerfile, realice una de las siguientes acciones: • Cree el archivo Dockerfile manualmente usando el Dockerfile de ejemplo de la sección Código. Según los requisitos, seleccione la imagen base de .NET adecuada. Para obtener información sobre las imágenes relacionadas con .NET y ASP.NET Core, consulte Centro Docker. • Cree el archivo Dockerfile con Visual Studio y Escritorio Docker. En el explorador de soluciones, haga clic con el botón derecho del proyecto y seleccione Agregar -> Soporte Docker. Para OS de destino, seleccione Linux. Asegúrese de que el nuevo Dockerfile esté en la misma ruta que el archivo de la solución (.sln). Para enviar los cambios a tu GitHub repositorio, ejecuta el siguiente comando. `git add --all`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`git commit -m “Dockerfile added”` `git push`	

Configurar la instancia de Amazon EC2

Tarea	Descripción	Habilidades requeridas
Configure la infraestructura.	Lance la CloudFormation plantilla de AWS para crear la infraestructura, que incluye lo siguiente: • Una nube privada virtual (VPC), que utiliza la Introducción a VPC de AWS, con dos subredes públicas y dos subredes privadas que abarcan dos zonas de disponibilidad. • El rol de IAM necesario para habilitar AWS Systems Manager. • En una de las subredes privadas, una instancia de demostración de Amazon Linux 2 con el agente SSM más reciente. Aunque esta instancia no tiene conectividad directa desde Internet, se puede acceder a ella de forma segura mediante el administrador de sesiones de AWS Systems Manager	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	sin necesidad de un host bastión. Para obtener más informaci ón sobre cómo acceder a una instancia privada de Amazon EC2 mediante Session Manager sin necesidad de un host bastión, consulte la entrada del blog Toward a bastion-less world.	
Inicie sesión en la instancia Linux de Amazon EC2.	Para conectarse a la instancia Linux de Amazon EC2 en la subred privada, haga lo siguiente: 1. Abra la consola de Amazon EC2. 2. En el panel de navegación, seleccione Instancias. 3. Seleccione la instancia de demostración de Amazon Linux 2 y elija Conectarse. 4. Elija Session Manager. 5. Elija Conectarse para abrir una nueva ventana de terminal. 6. Ejecute el siguiente comando de la . `sudo su`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Instale e inicie Docker.	Para instalar e iniciar Docker en la instancia Linux de Amazon EC2, haga lo siguiente: 1. Para instalar Docker, ejecute el siguiente comando. `yum install -y docker` 2. Para iniciar el servicio Docker, ejecute el comando siguiente. `service docker start` 3. Para verificar la instalación de Docker, ejecute el siguiente comando. `docker info`	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
Instale GitHub y clone el repositorio.	Para instalar Git en la instancia Linux Amazon EC2 y clonar el repositorio desde ella GitHub, haga lo siguiente. 1. Para instalar Git, ejecute el siguiente comando. `yum install git -y` 2. Para clonar el repositor io, ejecute el siguiente comando. `git clone https://g ithub.com/<usernam e>/<repo-name>.git` 3. Para ir al Dockerfile, ejecute el siguiente comando. `cd <repo-name>/DemoNe tCoreWebAPI/`	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
Cree y ejecute el contenedor de Docker.	Para crear la imagen de Docker y ejecutar el contenedor dentro de la instancia de Linux Amazon EC2, haga lo siguiente: 1. Para crear la imagen de Docker, ejecute el siguiente comando. `docker build -t aspnetcorewebapiimage -f Dockerfile .` 2. Para ver todas las imágenes de Docker, ejecute el siguiente comando. `docker images` 3. Para crear y ejecutar el contenedor, ejecute el siguiente comando. `docker run -d -p 80:80 --name aspnetcorewebapicontainer aspnetcorewebapiimage`	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps

Pruebe la API web

Tarea	Descripción	Habilidades requeridas
Pruebe la API web con el comando curl.	Para probar la API web, ejecute el siguiente comando. `curl -X GET "http://localhost/WeatherForecast" -H  "accept: text/plain"` Verifique la respuesta de la API. Nota: Puede obtener los comandos curl para cada punto de conexión de Swagger cuando lo ejecuta localmente.	Desarrollador de aplicaciones

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Elimine todos los recursos.	Eliminar la pila para eliminar todos los recursos. Esto asegura que no se le cobre por ningún servicio que no utilice.	Administrador de AWS, AWS DevOps

Recursos relacionados

- Conectarse a la instancia de Linux desde Windows mediante PuTTY
- Crear una API web con ASP.NET Core
- Toward a bastion-less world

Ejecute cargas de trabajo basadas en mensajes a escala con AWS Fargate

Creado por Stan Zubarev (AWS)

Entorno: PoC o piloto	Tecnologías: contenedores y microservicios; mensajería y comunicaciones; bases de datos	Servicios de AWS: AWS Fargate; Amazon SQS; Amazon DynamoDB

Resumen

Este patrón muestra cómo ejecutar cargas de trabajo basadas en mensajes a escala en la nube de AWS mediante contenedores y AWS Fargate.

El uso de contenedores para procesar datos puede resultar útil cuando la cantidad de datos que procesa una aplicación supera las limitaciones de los servicios de computación sin servidor basados en funciones. Por ejemplo, si una aplicación requiere más capacidad de procesamiento o tiempo de procesamiento que los que ofrece AWS Lambda, el uso de Fargate puede mejorar el rendimiento.

El siguiente ejemplo de configuración utiliza el AWS Cloud Development Kit (AWS CDK) TypeScript para configurar e implementar los siguientes recursos en la nube de AWS:

- Un servicio de Fargate
- La cola de Amazon Simple Queue Service (Amazon SQS)
- La tabla de Amazon DynamoDB.
- Un CloudWatch panel de Amazon

El servicio Fargate recibe y procesa los mensajes de la cola de Amazon SQS y, a continuación, los almacena en la tabla Amazon DynamoDB. Puede monitorizar cuántos mensajes de Amazon SQS se procesan y cuántos elementos de DynamoDB crea Fargate mediante el panel de control. CloudWatch

Nota: También puede utilizar el código de ejemplo de este patrón para crear cargas de trabajo de procesamiento de datos más complejas en arquitecturas sin servidor basadas en eventos. Para

obtener más información, consulte Ejecute cargas de trabajo programadas y basadas en eventos a escala con AWS Fargate.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- La última versión de la interfaz de la línea de comandos de AWS (AWS CLI), instalada y configurada en su máquina local.
- Git, instalado y configurado en la máquina local.
- La AWS CDK, instalada y configurada en la máquina local.
- Go, instalado y configurada en la máquina local.
- Docker, instalado y configurado en la máquina local.

Arquitectura

Pila de tecnología de destino

- Amazon SQS
- AWS Fargate
- Amazon DynamoDB

Arquitectura de destino

El siguiente diagrama muestra un ejemplo de flujo de trabajo para ejecutar cargas de trabajo basadas en mensajes a escala en la nube de AWS mediante Fargate:

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El servicio Fargate utiliza el sondeo largo de Amazon SQS para recibir mensajes de una cola de Amazon SQS.
2. A continuación, el servicio Fargate procesa los mensajes de Amazon SQS y los almacena en una tabla DynamoDB.

Automatizar y escalar

Para automatizar el escalado del recuento de tareas de Fargate, puede configurar el servicio de escalado automático de Amazon Elastic Container Service (Amazon ECS). Se recomienda configurar la política de escalado en función del número de mensajes visibles en la cola de Amazon SQS de la aplicación.

Para obtener más información, consulte Escalado en función de Amazon SQS en la guía del usuario de Amazon EC2 Auto Scaling.

Herramientas

Servicios de AWS

- AWS Fargate le permite ejecutar contenedores sin necesidad de administrar servidores o instancias de Amazon Elastic Compute Cloud (Amazon EC2). Se utiliza en conjunto con Amazon Elastic Container Service (Amazon ECS).
- Amazon Simple Queue Service (Amazon SQS) ofrece una cola alojada segura, duradera y disponible que le permite integrar y desacoplar sistemas y componentes de software distribuidos.
- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- Amazon le CloudWatch ayuda a monitorizar las métricas de sus recursos de AWS y las aplicaciones que ejecuta en AWS en tiempo real.

Código

El código de este patrón está disponible en el repositorio GitHub sqs-fargate-ddb-cdk-go.

Epics

Cree e implemente los recursos mediante la AWS CDK

Tarea	Descripción	Habilidades requeridas
Clona el GitHub repositorio.	Clone el repositorio GitHub sqs-fargate-ddb-cdk-go en su máquina local ejecutando el siguiente comando:	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`git clone https://github.com/aws-samples/sqs-fargate-ddb-cdk-go.git`	
Compruebe que la CLI de AWS esté configurada en la cuenta de AWS correcta y que la AWS CDK tenga los permisos necesarios.	Para comprobar si los ajustes de configuración de la CLI de AWS son correctos, ejecute el siguiente comando ls de Amazon Simple Storage Service (Amazon S3): `aws s3 ls` Este procedimiento también requiere que la CDK de AWS tenga permisos para aprovisionar la infraestructura en su cuenta de AWS. Para conceder los permisos necesarios, debe crear un perfil de AWS con nombre en la CLI de AWS y exportarlo como una variable de entorno AWS_PROFILE. Nota: Si no ha utilizado anteriormente la CDK de AWS en su cuenta de AWS, primero debe aprovisionar los recursos de la CDK de AWS necesarios. Para obtener más información, consulte Proceso de arranque en la Guía para desarrolladores de AWS CDK v2.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Implemente la pila de AWS CDK en su cuenta de AWS.	1. Ejecute el siguiente comando de la CLI de AWS para crear una imagen de contenedor: `docker build -t go-fargate .` 2. Ejecute el siguiente comando para abrir el directorio CDK de AWS: `cd cdk` 3. Instale los módulos npm requeridos para ejecutar el siguiente comando: `npm i` 4. Implemente el patrón CDK de AWS en su cuenta de AWS ejecutando el siguiente comando: `cdk deploy --profile ${AWS_PROFILE}`	Desarrollador de aplicaciones

Prueba de la configuración

Tarea	Descripción	Habilidades requeridas
Envíe un mensaje de prueba a la cola de Amazon SQS.	Para obtener instrucciones, consulte Enviar mensajes a una cola (consola) en la Guía para desarrolladores de Amazon SQS.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	Ejemplo de mensaje de prueba de Amazon SQS `{ "message": "hello, Fargate" }`	
Compruebe que el mensaje de prueba aparezca en los registros del CloudWatch servicio Fargate.	Siga las instrucciones de Visualización de CloudWatch registros de la Guía para desarrolladores de Amazon ECS. Asegúrese de revisar los registros del grupo de go-fargate-serviceregistros del clúster de go-service-cluster ECS.	Desarrollador de aplicaciones
Compruebe que el mensaje de prueba aparece en la tabla de DynamoDB.	1. Abra la consola de DynamoDB. 2. En el panel de navegación izquierdo, elija Tables (Tablas). Luego, seleccione la siguiente tabla de la lista: sqs-fargate-ddb-table. 3. Elija Explorar elementos de la tabla. 4. Compruebe que el mensaje de prueba aparece en la lista de Artículos devueltos.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Compruebe que el servicio Fargate envíe mensajes a CloudWatch Logs.	1. Abra la consola de CloudWatch . 2. En el panel de navegación izquierdo, elija Dashboard (Paneles). 3. En la lista de paneles personalizados, seleccione el panel denominado. go-service-dashboard 4. Compruebe que el mensaje de prueba aparece en los registros. Nota: La AWS CDK crea el CloudWatch panel de control en su cuenta de AWS automáticamente.	Desarrollador de aplicaciones

Limpieza

Tarea	Descripción	Habilidades requeridas
Elimine la pila de CDK de AWS.	1. Abra el directorio AWS CDK en la CLI de AWS ejecutando el siguiente comando: `cd cdk` 2. Elimine la pila AWS CDK ejecutando el siguiente comando:	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`cdk destroy --profile ${AWS_PROFILE}`	
Compruebe que se haya eliminado la pila de CDK de AWS.	Para asegurarse de que se eliminó la pila, ejecute el siguiente comando: `aws cloudformation list-stacks --query \ "StackSummaries[?contains(StackName,'SqsFargate')].StackStatus" \ --profile ${AWS_PROFILE}` El valor `StackStatus` devuelto en el resultado del comando es `DELETE_COMPLETE` si se elimina la pila. Para obtener más información, consulte Describir y enumerar sus pilas en la Guía del CloudFormation usuario de AWS.	Desarrollador de aplicaciones

Recursos relacionados

- Configuración de la CLI de AWS (Guía del usuario de la CLI de AWS versión 2)
- Referencia de API (referencia de API de AWS CDK)
- AWS SDK para Go v2 (documentación de Go)

Ejecutar cargas de trabajo con estado y almacenamiento de datos persistente mediante Amazon EFS en Amazon EKS con AWS Fargate

Creado por Ricardo Morais (AWS), Rodrigo Bersa (AWS) y Lucio Pereira (AWS)

Repositorio de código: Amazon EKS con Fargate y Amazon EFS	Entorno: PoC o piloto	Tecnologías: contenedores y microservicios; almacenamiento y copia de seguridad
Carga de trabajo: código abierto	Servicios de AWS: Amazon EFS; Amazon EKS; AWS Fargate	

Resumen

Este patrón proporciona orientación para habilitar Amazon Elastic File System (Amazon EFS) como dispositivo de almacenamiento para contenedores que se ejecutan en Amazon Elastic Kubernetes Service (Amazon EKS) mediante AWS Fargate para aprovisionar sus recursos informáticos.

La configuración descrita en este patrón sigue las prácticas recomendadas de seguridad y proporciona seguridad en reposo y seguridad en tránsito de forma predeterminada. Para cifrar su sistema de archivos Amazon EFS, utiliza una clave de AWS Key Management Service (AWS KMS), pero también puede especificar un alias de clave que gestione el proceso de creación de una clave de KMS.

Puede seguir los pasos de este patrón para crear un espacio de nombres y un perfil de Fargate para una aplicación proof-of-concept (PoC), instalar el controlador Amazon EFS Container Storage Interface (CSI) que se utiliza para integrar el clúster de Kubernetes con Amazon EFS, configurar la clase de almacenamiento e implementar la aplicación PoC. Estos pasos dan como resultado un sistema de archivos Amazon EFS que se comparte entre varias cargas de trabajo de Kubernetes y se ejecuta en Fargate. El patrón va acompañado de scripts que automatizan estos pasos.

Puede utilizar este patrón si desea que los datos persistan en sus aplicaciones contenerizadas y si desea evitar la pérdida de datos durante las operaciones de escalado. Por ejemplo:

- DevOps herramientas: un escenario habitual es desarrollar una estrategia de integración y entrega continuas (CI/CD). En este caso, puede utilizar Amazon EFS como un sistema de archivos compartido para almacenar configuraciones entre distintas instancias de la herramienta de CI/CD o para almacenar una memoria caché (por ejemplo, un repositorio de Apache Maven) para las etapas de canalización entre distintas instancias de la herramienta de CI/CD.
- Servidores web: un escenario común es utilizar Apache como servidor web HTTP. Puede utilizar Amazon EFS como un sistema de archivos compartidos para almacenar archivos estáticos que se comparten entre distintas instancias del servidor web. En este escenario de ejemplo, las modificaciones se aplican directamente al sistema de archivos en lugar de incluir los archivos estáticos en una imagen de Docker.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un clúster de Amazon EKS existente con Kubernetes versión 1.17 o posterior (probado hasta la versión 1.27)
- Un sistema de archivos Amazon EFS existente para vincular un Kubernetes StorageClass y aprovisionar sistemas de archivos de forma dinámica
- Permisos de administración de clústeres
- El contexto está configurado para apuntar al clúster de Amazon EKS deseado

Limitaciones

- Hay algunas limitaciones que se deben tener en cuenta al utilizar Amazon EKS con Fargate. Por ejemplo, no se admite el uso de algunas construcciones de Kubernetes, como los contenedores DaemonSets privilegiados. Para obtener más información sobre las limitaciones de Fargate, consulte las consideraciones sobre AWS Fargate en la documentación de Amazon EKS.
- El código que se proporciona con este patrón es compatible con estaciones de trabajo que ejecutan Linux o macOS.

Versiones de producto

- Interfaz de la línea de comandos de AWS (AWS CLI) versión 2 o posterior

- Controlador Amazon EFS CSI versión 1.0 o posterior (probado hasta la versión 2.4.8)
- eksctl versión 0.24.0 o posterior (probado hasta la versión 0.158.0)
- jq versión 1.6 o posterior
- kubectl versión 1.17 o posterior (probado hasta la versión 1.27)
- Kubernetes versión 1.17 o posterior (probado hasta la versión 1.27)

Arquitectura

La arquitectura de destino se compone de la siguiente infraestructura:

- Una nube privada virtual (VPC)
- Dos zonas de disponibilidad
- Una subred pública con una puerta de enlace NAT que proporciona acceso a Internet
- Una subred privada con un clúster de Amazon EKS y objetivos de montaje de Amazon EFS (también conocidos como puntos de montaje)
- Amazon EFS a nivel de VPC

La siguiente es la infraestructura del entorno del clúster de Amazon EKS:

- Perfiles de AWS Fargate que admiten las construcciones de Kubernetes a nivel de espacio de nombres
- Un espacio de nombres de Kubernetes con:
  - Dos módulos de aplicaciones distribuidos en las zonas de disponibilidad
  - Una reclamación de volumen persistente (PVC) vinculada a un volumen persistente (PV) a nivel de clúster
- Un PV de todo el clúster que esté enlazado al PVC del espacio de nombres y que apunte a los objetivos de montaje de Amazon EFS en la subred privada, fuera del clúster

Herramientas

Servicios de AWS

- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que puede utilizar para interactuar con los servicios de AWS desde la línea de comandos.
- Amazon Elastic File System (Amazon EFS) le ayuda a crear y configurar sistemas de archivos compartidos en la nube de AWS. Siguiendo este patrón, proporciona un sistema de archivos simple, escalable, completamente administrado y compartido para su uso con Amazon EKS.
- Amazon Elastic Kubernetes Service (Amazon EKS) le ayuda a ejecutar Kubernetes en AWS sin necesidad de instalar ni operar sus propios clústeres.
- AWS Fargate es un motor de cómputo sin servidor para Amazon EKS. Crea y administra recursos de computación para sus aplicaciones de Kubernetes.
- AWS Key Management Service (AWS KMS) facilita poder crear y controlar claves criptográficas para proteger los datos.

Otras herramientas

- Docker es un conjunto de productos de plataforma como servicio (PaaS) que utiliza la virtualización a nivel del sistema operativo para entregar software en contenedores.
- eksctl: es una utilidad sencilla de línea de comandos para crear y administrar clústeres de Kubernetes en Amazon EKS.
- kubectl: una interfaz de la línea de comandos que le ayuda en la ejecución de comandos en clústeres de Kubernetes.
- jq es una herramienta de línea de comandos para analizar JSON.

Código

El código de este patrón se proporciona en la configuración de GitHub persistencia con Amazon EFS en Amazon EKS mediante el repositorio de AWS Fargate. Los scripts están organizados por epic, agrupados en carpetas `epic01`–`epic06`, según el orden de la sección Epics de este patrón.

Prácticas recomendadas

La arquitectura de destino incluye los siguientes servicios y componentes, y sigue las prácticas recomendadas de AWS Well-Architected Framework:

- Amazon EFS, que proporciona un sistema de archivos NFS elástico, simple, escalable y completamente administrado. Se utiliza como un sistema de archivos compartido entre todas las

replicaciones de la aplicación PoC que se ejecutan en pods, que se distribuyen en las subredes privadas del clúster de Amazon EKS elegido.

- Un destino de montaje de Amazon EFS para cada subred privada. Esto proporciona redundancia por zona de disponibilidad dentro de la nube privada virtual (VPC) del clúster.
- Amazon EKS, que ejecuta las cargas de trabajo de Kubernetes. Debe aprovisionar un clúster de Amazon EKS antes de utilizar este patrón, tal y como se describe en la sección Requisitos previos.
- AWS KMS, que proporciona cifrado en reposo para el contenido almacenado en el sistema de archivos Amazon EFS.
- Fargate, que administra los recursos informáticos de los contenedores para que pueda centrarse en los requisitos empresariales y no en la carga de la infraestructura. El perfil de Fargate se crea para todas las subredes privadas. Esto proporciona redundancia por zona de disponibilidad dentro de la nube privada virtual (VPC) del clúster.
- Kubernetes Pods, para validar que distintas instancias de una aplicación pueden compartir, consumir y escribir contenido.

Epics

Aprovisionar un clúster de Amazon EKS (opcional)

Tarea	Descripción	Habilidades requeridas
Cree un clúster de Amazon EKS.	Si ya tiene un clúster implementado, pase a la siguiente etapa. Cree un clúster de Amazon EKS en su cuenta de AWS existente. En el directorio GitHub Repo, utilice uno de los patrones para implementar un clúster de Amazon EKS mediante Terraform o eksctl. Para obtener más información, consulte Creación de un clúster de Amazon EKS en la documentación de	Administrador de AWS, administrador de Terraform o eksctl, administrador de Kubernetes

Tarea	Descripción	Habilidades requeridas
	Amazon EKS. Nota: En el patrón Terraform, también hay ejemplos que muestran cómo: vincular los perfiles de Fargate a su clúster de Amazon EKS, crear un sistema de archivos Amazon EFS e implementar el controlador CSI de Amazon EFS en su clúster de Amazon EKS.	

Tarea	Descripción	Habilidades requeridas
Exporte variables de entorno.	Ejecute el script env.sh. Esto proporciona la informaci ón necesaria en los pasos siguientes. `source ./scripts/env.sh` `Inform the AWS Account ID: <13-digit-account-id>` `Inform your AWS Region: <aws-Region-code>` `Inform your Amazon EKS Cluster Name: <amazon-eks-cluster-name>` `Inform the Amazon EFS Creation Token: <self-genereated-uuid>` Si aún no lo ha indicado, puede obtener toda la información solicitada anteriormente con los siguientes comandos CLI. `# ACCOUNT ID` `aws sts get-caller-identity --query "Account" --output text` `# REGION CODE` `aws configure get region` `# CLUSTER EKS NAME`	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	`aws eks list-clusters --query "clusters" --output text` `# GENERATE EFS TOKEN uuidgen`	

Crear un espacio de nombres de Kubernetes y un perfil de Fargate vinculado

Tarea	Descripción	Habilidades requeridas
Cree un espacio de nombres de Kubernetes y un perfil de Fargate para las cargas de trabajo de las aplicaciones.	Cree un espacio de nombres para recibir las cargas de trabajo de las aplicacio nes que interactúan con Amazon EFS. Ejecute el script `create-k8s-ns-and-linked-fargate-pro file.sh` . Puede elegir usar un nombre de espacio de nombres personalizado o el espacio de nombres proporcio nado por defecto. `poc-efs-e ks-fargate` Con un nombre de espacio de nombres de aplicación personalizado: `export $APP_NAME SPACE=<CUSTOM_NAME> ./scripts/epic01/ create-k8s-ns-and -linked-fargate-pr ofile.sh \`	Usuario de Kubernetes con permisos concedidos

Tarea	Descripción	Habilidades requeridas
	`-c "$CLUSTER_NAME" -n "$APP_NAMESPACE"` Sin un nombre de espacio de nombres de aplicación personalizado: `./scripts/epic01/create-k8s-ns-and-linked-fargate-profile.sh \ -c "$CLUSTER_NAME"` donde `$CLUSTER_NAME` es el nombre de su clúster de Amazon EKS. El `-n <NAMESPACE>` parámetro es opcional; si no se informa, se proporcionará un nombre de espacio de nombres generado por defecto.	

Crear un sistema de archivos de Amazon EFS

Tarea	Descripción	Habilidades requeridas
Genera un token único.	Amazon EFS requiere la creación de un token para garantizar la operación de idempotencia (llamar a la operación con el mismo token de creación no tiene ningún efecto). Para cumplir con este requisito, debes generar un token único mediante	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	una técnica disponible. Por ejemplo, puedes generar un identificador único universal (UUID) para usarlo como token de creación.	

Tarea	Descripción	Habilidades requeridas
Crear un sistema de archivos de Amazon EFS.	Cree el sistema de archivos para recibir los archivos de datos que leen y escriben las cargas de trabajo de la aplicación. Puede crear un sistema de archivos cifrado o no cifrado. (Como práctica recomendada, el código de este patrón crea un sistema cifrado para habilitar el cifrado en reposo de forma predeterminada). Puede usar una clave única y simétrica de AWS KMS para cifrar su sistema de archivos. Si no se especifica una clave personalizada, se utiliza una clave gestionada por AWS. Utilice el script create-efs.sh para crear un sistema de archivos Amazon EFS cifrado o no cifrado, después de generar un token único para Amazon EFS. Con el cifrado en reposo, sin clave KMS: `./scripts/epic02/create-efs.sh \` `  -c "$CLUSTER_NAME" \` `  -t "$EFS_CREATION_TOKEN"`	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	donde `$CLUSTER_NAME` es el nombre de su clúster de Amazon EKS y `$EFS_CREATION_TOKEN` es un token de creación único para el sistema de archivos. Con el cifrado en reposo, con una clave KMS: `./scripts/epic02/create-efs.sh \` `  -c "$CLUSTER_NAME" \` `  -t "$EFS_CREATION_TOKEN" \` `  -k "$KMS_KEY_ALIAS"` donde `$CLUSTER_NAME` es el nombre de su clúster de Amazon EKS, `$EFS_CREATION_TOKEN` es un token de creación único para el sistema de archivos y `$KMS_KEY_ALIAS` es el alias para la clave KMS. Sin cifrado: `./scripts/epic02/create-efs.sh -d \` `  -c "$CLUSTER_NAME" \` `  -t "$EFS_CREATION_TOKEN"`	

Tarea	Descripción	Habilidades requeridas
	donde `$CLUSTER_NAME` es el nombre de su clúster de Amazon EKS, `$EFS_CREATION_TOKEN` es un token de creación único para el sistema de archivos y `–d` deshabilita el cifrado en reposo.	
Crear un grupo de seguridad.	Cree un grupo de seguridad para permitir al clúster de Amazon EKS acceder al sistema de archivos de Amazon EFS.	Administrador de sistemas de AWS
Actualizar la regla de entrada del grupo de seguridad.	Actualice las reglas de entrada del grupo de seguridad para permitir el tráfico entrante para las siguientes configuraciones: • Protocolo TCP: puerto 2049 • Fuente: rangos de bloques CIDR para las subredes privadas de la VPC que contiene el clúster de Kubernetes	Administrador de sistemas de AWS
Agregar un destino de montaje para cada subred privada.	Para cada subred privada del clúster de Kubernetes, cree un destino de montaje para el sistema de archivos y el grupo de seguridad.	Administrador de sistemas de AWS

Instalar los componentes de Amazon EFS en el clúster de Kubernetes

Tarea	Descripción	Habilidades requeridas
Implementar el controlador de CSI de Amazon EFS.	Implemente el controlador de CSI de Amazon EFS en el clúster. El controlador aprovisiona el almacenamiento de acuerdo con las notificaciones de volumen persistentes creadas por las aplicaciones. Ejecute el `create-k8s-efs-csi-sc.sh` script para implementar el controlador CSI de Amazon EFS y la clase de almacenamiento en el clúster. `./scripts/epic03/create-k8s-efs-csi-sc.sh` Este script usa la `kubectl` utilidad, así que asegúrese de que el contexto se haya configurado y apunte al clúster de Amazon EKS deseado.	Usuario de Kubernetes con permisos concedidos
Implementar la clase de almacenamiento.	Implemente la clase de almacenamiento en el clúster del aprovisionador de Amazon EFS (efs.csi.aws.com).	Usuario de Kubernetes con permisos concedidos

Instalear la aplicación PoC en el clúster de Kubernetes

Tarea	Descripción	Habilidades requeridas
Implementar el volumen persistente.	Implemente el volumen persistente y vincúlelo a la clase de almacenamiento creada y al ID del sistema de archivos Amazon EFS. La aplicación utiliza el volumen persistente para leer y escribir contenido. Puede especific ar cualquier tamaño para el volumen persistente en el campo de almacenam iento. Kubernetes requiere este campo, pero dado que Amazon EFS es un sistema de archivos elástico, no aplica ningún límite de capacidad del sistema de archivos. Puede implementar el volumen persistente con o sin cifrado. (El controlador CSI de Amazon EFS habilita el cifrado de forma predeterminada, como práctica recomendada). Ejecute el `deploy-poc-app.sh` script para implement ar el volumen persistente, la notificación del volumen persistente y las dos cargas de trabajo. Con cifrado en tránsito:	Usuario de Kubernetes con permisos concedidos

Tarea	Descripción	Habilidades requeridas
	`./scripts/epic04/deploy-poc-app.sh \ -t "$EFS_CREATION_TOKEN"` donde `$EFS_CREATION_TOKEN` es el token de creación único para el sistema de archivos. Sin cifrado en tránsito: `./scripts/epic04/deploy-poc-app.sh -d \ -t "$EFS_CREATION_TOKEN"` donde `$EFS_CREATION_TOKEN` es el token de creación único para el sistema de archivos y `-d` desactiva el cifrado en tránsito.	

Tarea	Descripción	Habilidades requeridas
Implementar la demanda de volumen persistente solicitada por la aplicación.	Implemente la demanda de volumen persistente solicitada por la aplicación y vincúlela a la clase de almacenamiento. Utilice el mismo modo de acceso que el volumen persistente que creó anteriormente. Puede especificar cualquier tamaño para la demanda de volumen persistente en el campo de almacenamiento. Kubernetes requiere este campo, pero dado que Amazon EFS es un sistema de archivos elástico, no aplica ningún límite de capacidad del sistema de archivos.	Usuario de Kubernetes con permisos concedidos
Implementar la carga de trabajo 1.	Implemente el pod que representa la carga de trabajo 1 de la aplicación. Esta carga de trabajo escribe contenido en el archivo `/data/out1.txt` .	Usuario de Kubernetes con permisos concedidos
Implementar la carga de trabajo 2.	Implemente el pod que representa la carga de trabajo 2 de la aplicación. Esta carga de trabajo escribe contenido en el archivo `/data/out2.txt` .	Usuario de Kubernetes con permisos concedidos

Validar la persistencia, durabilidad y compartibilidad del sistema de archivos

Tarea	Descripción	Habilidades requeridas
Compruebe el estado del`PersistentVolume` .	Introduzca el siguiente comando para comprobar el estado del`PersistentVolume` . `kubectl get pv` Para ver un ejemplo de resultado, consulte la sección de información adicional.	Usuario de Kubernetes con permisos concedidos
Compruebe el estado del`PersistentVolumeClaim` .	Introduzca el siguiente comando para comprobar el estado del`PersistentVolumeClaim` . `kubectl -n poc-efs-eks-fargate get pvc` Para ver un ejemplo de resultado, consulte la sección de información adicional.	Usuario de Kubernetes con permisos concedidos
Validar que la carga de trabajo 1 pueda escribir en el sistema de archivos.	Introduzca el siguiente comando para validar que la carga de trabajo 1 está escribiendo en`/data/out1.txt` . `kubectl exec -ti poc-app1 -n poc-efs-eks-fargate -- tail -f /data/out1.txt`	Usuario de Kubernetes con permisos concedidos

Tarea	Descripción	Habilidades requeridas
	Los resultados son similares a los siguientes: `...` `Thu Sep  3 15:25:07 UTC 2023 - PoC APP 1` `Thu Sep  3 15:25:12 UTC 2023 - PoC APP 1` `Thu Sep  3 15:25:17 UTC 2023 - PoC APP 1` `...`	
Validar que la carga de trabajo 2 pueda escribir en el sistema de archivos.	Introduzca el siguiente comando para validar que la carga de trabajo 2 está escribiendo en `/data/out2.txt` . `kubectl -n $APP_NAMESPACE exec -ti poc-app2 -- tail -f /data/out2.txt` Los resultados son similares a los siguientes: `...` `Thu Sep  3 15:26:48 UTC 2023 - PoC APP 2` `Thu Sep  3 15:26:53 UTC 2023 - PoC APP 2` `Thu Sep  3 15:26:58 UTC 2023 - PoC APP 2` `...`	Usuario de Kubernetes con permisos concedidos

Tarea	Descripción	Habilidades requeridas
Validar que la carga de trabajo 1 pueda leer el archivo escrito por la carga de trabajo 2.	Introduzca el siguiente comando para validar que la carga de trabajo 1 pueda leer el `/data/out2.txt` archivo escrito por la carga de trabajo 2. `kubectl exec -ti poc-app1 -n poc-efs-eks-fargate -- tail -n 3 /data/out2.txt` Los resultados son similares a los siguientes: `... Thu Sep 3 15:26:48 UTC 2023 - PoC APP 2 Thu Sep 3 15:26:53 UTC 2023 - PoC APP 2 Thu Sep 3 15:26:58 UTC 2023 - PoC APP 2 ...`	Usuario de Kubernetes con permisos concedidos

Tarea	Descripción	Habilidades requeridas
Validar que la carga de trabajo 2 pueda leer el archivo escrito por la carga de trabajo 1.	Introduzca el siguiente comando para validar que la carga de trabajo 2 pueda leer el `/data/out1.txt` archivo escrito por la carga de trabajo 1. `kubectl -n $APP_NAMESPACE exec -ti poc-app2 -- tail -n 3 /data/out1.txt` Los resultados son similares a los siguientes: `... Thu Sep 3 15:29:22 UTC 2023 - PoC APP 1 Thu Sep 3 15:29:27 UTC 2023 - PoC APP 1 Thu Sep 3 15:29:32 UTC 2023 - PoC APP 1 ...`	Usuario de Kubernetes con permisos concedidos

Tarea	Descripción	Habilidades requeridas
Validar que los archivos se conserven después de eliminar los componentes de la aplicación.	A continuación, utilice un script para eliminar los componentes de la aplicación (volumen persistente, notificación de volumen persistente y pods) y validar que los archivos `/data/out1.txt` `/data/out2.txt` se conserven en el sistema de archivos. Ejecute el script `validate-efs-content.sh` mediante el comando siguiente. `./scripts/epic05/validate-efs-content.sh \` `-t "$EFS_CREATION_TOKEN"` donde `$EFS_CREATION_TOKEN` es el token de creación único para el sistema de archivos. Los resultados son similares a los siguientes: `pod/poc-app-validation created` `Waiting for pod get Running state...` `Waiting for pod get Running state...` `Waiting for pod get Running state...`	Usuario de Kubernetes con permisos concedidos, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	`Results from execution of 'find /data' on validation process pod:` `/data` `/data/out2.txt` `/data/out1.txt`	

Operaciones de supervisión

Tarea	Descripción	Habilidades requeridas
Supervisar los registros de aplicación.	Como parte de una operación de dos días, envía los registros de la aplicación a Amazon CloudWatch para que los supervisen.	Administrador de sistemas de AWS, usuario de Kubernetes con permisos concedidos
Supervisar contenedores de Amazon EKS y de Kubernetes con Container Insights.	Como parte de una operación de dos días, supervise los sistemas Amazon EKS y Kubernetes mediante Amazon Container Insights. CloudWatch Esta herramienta recopila, agrega y resume métricas de aplicaciones en contenedores en diferentes niveles y dimensiones. Para obtener más información, consulte la sección Recursos relacionados.	Administrador de sistemas de AWS, usuario de Kubernetes con permisos concedidos
Supervise Amazon EFS con CloudWatch.	Como parte de una operación de dos días, supervise los sistemas de archivos con Amazon CloudWatch, que	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	recopila y procesa datos sin procesar de Amazon EFS para convertirlos en métricas legibles y prácticamente en tiempo real. Para obtener más información, consulte la sección Recursos relacionados.	

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Limpiar todos los recursos creados para el patrón.	Tras completar este patrón, limpie todos los recursos para evitar incurrir en cargos de AWS. Ejecute el `clean-up-resources.sh` script para eliminar todos los recursos una vez que haya terminado de usar la aplicación PoC. Complete una de las siguientes opciones. Con el cifrado en reposo, con una clave KMS: `./scripts/epic06/clean-up-resources.sh \` `  -c "$CLUSTER_NAME" \` `  -t "$EFS_CREATION_TOKEN" \` `  -k "$KMS_KEY_ALIAS"`	Usuario de Kubernetes con permisos concedidos, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	donde `$CLUSTER_NAME` es el nombre de su clúster de Amazon EKS, `$EFS_CREATION_TOKEN` es un token de creación único para el sistema de archivos y `$KMS_KEY_ALIAS` es el alias para la clave KMS. Sin cifrado en reposo: `./scripts/epic06/clean-up-resources.sh \ -c "$CLUSTER_NAME" \ -t "$EFS_CREATION_TOKEN"` donde `$CLUSTER_NAME` es el nombre de su clúster de Amazon EKS y `$EFS_CREATION_TOKEN` es un token de creación único para el sistema de archivos.	

Recursos relacionados

Referencias

- AWS Fargate para Amazon EKS ahora es compatible con Amazon EFS (anuncio)
- Cómo capturar los registros de las aplicaciones al usar Amazon EKS en AWS Fargate (entrada del blog)
- Uso de Container Insights (CloudWatch documentación de Amazon)

- Configuración de Container Insights en Amazon EKS y Kubernetes (documentación de Amazon) CloudWatch
- Métricas de Amazon EKS y Kubernetes Container Insights (documentación de Amazon) CloudWatch
- Supervisión de Amazon EFS con Amazon CloudWatch (documentación de Amazon EFS)

GitHub tutoriales y ejemplos

- Aprovisionamiento estático
- Cifrado en tránsito
- Acceder al sistema de archivos desde varios pods
- Consumir Amazon EFS en StatefulSets
- Montaje de subrutas
- Uso de puntos de acceso de Amazon EFS
- Planos de Amazon EKS para Terraform

Herramientas necesarias

- Instalación de la versión 2 de la AWS CLI
- Instalación de eksctl
- Instalación de kubectl
- Instalación de jq

Información adicional

A continuación, se muestra un ejemplo del resultado del `kubectl get pv` comando.

```
NAME         CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS   CLAIM
            STORAGECLASS   REASON   AGE
poc-app-pv   1Mi        RWX            Retain           Bound    poc-efs-eks-fargate/
poc-app-pvc   efs-sc                  3m56s
```

A continuación se muestra un ejemplo del resultado del `kubectl -n poc-efs-eks-fargate get pvc` comando.

```
NAME          STATUS   VOLUME       CAPACITY   ACCESS MODES   STORAGECLASS   AGE
poc-app-pvc   Bound    poc-app-pv   1Mi        RWX            efs-sc         4m34s
```

Más patrones

- Evaluar la preparación de las aplicaciones para la migración a la nube de AWS mediante CAST Highlight
- Crear automáticamente canalizaciones de CI/CD y clústeres de Amazon ECS para microservicios mediante AWS CDK
- Cree e inserte imágenes de Docker en Amazon ECR mediante GitHub Actions y Terraform
- Almacenamiento en contenedores de las cargas de trabajo de mainframe que Blu Age ha modernizado
- Crear un analizador de registros personalizado para Amazon ECS mediante un enrutador de registros Firelens
- Implemente una canalización de CI/CD para microservicios de Java en Amazon ECS
- Implementar un clúster de Amazon EKS desde AWS Cloud9 mediante un perfil de instancia de EC2
- Implementar un entorno para aplicaciones de Blu Age en contenedores mediante Terraform
- Implemente la lógica de preprocesamiento en un modelo de aprendizaje automático en un único punto final mediante una canalización de inferencias en Amazon SageMaker
- Gestione las implementaciones azul/verde de microservicios en varias cuentas y regiones mediante los servicios de código de AWS y las claves multirregionales de AWS KMS
- Gestión de las aplicaciones de contenedores en las instalaciones mediante la configuración de Amazon ECS Anywhere con AWS CDK
- Migre de Oracle GlassFish a AWS Elastic Beanstalk
- Migre de Oracle WebLogic a Apache Tomcat (ToMEE) en Amazon ECS
- Modernizar las aplicaciones de ASP.NET Web Forms en AWS
- Supervise los repositorios de Amazon ECR en busca de permisos comodín mediante AWS y AWS Config CloudFormation
- Configure una canalización de CI/CD para cargas de trabajo híbridas en Amazon ECS Anywhere mediante AWS CDK y GitLab
- Configure un repositorio de gráficos de Helm v3 en Amazon S3
- ???
- Configure el end-to-end cifrado para aplicaciones en Amazon EKS mediante cert-manager y Let's Encrypt
- Simplifique la implementación de aplicaciones multiusuario de Amazon EKS mediante Flux

- Estructure un proyecto de Python en una arquitectura hexagonal con AWS Lambda
- Entrena e implementa un modelo de aprendizaje automático personalizado compatible con GPU en Amazon SageMaker

Entrega de contenido

Temas

- Envíe los registros de AWS WAF a Splunk mediante AWS Firewall Manager y Amazon Data Firehose
- Sirva contenido estático en un bucket de Amazon S3 a través de una VPC mediante Amazon CloudFront
- Más patrones

Envíe los registros de AWS WAF a Splunk mediante AWS Firewall Manager y Amazon Data Firehose

Creado por Michael Friedenthal (AWS), Aman Kaur Gandhi (AWS) y JJ Johnson (AWS)

Entorno: PoC o piloto	Tecnologías: entrega de contenido; seguridad, identidad, conformidad	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: AWS Firewall Manager; Amazon Kinesis Data Firehose; AWS WAF		

Resumen

Históricamente, había dos formas de mover los datos a Splunk: una arquitectura de inserción o una arquitectura de extracción. Una arquitectura de extracción ofrece garantías de entrega de los datos mediante reintentos, pero requiere recursos dedicados en Splunk que recopilen los datos. Las arquitecturas de extracción no suelen funcionar en tiempo real debido a las encuestas. Una arquitectura de inserción suele tener una latencia más baja, es más escalable y reduce la complejidad y los costos operativos. Sin embargo, no garantiza la entrega y, por lo general, requiere agentes.

La integración de Splunk con Amazon Data Firehose proporciona datos de streaming en tiempo real a Splunk a través de un recopilador de eventos HTTP (HEC). Esta integración ofrece las ventajas de las arquitecturas de inserción y extracción: garantiza la entrega de datos mediante reintentos, es prácticamente en tiempo real, es de baja latencia y tiene poca complejidad. El HEC envía los datos de forma rápida y eficiente a través de HTTP o HTTPS directamente a Splunk. Los HEC están basados en tokens, lo que elimina la necesidad de codificar las credenciales en una aplicación o en los archivos auxiliares.

En una política de AWS Firewall Manager, puede configurar el registro de todo el tráfico de ACL web de AWS WAF en todas sus cuentas y, a continuación, puede utilizar una transmisión de entrega de Firehose para enviar los datos de registro a Splunk para su supervisión, visualización y análisis. Esta solución proporciona los siguientes beneficios:

- Administración y registro centralizados del tráfico de ACL web de AWS WAF en todas sus cuentas
- Integración de Splunk con una sola cuenta de AWS
- Escalabilidad
- Entrega de datos de registro prácticamente en tiempo real
- Optimización de costos mediante el uso de una solución sin servidor, de forma que no tenga que pagar por los recursos no utilizados.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa que forma parte de una organización en AWS Organizations.
- Debe tener los siguientes permisos para habilitar el registro con Firehose:
  - `iam:CreateServiceLinkedRole`
  - `firehose:ListDeliveryStreams`
  - `wafv2:PutLoggingConfiguration`
- Se deben configurar AWS WAF y sus ACL web. Consulte Introducción a AWS WAF para obtener instrucciones.
- Se debe configurar AWS Firewall Manager. Para obtener instrucciones, consulte los requisitos previos de AWS Firewall Manager.
- Se deben configurar las políticas de seguridad de Firewall Manager para AWS WAF. Para obtener instrucciones, consulte Introducción a las políticas AWS WAF de AWS Firewall Manager.
- Splunk debe estar configurado con un punto final HTTP público al que Firehose pueda acceder.

Limitaciones

- Las cuentas de AWS deben administrarse en una sola organización en AWS Organizations.
- La ACL web debe estar en la misma región que la transmisión de entrega. Si vas a capturar registros para Amazon CloudFront, crea el flujo de entrega Firehose en la región EE.UU. Este (Norte de Virginia),. `us-east-1`
- El complemento Splunk para Firehose está disponible para despliegues de pago de Splunk Cloud, despliegues distribuidos de Splunk Enterprise y despliegues de Splunk Enterprise de instancia única. Este complemento no es compatible con las implementaciones de prueba gratuitas de Splunk Cloud.

Arquitectura

Pila de tecnología de destino

- Firewall Manager
- Firehose
- Amazon S3
- AWS WAF
- Splunk

Arquitectura de destino

La siguiente imagen muestra cómo puede utilizar Firewall Manager para registrar de forma centralizada todos los datos de AWS WAF y enviarlos a Splunk a través de Kinesis Data Firehose.

1. Las ACL web de AWS WAF envían los datos de registro del firewall a Firewall Manager.
2. Firewall Manager envía los datos de registro a Firehose.
3. El flujo de entrega de Firehose reenvía los datos de registro a Splunk y a un depósito S3. El bucket de S3 actúa como respaldo en caso de que se produzca un error en el flujo de entrega de Firehose.

Automatizar y escalar

Esta solución está diseñada para escalar y adaptarse a todos los ALC web de AWS WAF de la organización. Puede configurar todas las ACL web para que usen la misma instancia de Firehose. Sin embargo, si quieres configurar y usar varias instancias de Firehose, puedes hacerlo.

Herramientas

Servicios de AWS

- AWS Firewall Manager es un servicio de administración de la seguridad que le ayuda a configurar y administrar de forma centralizada las reglas del firewall en todas sus cuentas y aplicaciones en AWS Organizations.

- Amazon Data Firehose le ayuda a entregar datos de streaming en tiempo real a otros servicios de AWS, puntos de enlace HTTP personalizados y puntos de enlace HTTP propiedad de proveedores de servicios externos compatibles, como Splunk.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS WAF es un firewall de aplicación web que le ayuda a monitorizar las solicitudes HTTP y HTTPS que se reenvíen a los recursos de su aplicación web protegida.

Otras herramientas

- Splunk le permite monitorear, visualizar y analizar los datos de registro.

Epics

Configurar Splunk

Tarea	Descripción	Habilidades requeridas
Instale la aplicación Splunk para AWS.	1. Inicie sesión en su programa de envío intensivo de Splunk. La URL predeterminada es `http://<IP address>:8000` . 2. En el panel de navegación de la izquierda, junto a Aplicaciones, seleccione el botón de engranaje. 3. Seleccione Buscar más aplicaciones. 4. Busque AWS. 5. En Aplicación Splunk para AWS, elija Instalar. 6. Introduzca sus credenciales de inicio de sesión en	Administrador de seguridad, administrador de Splunk

Tarea	Descripción	Habilidades requeridas
	Splunk.com, acepte los términos y condiciones y, a continuación, seleccione Iniciar sesión e instalar. 7. Seleccione Listo.	
Instale el complemento para AWS WAF.	Repita las instrucciones anteriores para instalar el complemento AWS Web Application Firewall para Splunk.	Administrador de seguridad, administrador de Splunk

Tarea	Descripción	Habilidades requeridas
Instala y configura el complemento Splunk para Firehose.	1. Instala y configura el complemento Splunk para Firehose. Como parte de la instalación y la configuración, si es necesario para su plataforma Splunk, debe configurar un recopilador de eventos HTTP y preparar la infraestructura para enviar los datos de registro a sus indexadores. Consulte las instrucciones correspondientes a su implementación de Splunk: • Implementación de Splunk Cloud (documentación de Splunk) • Implementación distribuida de Splunk Enterprise (documentación de Splunk) • Implementación de Splunk Enterprise en una sola instancia (documentación de Splunk) Importante: detenga este procedimiento después de haber instalado y configurado el complemento Splunk. No continúe con las instrucciones para configurar Firehose para	Administrador de seguridad, administrador de Splunk

Tarea	Descripción	Habilidades requeridas
	enviar datos a la plataforma Splunk. 2. Anote el token del recopilador de eventos HTTP y el punto de conexión HTTP. Necesitará este valor más adelante, cuando configure el flujo de entrega.	

Crea el flujo de entrega de Firehose

Tarea	Descripción	Habilidades requeridas
Concede a Firehose acceso a un destino de Splunk.	Configure la política de acceso que permite a Firehose acceder a un destino de Splunk y hacer una copia de seguridad de los datos de registro en un bucket de S3. Para obtener más información, consulta Otorgar a Firehose acceso a un destino de Splunk.	Administrador de seguridad
Crea un flujo de entrega de Firehose.	En la misma cuenta en la que administra las ACL web de AWS WAF, cree una transmisión de entrega en Firehose. Es obligatorio contar con un rol de IAM al crear un flujo de entrega. Firehose asume esa función de IAM y obtiene acceso al bucket S3 especificado. Para obtener instrucci	Administrador de seguridad

Tarea	Descripción	Habilidades requeridas
	ones, consulte Crear un flujo de entrega. Tenga en cuenta lo siguiente: • El nombre de flujo de entrega debe empezar por `aws-waf-logs-` . • Para el origen, elija Direct PUT. • En Modo de copia de seguridad de S3, seleccione Hacer copia de seguridad de todos los eventos y, a continuación, elija un bucket existente o cree uno nuevo. • Para el destino, siga las instrucciones de Elija Splunk para su destino en la documentación de Firehose. Para obtener información sobre los valores de los puntos de enlace y los tipos de puntos de enlace de Splunk, consulte Configurar Amazon Data Firehose en la documentación de Splunk. Repita este proceso para cada token que haya configurado en el recopilador de eventos HTTP.	

Tarea	Descripción	Habilidades requeridas
Pruebe el flujo de entrega.	Pruebe el flujo de entrega para comprobar que está configurado correctamente. Para obtener instrucciones, consulte Probar con Splunk como destino en la documentación de Firehose.	Administrador de seguridad

Configurar Firewall Manager para registrar datos

Tarea	Descripción	Habilidades requeridas
Configure las políticas de Firewall Manager.	Las políticas de Firewall Manager deben configurarse para habilitar el registro y reenviar los registros al flujo de entrega de Firehose correcto. Para obtener más información e instrucciones, consulte Configuración de registros para una política WAF de AWS WAF.	Administrador de seguridad

Recursos relacionados

Recursos de AWS

- Registro del tráfico de ACL web (documentación de AWS WAF)
- Configuración del registro para una política de AWS WAF (documentación de AWS WAF)
- Tutorial: Envío de registros de flujo de VPC a Splunk mediante Amazon Data Firehose (documentación de Firehose)
- ¿Cómo puedo enviar los registros de flujo de VPC a Splunk con Amazon Data Firehose? (Centro de conocimientos de AWS)

- Impulse la ingesta de datos en Splunk mediante Amazon Data Firehose (entrada del blog de AWS)

Documentación de Splunk

- Complemento Splunk para Amazon Data Firehose

Sirva contenido estático en un bucket de Amazon S3 a través de una VPC mediante Amazon CloudFront

Creada por Angel Emmanuel Hernandez Cebrian

Entorno: PoC o piloto	Tecnologías: entrega de contenido; redes; seguridad, identidad y conformidad; sin servidor; aplicaciones web y móviles	Servicios de AWS: Amazon CloudFront; Elastic Load Balancing (ELB); AWS Lambda

Resumen

Cuando publicas contenido estático alojado en Amazon Web Services (AWS), el enfoque recomendado es utilizar un depósito de Amazon Simple Storage Service (S3) como origen y utilizar CloudFront Amazon para distribuir el contenido. Esta solución tiene dos ventajas principales: la comodidad de almacenar en caché el contenido estático en las ubicaciones periféricas y la capacidad de definir listas de control de acceso web (ACL web) para la CloudFront distribución, lo que le ayuda a proteger las solicitudes de contenido con una configuración y una sobrecarga administrativa mínimas.

Sin embargo, el enfoque estándar recomendado tiene una limitación arquitectónica común. En algunos entornos, puede ser deseable que los dispositivos de firewall virtual se implementen en una nube privada virtual (VPC) para inspeccionar todo el contenido, incluido el contenido estático. El enfoque estándar no dirige el tráfico a través de la VPC para su inspección. Este patrón proporciona una solución arquitectónica alternativa. Se sigue utilizando una CloudFront distribución para ofrecer contenido estático en un bucket de S3, pero el tráfico se enruta a través de la VPC mediante un Application Load Balancer. A continuación, una función de Lambda de AWS recupera y devuelve el contenido del bucket de S3.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Contenido estático del sitio web alojado en un bucket de S3.

Limitaciones

- Los recursos de este patrón deben estar en una sola región de AWS, pero se pueden aprovisionar en diferentes cuentas de AWS.
- Los límites se aplican al tamaño máximo de solicitud y respuesta que la función de Lambda puede, respectivamente, recibir y enviar. Para obtener más información, consulte Límites en Funciones de Lambda como destinos (documentación de Elastic Load Balancing).
- Al usar este enfoque, es importante encontrar un buen equilibrio entre el rendimiento, la escalabilidad, la seguridad y la rentabilidad. A pesar de la alta escalabilidad de Lambda, si el número de invocaciones simultáneas de Lambda supera la cuota máxima, algunas solicitudes se limitarán. Para más información, consulte las cuotas de Lambda (documentación de Lambda). También debe tener en cuenta los precios de uso de Lambda. Para minimizar las invocaciones a Lambda, asegúrese de definir correctamente la caché de la distribución. CloudFront Para obtener más información, consulte Optimización del almacenamiento en caché y la disponibilidad (documentación)CloudFront .

Arquitectura

Pila de tecnología de destino

- CloudFront
- Amazon Virtual Private Cloud (Amazon VPC)
- Equilibrador de carga de aplicación
- Lambda
- Amazon S3

Arquitectura de destino

La siguiente imagen muestra la arquitectura sugerida cuando es necesario utilizarla CloudFront para servir contenido estático desde un bucket de S3 a través de una VPC.

1. El cliente solicita la URL de CloudFront distribución para incluir un archivo de sitio web concreto en el bucket de S3.

2. CloudFront envía la solicitud a AWS WAF. AWS WAF filtra la solicitud mediante las ACL web aplicadas a la distribución. CloudFront Si se determina que la solicitud es válida, el flujo continúa. Si se determina que la solicitud no es válida, el cliente recibe un error 403.
3. CloudFront comprueba su caché interna. Si hay una clave válida que coincida con la solicitud entrante, el valor asociado se devuelve al cliente como respuesta. Si no es así, el flujo continúa.
4. CloudFront reenvía la solicitud a la URL del Application Load Balancer especificado.
5. El equilibrador de carga de aplicación tiene un oyente asociado a un grupo objetivo basado en una función de Lambda. El equilibrador de carga de aplicación invoca la función de Lambda.
6. La función de Lambda se conecta al bucket de S3, realiza una operación `GetObject` en él y devuelve el contenido como respuesta.

Automatizar y escalar

Para automatizar la implementación de contenido estático mediante este enfoque, cree procesos de CI/CD para actualizar los buckets de Amazon S3 que alojan sitios web.

La función de Lambda escala automáticamente para gestionar las solicitudes concurrentes, dentro de las cuotas y limitaciones del servicio. Para obtener más información, consulte Escalado de función de Lambda y Cuotas de Lambda (documentación de Lambda). Para los demás servicios y características de AWS, como CloudFront el Application Load Balancer, AWS los escala automáticamente.

Herramientas

- Amazon CloudFront acelera la distribución de tu contenido web al distribuirlo a través de una red mundial de centros de datos, lo que reduce la latencia y mejora el rendimiento.
- Elastic Load Balancing (ELB) distribuye el tráfico entrante de aplicaciones o redes entre varios destinos. En este patrón, se emplea un equilibrador de carga de aplicación, aprovisionado mediante Elastic Load Balancing, para dirigir el tráfico a la función de Lambda.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esta red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Epics

Se utiliza CloudFront para ofrecer contenido estático de Amazon S3 a través de una VPC

Tarea	Descripción	Habilidades requeridas
Cree una VPC.	Cree una VPC para alojar los recursos implementados en este patrón, como el equilibrador de carga de aplicación y la función de Lambda. Para obtener instrucciones, consulte Crear una VPC (documentación de Amazon VPC).	Arquitecto de la nube
Cree una ACL web de AWS WAF.	Cree una ACL web de AWS WAF. Más adelante en este patrón, se aplica esta ACL web a la CloudFront distribución. Para obtener instrucciones, consulte Crear una ACL web (documentación de AWS WAF).	Arquitecto de la nube
Crear la función de Lambda.	Cree la función de Lambda que sirva el contenido estático alojado en el bucket de S3 como sitio web. Use el código que se proporciona en la sección de Información adicional de este patrón. Personalice el código para	AWS general

Tarea	Descripción	Habilidades requeridas
	identificar su bucket de S3 de destino.	
Cargar la función de Lambda.	Introduzca el siguiente comando para cargar el código de la función de Lambda en un archivo .zip en Lambda. `aws lambda update-function-code \ --function-name \ --zip-file fileb://lambda-alb-s3-website.zip`	AWS general
Cree un Equilibrador de carga de aplicación.	Cree un equilibrador de carga de aplicación con acceso a Internet que apunte a la función de Lambda. Para obtener instrucciones, consulte Crear un grupo de destino para la función de Lambda (documentación de Elastic Load Balancing). Para una configuración de alta disponibilidad, cree el equilibrador de carga de aplicación y adjúntelo a subredes privadas en distintas zonas de disponibilidad.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Cree una CloudFront distribución.	Cree una CloudFront distribución que apunte al Application Load Balancer que creó. 1. Inicie sesión en la consola de administración de AWS y abra la CloudFront consola en https://console.aws.amazon.com/cloudfront/v3/home. 2. Seleccione Create Distribution (Crear distribución). 3. En la primera página del Create Distribution Wizard (Asistente de creación de distribuciones), en la sección Web, elija Get Started (Empezar). 4. Especifique la configuración de su distribución. Para obtener más información, consulte Valores que especifica cuando crea o actualiza una distribución. Tenga en cuenta lo siguiente: a. Establezca el equilibrador de carga de aplicación como origen. b. En la configuración de distribución, elija las ACL web existentes que desee aplicar a través de AWS WAF. Para más	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	información, consulte ACL web de AWS WAF. 5. Guarde los cambios. 6. Una CloudFront vez creada la distribución, el valor de la columna Estado de la distribución cambia de InProgressa Implement ada. Si decidió habilitar la distribución, estará lista para procesar solicitudes cuando el estado cambie a Deployed (Implementado).	

Recursos relacionados

Documentación de AWS

- Optimización del almacenamiento en caché y la disponibilidad (CloudFront documentación)
- Funciones de Lambda como destinos (documentación de Elastic Load Balancing)
- Cuotas de Lambda (documentación de Lambda)

Sitios web de servicios de AWS

- Equilibrador de carga de aplicación
- Lambda
- CloudFront
- Amazon S3
- AWS WAF
- Amazon VPC

Información adicional

Código

El siguiente ejemplo de función de Lambda está escrito en Node.js. Esta función de Lambda actúa como un servidor web que realiza una operación `GetObject` en un bucket de S3 que contiene los recursos del sitio web.

```
/**

 * This is an AWS Lambda function created for demonstration purposes.

 * It retrieves static assets from a defined Amazon S3 bucket.

 * To make the content available through a URL, use an Application Load Balancer with a
 Lambda integration.
 *
 * Set the S3_BUCKET environment variable in the Lambda function definition.
 */

var AWS = require('aws-sdk');

exports.handler = function(event, context, callback) {

    var bucket = process.env.S3_BUCKET;
    var key = event.path.replace('/', '');

    if (key == '') {
        key = 'index.html';
    }

    // Fetch from S3
    var s3 = new AWS.S3();
    return s3.getObject({Bucket: bucket, Key: key},
       function(err, data) {

            if (err) {
                return err;
            }

            var isBase64Encoded = false;
            var encoding = 'utf8';
```

```
            if (data.ContentType.indexOf('image/') > -1) {
                isBase64Encoded = true;
                encoding = 'base64'
            }

            var resp = {
                statusCode: 200,
                headers: {
                    'Content-Type': data.ContentType,
                },
                body: new Buffer(data.Body).toString(encoding),
                isBase64Encoded: isBase64Encoded
            };

            callback(null, resp);
        }
    );
};
```

Más patrones

- Comprueba la versión de registro de acceso, HTTPS y TLS en una CloudFront distribución de Amazon
- Implemente una aplicación basada en gRPC en un clúster de Amazon EKS y acceda a ella con un Equilibrador de carga de aplicación
- ???
- Implementar la solución Security Automations para AWS WAF mediante Terraform
- Vea los registros y las métricas de AWS Network Firewall mediante Splunk

Administración de costos

Temas

- Crear informes detallados de costos y uso para los trabajos de AWS Glue con el explorador de costos de AWS
- Crear informes detallados de costos y uso para los clústeres de Amazon EMR mediante el explorador de costos de AWS.
- Más patrones

Crear informes detallados de costos y uso para los trabajos de AWS Glue con el explorador de costos de AWS

Creado por Parijat Bhide (AWS) y Aromal Raj Jayarajan (AWS)

Entorno: producción	Tecnologías: Gestión de costos; análisis	Servicios de AWS: Administración de facturación y costos de AWS; AWS Glue

Resumen

Este patrón muestra cómo realizar un seguimiento de los costos de uso de los trabajos de integración de datos de AWS Glue mediante la configuración de etiquetas de asignación de costos definidas por el usuario. Puede usar estas etiquetas para crear informes detallados de costos y uso en el explorador de costos de AWS para trabajos en varias dimensiones. Por ejemplo, puede realizar un seguimiento de los costos de uso a nivel de equipo, proyecto o centro de costos.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Uno o más Trabajos de AWS Glue que tienen activadas las etiquetas definidas por el usuario

Arquitectura

Pila de tecnología de destino

- AWS Glue
- AWS Cost Explorer

En el siguiente diagrama se muestra cómo aplicar etiquetas para realizar un seguimiento de los costos de uso de los trabajos de AWS Glue.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un ingeniero de datos o un administrador de AWS crea etiquetas de asignación de costos definidas por el usuario para los trabajos de AWS Glue.
2. Un administrador de AWS activa las etiquetas.
3. Las etiquetas envían los metadatos al explorador de costos de AWS.

Herramientas

- AWS Glue es un servicio de extracción, transformación y carga (ETL) completamente administrado. le ayuda a clasificar, limpiar, enriquecer y mover datos de forma fiable entre almacenes de datos y flujos de datos.
- El Explorador de costos de AWS permite ver y analizar los costos y el uso.

Epics

Crear y activar etiquetas para sus trabajos de AWS Glue

Tarea	Descripción	Habilidades requeridas
Cree etiquetas de asignación de costos definidas por el usuario para los trabajos de AWS Glue.	Para añadir etiquetas a un trabajo de AWS Glue existente 1. Inicie sesión en la consola de administración de AWS y, a continuación, abra la consola de AWS Glue. 2. En el panel de navegación izquierdo, en ETL, elija Trabajos. 3. En la sección Sus trabajos, seleccione el nombre del trabajo que va a etiquetar. 4. Elija la pestaña Detalles del trabajo. A continuac	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	ión, expanda la sección de Propiedades avanzadas. 5. En Etiquetas, elija Agregar etiqueta nueva. 6. En Nombre, escriba un nombre para su etiqueta. 7. (Opcional) En Valor, introduzca un valor que desee asociar a la clave. 8. (Opcional) Repita los pasos del 5 al 7 para cada etiqueta que quiera crear para la tarea. 9. Seleccione Guardar. Para añadir etiquetas a un nuevo trabajo de AWS Glue 1. Cree un nuevo trabajo de AWS Glue en función de los requisitos del caso de uso. Para obtener instrucciones, consulte Trabajar con trabajos en la consola de AWS Glue en la Guía para desarrolladores de AWS Glue. 2. Cuando configure los ajustes de Detalles del trabajo, siga los pasos del 4 al 9 de la sección Añadir etiquetas a un trabajo de AWS Glue existente de esta tarea.	

Tarea	Descripción	Habilidades requeridas
	Nota: para obtener más información, consulte Etiquetas de AWS en AWS Glue en la Guía para desarroll adores de AWS Glue.	
Active las etiquetas de asignación de costos definidas por el usuario.	Siga las instrucciones de Activación de etiquetas de asignación de costos definidas por el usuario en la Guía del usuario de facturación de AWS.	Administrador de AWS

Crear informes de costos y uso para sus trabajos de AWS Glue

Tarea	Descripción	Habilidades requeridas
Cree informes de costos y uso para sus trabajos de AWS Glue mediante filtros de etiquetas en el explorador de costos de AWS.	1. Inicie sesión en la consola de administración de AWS y abra la consola de administración de AWS. 2. En el panel de navegación izquierdo, elija Informes. 3. Elija Crear nuevo informe. 4. En Seleccione un tipo de informe, seleccione Costo y uso (recomendado). A continuación, elija Crear informe. 5. En Filtros, seleccione Servicio. Se muestra el menú desplegable del Servicio.	AWS general, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	6. Seleccione la casilla situada junto a Glue. A continuación, seleccione Aplicar filtros. 7. Para los Filtros, seleccione Etiqueta. Se muestra el menú desplegable de Etiqueta. 8. Seleccione Equipo. A continuación, seleccione las casillas de verificación situadas junto a los equipos a los que haya asignado etiquetas. Excluya a los equipos a los que no haya asignado etiquetas. A continuación, seleccione Aplicar filtros. 9. En la parte superior del gráfico, seleccione Etiqueta. A continuación, seleccione las etiquetas de los trabajos de AWS Glue para los que desee crear un informe. 10. En la parte superior del gráfico, seleccione el menú desplegable de los Últimos 3 meses y seleccione el período que desea que abarque el informe. A continuación, seleccione el menú desplegable Mensual y seleccione cómo quiere que se agreguen	

Tarea	Descripción	Habilidades requeridas
	las partidas del informe en función del período de tiempo. 11 Elija Save as (Guardar como). A continuación, introduzca un título para su informe. 12 Elija Save report. Para obtener más información, consulte Exploración de sus datos con Cost Explorer en la Guía del usuario de administración de costos de AWS.	

Crear informes detallados de costos y uso para los clústeres de Amazon EMR mediante el explorador de costos de AWS.

Creado por Parijat Bhide (AWS) y Aromal Raj Jayarajan (AWS)

Entorno: producción	Tecnologías: Gestión de costos; análisis; macrodatos	Servicios de AWS: Administración de facturación y costos de AWS; Amazon EMR

Resumen

Este patrón muestra cómo realizar un seguimiento de los costos de uso de los clústeres de Amazon EMR mediante la configuración de etiquetas de asignación de costos definidas por el usuario. Puede usar estas etiquetas para crear informes detallados de costos y uso en el explorador de costos de AWS para clústeres en varias dimensiones. Por ejemplo, puede realizar un seguimiento de los costos de uso a nivel de equipo, proyecto o centro de costos.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Uno o más clústeres de EMR que tienen activadas las etiquetas definidas por el usuario

Arquitectura

Pila de tecnología de destino

- Amazon EMR
- AWS Cost Explorer

Arquitectura de destino

El siguiente diagrama muestra cómo puede aplicar etiquetas para realizar un seguimiento de los costos de uso de clústeres de Amazon EMR específicos.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un ingeniero de datos o un administrador de AWS crea etiquetas de asignación de costos definidas por el usuario para los clústeres de Amazon EMR.
2. Un administrador de AWS activa las etiquetas.
3. Las etiquetas envían los metadatos al explorador de costos de AWS.

Herramientas

Herramientas

- Amazon EMR Amazon EMR es una plataforma de clústeres administrada que simplifica la ejecución de marcos de macrodatos en AWS para procesar y analizar grandes cantidades de datos.
- El Explorador de costos de AWS permite ver y analizar los costos y el uso.

Epics

Crear y activar etiquetas para sus clústeres de Amazon EMR

Tarea	Descripción	Habilidades requeridas
Cree etiquetas de asignación de costos definidas por el usuario para los clústeres de Amazon EMR.	Para añadir etiquetas a un clúster de Amazon EMR existente Siga las instrucciones en Añadir etiquetas a un clúster existente en la Guía de administración de Amazon EMR. Para añadir etiquetas a un nuevo clúster de Amazon EMR	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	Siga las instrucciones en Añadir etiquetas a un nuevo clúster en la Guía de administración de Amazon EMR. Para obtener más información sobre cómo configurar un clúster de Amazon EMR, consulte Planificar y configurar clústeres en la Guía de administración de Amazon EMR.	
Active las etiquetas de asignación de costos definidas por el usuario.	Siga las instrucciones de Activación de etiquetas de asignación de costos definidas por el usuario en la Guía del usuario de facturación de AWS.	Administrador de AWS

Crear informes de costos y uso para sus clústeres de Amazon EMR

Tarea	Descripción	Habilidades requeridas
Cree informes de costo y uso para sus clústeres de Amazon EMR mediante filtros de etiquetas en al explorador de costos de AWS.	1. Inicie sesión en la consola de administración de AWS y abra la consola de administración de AWS. 2. En el panel de navegación izquierdo, elija Informes. 3. Elija Crear nuevo informe. 4. En Seleccione un tipo de informe, seleccione Costo y uso (recomendado). A	AWS general, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	continuación, elija Crear informe. 5. En Filtros, seleccione Servicio. Se muestra el menú desplegable del Servicio. 6. Seleccione las casillas de verificación situadas junto a las instancias EMR (Elastic MapReduce) y EC2 (Elastic Compute Cloud — Compute). A continuación, seleccione Aplicar filtros. 7. Para los Filtros, seleccion e Etiqueta. Se muestra el menú desplegable de Etiqueta. 8. Seleccione Equipo. A continuación, seleccion e las casillas de verificac ión situadas junto a los equipos a los que haya asignado etiquetas. Excluya a los equipos a los que no haya asignado etiquetas. A continuación, seleccione Aplicar filtros. 9. En la parte superior del gráfico, seleccione Etiqueta. A continuación, seleccion e las etiquetas de los clústeres de Amazon EMR para los que desee crear un informe.	

Tarea	Descripción	Habilidades requeridas
	10. En la parte superior del gráfico, seleccione el menú desplegable de los Últimos 3 meses y seleccione el período que desea que abarque el informe. A continuación, seleccione el menú desplegable Mensual y seleccione cómo quiere que se agreguen las partidas del informe en función del período de tiempo. 11. Elija Save as (Guardar como). A continuación, introduzca un título para su informe. 12. Elija Save report. Para obtener más información, consulte Exploración de sus datos con Cost Explorer en la Guía del usuario de administración de costos de AWS.	

Más patrones

- Automatice la creación de recursos AppStream 2.0 con AWS CloudFormation
- Archivar automáticamente los elementos en Amazon S3 con DynamoDB TTL
- ???
- Crear informes detallados de costos y uso para Amazon RDS y Amazon Aurora
- Eliminar volúmenes de Amazon Elastic Block Store (Amazon EBS) no utilizados con AWS Config y AWS Systems Manager
- Costos de almacenamiento estimados para una tabla de Amazon DynamoDB
- Estime el costo de una tabla de DynamoDB para la capacidad bajo demanda

Lagos de datos

Temas

Automatizar la ingesta de datos de AWS Data Exchange en Amazon S3

Creado por Adnan Alvee (AWS) y Manikanta Gona (AWS)

Tecnologías: análisis; lagos de datos	Entorno: producción	Servicios de AWS: Amazon S3; Amazon CloudWatch; AWS Lambda; Amazon SNS

Resumen

Este patrón proporciona una CloudFormation plantilla de AWS que le permite incorporar automáticamente datos de AWS Data Exchange a su lago de datos en Amazon Simple Storage Service (Amazon S3).

AWS Data Exchange es un servicio que facilita intercambiar con seguridad conjuntos de datos basados en archivos de la nube de AWS. Los conjuntos de datos de AWS Data Exchange son mediante suscripción. Como suscriptor, también puede acceder a las revisiones de los conjuntos de datos a medida que los proveedores publican nuevos datos.

La CloudFormation plantilla de AWS crea un evento de Amazon CloudWatch Events y una función de AWS Lambda. El evento está pendiente de cualquier actualización del conjunto de datos del suscriptor. Si hay una actualización, CloudWatch inicia una función Lambda, que copia los datos en el bucket de S3 que especifique. Cuando los datos se han copiado correctamente, Lambda le envía una notificación de Amazon Simple Notification Service (Amazon SNS).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Suscripción a un conjunto de datos en AWS Data Exchange

Limitaciones

- La CloudFormation plantilla de AWS debe implementarse por separado para cada conjunto de datos suscrito en AWS Data Exchange.

Arquitectura

Pila de tecnología de destino

- AWS Lambda
- Amazon S3
- AWS Data Exchange
- Amazon CloudWatch
- Amazon SNS

Arquitectura de destino

Automatizar y escalar

Puede usar la CloudFormation plantilla de AWS varias veces para los conjuntos de datos que desee incorporar al lago de datos.

Herramientas

- AWS Data Exchange: es un servicio que facilita que los clientes de AWS intercambien con seguridad los conjuntos de datos basados en archivos en la nube de AWS. Como suscriptor, puede encontrar y suscribirse a cientos de productos de proveedores de datos cualificados. A continuación, puede descargar rápidamente el conjunto de datos o copiarlo en Amazon S3 para usarlo en una variedad de servicios de machine learning y análisis de AWS. Cualquier persona con una cuenta de AWS puede suscribirse a AWS Data Exchange.
- AWS Lambda: un servicio informático que permite ejecutar código sin aprovisionar ni administrar servidores. AWS Lambda ejecuta el código solo cuando es necesario y amplia la capacidad de manera automática, pasando de pocas solicitudes al día a miles por segundo. Solo se paga por el tiempo de computación que se consume, sin ningún cargo mientras el código no se ejecuta. Con AWS Lambda puede ejecutar código para prácticamente cualquier tipo de aplicación o

servicio backend, sin ningún esfuerzo de administración. AWS Lambda ejecuta el código en una infraestructura informática de alta disponibilidad y realiza todas las tareas de administración de los recursos informáticos, incluidos el mantenimiento del servidor y del sistema operativo, el aprovisionamiento de capacidad y el escalado automático, así como la monitorización del código y las funciones de registro.

- Amazon S3: almacenamiento para Internet. Puede utilizar Amazon S3 para almacenar y recuperar cualquier cantidad de datos en cualquier momento y desde cualquier parte de la web.
- Amazon CloudWatch Events: ofrece una transmisión casi en tiempo real de los eventos del sistema que describen los cambios en los recursos de AWS. Con reglas sencillas que puede configurar rápidamente, puede hacer coincidir los eventos y dirigirlos a una o más funciones o transmisiones de destino. CloudWatch Los eventos se dan cuenta de los cambios operativos a medida que se producen. Responde a estos cambios operativos y toma medidas correctoras según sea necesario, enviando mensajes para responder al entorno, activando funciones, realizando cambios y captando información de estado. También puedes usar CloudWatch Events para programar acciones automatizadas que se inicien automáticamente en determinados momentos mediante expresiones cron o rate.
- Amazon SNS: un servicio web que facilita que las aplicaciones, los usuarios finales y los dispositivos puedan enviar y recibir al instante notificaciones desde la nube. Amazon SNS proporciona temas (canales de comunicación) para mensajes push de alto rendimiento. many-to-many Al utilizar los temas de Amazon SNS, los publicadores pueden distribuir mensajes a un gran número de suscriptores para su procesamiento en paralelo, incluidas las colas de Amazon Simple Queue Service (Amazon SQS), las funciones de AWS Lambda y los webhooks HTTP/S. También puede utilizar Amazon SNS para enviar notificaciones a usuarios finales mediante notificaciones push para móvil, SMS y correo electrónico.

Epics

Suscribirse a un conjunto de datos

Tarea	Descripción	Habilidades requeridas
Suscríbase a un conjunto de datos.	En la consola de AWS Data Exchange, suscríbase a un conjunto de datos. Para obtener instrucciones, consulte el enlace de la	AWS general

Tarea	Descripción	Habilidades requeridas
	sección «Recursos relaciona dos».	
Tenga en cuenta los atributos del conjunto de datos.	Anote la región de AWS, el ID y el ID de revisión del conjunto de datos. Lo necesitará para la CloudFormation plantilla de AWS en el siguiente paso.	AWS general

Implemente la CloudFormation plantilla de AWS

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3 y una carpeta.	Si ya tiene un lago de datos en Amazon S3, cree una carpeta para almacenar los datos que desee incorporar desde AWS Data Exchange. Si va a implementar la plantilla con fines de prueba, cree un nuevo bucket de S3 y anote el nombre del bucket y el prefijo de la carpeta para el paso siguiente.	AWS general
Implemente la CloudFormation plantilla de AWS.	Implemente la CloudForm ation plantilla de AWS que se proporciona como adjunto a este patrón. Configure los parámetros siguientes para que se correspondan con la configuración de su cuenta de AWS, conjunto de datos y bucket de S3: región de AWS del conjunto de datos,	AWS general

Tarea	Descripción	Habilidades requeridas
	ID del conjunto de datos, ID de revisión, nombre del bucket de S3 (por ejemplo, DOC-EXAMPLE-BUCKET), prefijo de la carpeta (por ejemplo, myfolder/) y correo electrónico para notificaciones de SNS. Puede establecer el parámetro Nombre del conjunto de datos con cualquier nombre. Al implementar la plantilla , ejecuta una función de Lambda para incorporar automáticamente el primer conjunto de datos disponible en el conjunto de datos. En adelante, la ingesta posterior se lleva a cabo automáticamente, a medida que llegan nuevos datos al conjunto de datos.	

Recursos relacionados

- Subscribing to data products on AWS Data Exchange (Suscribirse a productos de datos en AWS Data Exchange) (documentación de AWS Data Exchange)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Cree una canalización de datos para incorporar, transformar y analizar los datos de Google Analytics con el kit de DataOps desarrollo de AWS

Creado por Anton Kukushkin (AWS) y Rudy Puig (AWS)

Repositorio de código: ejemplos de DDK de AWS: análisis de datos de Google Analytics con Amazon AppFlow, Amazon Athena y AWS Development Kit DataOps	Entorno: PoC o piloto	Tecnologías: lagos de datos; análisis; infraestructura DevOps
Carga de trabajo: código abierto	Servicios de AWS: Amazon AppFlow; Amazon Athena; AWS CDK; AWS Lambda; Amazon S3	

Resumen

Este patrón describe cómo crear una canalización de datos para incorporar, transformar y analizar los datos de Google Analytics mediante el kit de DataOps desarrollo de AWS (DDK) y otros servicios de AWS. El DDK de AWS es un marco de desarrollo de código abierto que le ayuda a crear flujos de trabajo de datos y arquitecturas de datos modernas en AWS. Uno de los principales objetivos del DDK de AWS es ahorrarle el tiempo y el esfuerzo que normalmente se dedican a tareas de canalización de datos que requieren mucha mano de obra, como la organización de canalizaciones, la creación de infraestructura y la creación de la infraestructura subyacente a esa infraestructura. DevOps Puede delegar estas laboriosas tareas en el DDK de AWS y centrar sus esfuerzos en escribir código y otras actividades de valor.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un AppFlow conector de Amazon para Google Analytics, configurado
- Python y pip (administrador de paquetes de Python)
- Git, instalado y configurado
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada
- AWS Cloud Development Kit (AWS CDK), instalado

Versiones de producto

- Python 3.7 o posterior
- pip 9.0.3 o posterior

Arquitectura

Pila de tecnología

- Amazon AppFlow
- Amazon Athena
- Amazon CloudWatch
- Amazon EventBridge
- Amazon Simple Storage Service (Amazon S3)
- Amazon Simple Queue Service (Amazon SQS)
- Kit de DataOps desarrollo de AWS (DDK)
- AWS Lambda

Arquitectura de destino

El siguiente diagrama muestra el proceso basado en eventos que incorpora, transforma y analiza los datos de Google Analytics.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Una regla de eventos CloudWatch programados de Amazon invoca a Amazon AppFlow.

2. Amazon AppFlow ingiere los datos de Google Analytics en un bucket de S3.
3. Una vez que el bucket de S3 ingiere los datos, EventBridge se generan las notificaciones de eventos, que se capturan mediante una regla de CloudWatch eventos y, a continuación, se colocan en una cola de Amazon SQS.
4. Una función de Lambda consume los eventos de la cola de Amazon SQS, lee los objetos S3 correspondientes, transforma los objetos al formato Apache Parquet, escribe los objetos transformados en el bucket de S3 y, a continuación, crea o actualiza la definición de tabla del catálogo de datos de AWS Glue.
5. Una consulta de Athena realiza comparaciones con la tabla.

Herramientas

Herramientas de AWS

- Amazon AppFlow es un servicio de integración totalmente gestionado que le permite intercambiar datos de forma segura entre aplicaciones de software como servicio (SaaS).
- Amazon Athena es un servicio de consultas interactivo que facilita el análisis de datos en Amazon S3 con SQL estándar.
- Amazon le CloudWatch ayuda a monitorizar las métricas de sus recursos de AWS y las aplicaciones que ejecuta en AWS en tiempo real.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, las funciones de Lambda de AWS, los puntos de conexión de invocación HTTP que utilizan destinos de API o los buses de eventos de otras cuentas de AWS.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Amazon Simple Queue Service (Amazon SQS) ofrece una cola alojada segura, duradera y disponible que le permite integrar y desacoplar sistemas y componentes de software distribuidos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- El AWS Cloud Development Kit (CDK) es un marco para definir la infraestructura de nube en el código y aprovisionarla a través de AWS. CloudFormation

- El kit de DataOps desarrollo de AWS (DDK) es un marco de desarrollo de código abierto que le ayuda a crear flujos de trabajo de datos y una arquitectura de datos moderna en AWS.

Código

El código de este patrón está disponible en los GitHub repositorios AWS DataOps Development Kit (DDK) y Analyzing Google Analytics data with Amazon AppFlow, Amazon Athena y DataOps AWS Development Kit.

Epics

Prepare el entorno

Tarea	Descripción	Habilidades requeridas
Clone el código fuente.	Para clonar el código fuente, ejecute el siguiente comando: `git clone https://github.com/aws-samples/aws-ddk-examples.git`	DevOps ingeniero
Cree un entorno virtual.	Navegue hasta el directorio de código fuente y, a continuación, ejecute el siguiente comando para crear un entorno virtual: `cd google-analytics-data-using-appflow/ python && python3 -m venv .venv`	DevOps ingeniero
Instalar las dependencias.	Para activar el entorno virtual e instalar las dependencias, ejecute el siguiente comando:	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`source .venv/bin/activate && pip install -r requirements.txt`	

Implemente la aplicación que usa su proceso de datos

Tarea	Descripción	Habilidades requeridas
Inicie el entorno.	1. Confirme que la CLI de AWS esté configurada con credenciales válidas para su cuenta de AWS. Para obtener más información, consulte Uso de perfiles con nombre en la documentación de la CLI de AWS. 2. Ejecute el comando `cdk bootstrap --profile [AWS_PROFILE] .`	DevOps ingeniero
Implemente los datos.	Para implementar el proceso de datos, ejecute el comando `cdk deploy --profile [AWS_PROFILE] .`	DevOps ingeniero

Cómo probar la implementación

Tarea	Descripción	Habilidades requeridas
Valide el estado de la pila.	1. Abra la CloudFormation consola de AWS.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	2. En la página Pilas, confirme que el estado de la pila `DdkAppflowAthenaStack` es `CREATE_COMPLETE` .	

Solución de problemas

Problema	Solución
La implementación falla durante la creación de un recurso `AWS::AppFlow::Flow` y recibe el siguiente error: `Connector Profile with name ga-connection does not exist`	Confirma que has creado un AppFlow conector de Amazon para Google Analytics y le has dado un nombre `ga-connection` . Para obtener instrucciones, consulta Google Analytics en la AppFlow documentación de Amazon.

Recursos relacionados

- Kit de DataOps desarrollo de AWS (DDK) (GitHub)
- Ejemplos de SDK de AWS () GitHub

Información adicional

Los procesos de datos de DDK de AWS se componen de una o varias etapas. Los siguientes ejemplos de código emplean `AppFlowIngestionStage` para incorporar datos de Google Analytics, `SqsToLambdaStage` para gestionar la transformación de datos y `AthenaSQLStage` para ejecutar la consulta de Athena.

En primer lugar, se crean las etapas de transformación e incorporación de datos, como se muestra en el siguiente ejemplo de código:

```
        appflow_stage = AppFlowIngestionStage(
```

```
            self,
            id="appflow-stage",
            flow_name=flow.flow_name,
        )
        sqs_lambda_stage = SqsToLambdaStage(
            self,
            id="lambda-stage",
            lambda_function_props={
                "code": Code.from_asset("./ddk_app/lambda_handlers"),
                "handler": "handler.lambda_handler",
                "layers": [
                    LayerVersion.from_layer_version_arn(
                        self,
                        id="layer",
                        layer_version_arn=f"arn:aws:lambda:
{self.region}:336392948345:layer:AWSDataWrangler-Python39:1",
                    )
                ],
                "runtime": Runtime.PYTHON_3_9,
            },
        )
        # Grant lambda function S3 read & write permissions
        bucket.grant_read_write(sqs_lambda_stage.function)
        # Grant Glue database & table permissions
        sqs_lambda_stage.function.add_to_role_policy(
            self._get_glue_db_iam_policy(database_name=database.database_name)
        )
        athena_stage = AthenaSQLStage(
            self,
            id="athena-sql",
            query_string=[
                (
                    "SELECT year, month, day, device, count(user_count) as cnt "
                    f"FROM {database.database_name}.ga_sample "
                    "GROUP BY year, month, day, device "
                    "ORDER BY cnt DESC "
                    "LIMIT 10; "
                )
            ],
            output_location=Location(
                bucket_name=bucket.bucket_name, object_key="query-results/"
            ),
            additional_role_policy_statements=[
                self._get_glue_db_iam_policy(database_name=database.database_name)
```

```
            ],
        )
```

A continuación, la `DataPipeline` construcción se utiliza para «conectar» las etapas mediante EventBridge reglas, como se muestra en el siguiente ejemplo de código:

```
        (
            DataPipeline(self, id="ingestion-pipeline")
            .add_stage(
                stage=appflow_stage,
                override_rule=Rule(
                    self,
                    "schedule-rule",
                    schedule=Schedule.rate(Duration.hours(1)),
                    targets=appflow_stage.targets,
                ),
            )
            .add_stage(
                stage=sqs_lambda_stage,
                # By default, AppFlowIngestionStage stage emits an event after the flow
run finishes successfully
                # Override rule below changes that behavior to call the the stage when
data lands in the bucket instead
                override_rule=Rule(
                    self,
                    "s3-object-created-rule",
                    event_pattern=EventPattern(
                        source=["aws.s3"],
                        detail={
                            "bucket": {"name": [bucket.bucket_name]},
                            "object": {"key": [{"prefix": "ga-data"}]},
                        },
                        detail_type=["Object Created"],
                    ),
                    targets=sqs_lambda_stage.targets,
                ),
            )
            .add_stage(stage=athena_stage)
        )
```

Para ver más ejemplos de código, consulte el GitHub [repositorio Análisis de datos de Google Analytics con Amazon AppFlow, Amazon Athena y AWS DataOps Development Kit](#).

Configurar el acceso entre cuentas a un catálogo de datos de AWS Glue compartido con Amazon Athena

Creado por Denis Avdonin (AWS)

Entorno: producción	Tecnologías: lagos de datos; Análisis, Macrodatos,	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon Athena; AWS Glue		

Resumen

Este patrón proporciona step-by-step instrucciones, incluidos ejemplos de políticas de AWS Identity and Access Management (IAM), para configurar el uso compartido entre cuentas de un conjunto de datos almacenado en un depósito de Amazon Simple Storage Service (Amazon S3) mediante el catálogo de datos de AWS Glue. Puede almacenar el conjunto de datos en un bucket de S3. Un rastreador de AWS Glue recopila los metadatos y los coloca en el catálogo de datos de AWS Glue. El bucket de S3 y el catálogo de datos de AWS Glue residen en una cuenta de AWS denominada cuenta de datos. Puede proporcionar acceso a las entidades principales de IAM en otra cuenta de AWS denominada cuenta de consumidor. Los usuarios pueden consultar los datos de la cuenta del consumidor mediante el motor de consultas sin servidor Amazon Athena.

Requisitos previos y limitaciones

Requisitos previos

- Dos cuentas de AWS activas
- Un bucket de S3 en una de las cuentas de AWS
- Versión 2 del motor Athena
- Interfaz de línea de comandos de AWS (AWS CLI), instalada y configurada (o CloudShellAWS para ejecutar comandos de la CLI de AWS)

Versiones de producto

Este patrón solo funciona con la versión 2 del motor Athena y la versión 3 del motor Athena. Le recomendamos que actualice a la versión 3 del motor Athena. Si no puede actualizar de la versión 1 del motor Athena a la versión 3, siga el enfoque del Acceso multi-cuenta al catálogo de datos de AWS Glue con Amazon Athena en el blog sobre macrodatos de AWS.

Arquitectura

Pila de tecnología de destino

- Amazon Athena
- Amazon Simple Storage Service (Amazon S3)
- AWS Glue
- AWS Identity y Access Management (IAM)
- AWS Key Management Service (AWS KMS)

El siguiente diagrama muestra una arquitectura que usa permisos de IAM para compartir datos de un bucket de S3 en una cuenta de AWS (cuenta de datos) con otra cuenta de AWS (cuenta de consumidor) a través del catálogo de datos de AWS Glue.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. La política de bucket de S3 de la cuenta de datos concede permisos a un rol de IAM en la cuenta de consumidor y al rol de servicio de rastreador de AWS Glue en la cuenta de datos.
2. La clave de AWS KMS de la cuenta de datos concede permisos a un rol de IAM en la cuenta de consumidor y al rol de servicio de rastreador de AWS Glue en la cuenta de datos.
3. El rastreador AWS Glue de la cuenta de datos descubre el esquema de los datos que están almacenados en el bucket de S3.
4. La política de recursos del catálogo de datos de AWS Glue de la cuenta de datos otorga acceso al rol de IAM en la cuenta del consumidor.
5. Un usuario crea una referencia de catálogo con nombre en la cuenta del consumidor mediante un comando de la CLI de AWS.
6. Una política de IAM otorga a un rol de IAM en la cuenta del consumidor el acceso a los recursos de la cuenta de datos. La política de confianza del rol de IAM permite a los usuarios de la cuenta de consumidor asumir el rol de IAM.

7. Un usuario de la cuenta de consumidor asume el rol de IAM y accede a los objetos del catálogo de datos mediante consultas SQL.
8. El motor sin servidor Athena ejecuta las consultas SQL.

Nota: Las prácticas recomendadas de IAM recomiendan conceder permisos a un rol de IAM y utilizar la federación de identidades.

Herramientas

- Amazon Athena es un servicio de consultas interactivo que facilita el análisis de datos en Amazon S3 con SQL estándar.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Glue es un servicio de extracción, transformación y carga (ETL) completamente administrado. Ayuda a clasificar, limpiar, enriquecer y mover datos de forma fiable entre almacenes de datos y flujos de datos.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Key Management Service (AWS KMS) le ayuda a crear y controlar claves criptográficas para proteger sus datos.

Epics

Configura los permisos en la cuenta de datos

Tarea	Descripción	Habilidades requeridas
Conceder acceso a los datos al bucket de S3.	Cree una política de bucket de S3 basada en la siguiente plantilla y asígnela al bucket en el que se almacenan los datos. `{ "Version": "2012-10-17",`	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	"Statement": [{ "Effect": "Allow", "Principal": { "AWS": ["arn:aws:iam::<consumer account id>:role/<role name>", "arn:aws:iam::<data account id>:role/service-role/AWSGlueServiceRole-data-bucket-crawler"] }, "Action": "s3:GetObject", "Resource": "arn:aws:s3:::data-bucket/*" }, { "Effect": "Allow", "Principal": { "AWS": ["arn:aws:iam::<consumer account id>:role/<role name>", "arn:aws:iam::<data account id>:role/service-role/AWSGlueServiceRole-data-bucket-crawler"]	

Tarea	Descripción	Habilidades requeridas
	<pre> }, "Action": "s3:ListBucket", "Resource": "arn:aws:s3:::data- bucket" }] }</pre> La política de bucket concede permisos a un rol de IAM en la cuenta de consumidor y al rol de servicio de rastreador de AWS Glue en la cuenta de datos.	

Tarea	Descripción	Habilidades requeridas
(Si es necesario) Conceda acceso a la clave de cifrado de datos.	Si el bucket de S3 está cifrado con una clave de AWS KMS, conceda el permiso `kms:Decrypt` sobre la clave al rol de IAM en la cuenta del consumidor y al rol de servicio de rastreador de AWS Glue en la cuenta de datos. Actualice la política de claves con la siguiente declaración: `{ "Effect": "Allow", "Principal": { "AWS": [ "arn:aws:iam::<consumer account id>:role/<role name>", "arn:aws:iam::<data account id>:role/service-role/AWSGlueServiceRole-data-bucket-crawler" ] }, "Action": "kms:Decrypt", "Resource": "arn:aws:kms:<region>:<data account id>:key/<key id>" }`	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Conceda al rastreador acceso a los datos.	Adjunte la siguiente política de IAM al rol de servicio del rastreador: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "s3:GetObject", "Resource": "arn:aws:s3:::data-bucket/*" }, { "Effect": "Allow", "Action": "s3:ListBucket", "Resource": "arn:aws:s3:::data-bucket" } ] }`	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
(Si es necesario) Conceda acceso al rastreador a la clave de cifrado de datos.	Si el bucket de S3 está cifrado mediante una clave de AWS KMS, conceda el permiso `kms:Decrypt` sobre la clave al rol de servicio de rastreador adjuntándole la siguiente política: `{ "Effect": "Allow", "Action": "kms:Decrypt", "Resource": "arn:aws:kms:<region>:<data account id>:key/<key id>" }`	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Conceda el rol de IAM en la cuenta del consumidor y al rastreador el acceso al catálogo de datos.	1. Inicie sesión en la consola de administración de AWS y abra la consola de AWS Glue. 2. En el panel de navegación, en Data Catalog (Catálogo de datos), elija Settings (Configuración). 3. En la sección Permissio ns (Permisos), añada la siguiente declaración y, a continuación, seleccione Save (Guardar). `{ "Version" : "2012-10-17", "Statement" : [ { "Effect" : "Allow", "Principa l" : { "AWS" : [ "arn:aws:iam::<con sumer account id>:role/ <role name>", "arn:aws:iam::<dat a account id>:role/ service-role/AWSGl ueServiceRole-data- bucket-crawler" ] }, ...`	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	<pre>"Action" : "glue:*", "Resource" : ["arn:aws:glue:<region>:<data account id>:catalog", "arn:aws:glue:<region>:<data account id>:database/*", "arn:aws:glue:<region>:<data account id>:table/*"] }] }</pre> Esta política permite realizar todas las acciones de AWS Glue en todas las bases de datos y tablas de la cuenta de datos. Puede personalizar la política para conceder únicamente los permisos necesarios a las entidades principales consumidoras. Por ejemplo, puede proporcionar acceso de solo lectura a tablas o vistas específicas de una base de datos.	

Acceda a los datos de la cuenta de consumidor

Tarea	Descripción	Habilidades requeridas
Cree una referencia con nombre para el catálogo de datos.	Para crear una referencia de catálogo de datos con nombre, utilice CloudShelluna AWS CLI instalada localment e para ejecutar el siguiente comando: `aws athena create-da ta-catalog --name <shared catalog name> --type GLUE --paramet ers catalog-id=<data account id>`	Administrador de la nube
Conceder acceso a los datos al rol de IAM en la cuenta del consumidor.	Adjunte la siguiente política al rol de IAM en la cuenta de consumidor para conceder al rol acceso entre cuentas a los datos: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "s3:GetObject", "Resource ": "arn:aws:s3:::data -bucket/*" }, { "Effect": "Allow",`	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	<pre>"Action": "s3:ListBucket", "Resource": "arn:aws:s3:::data-bucket" }, { "Effect": "Allow", "Action": "glue:*", "Resource": ["arn:aws:glue:<region>:<data account id>:catalog", "arn:aws:glue:<region>:<data account id>:database/*", "arn:aws:glue:<region>:<data account id>:table/*"] }] }</pre> A continuación, utilice la siguiente plantilla para especificar qué usuarios pueden aceptar el rol de IAM en su política de confianza: <pre>{ "Version": "2012-10-17", "Statement": [</pre>	

Tarea	Descripción	Habilidades requeridas
	<pre>{ "Effect": "Allow", "Principal": { "AWS": "arn:aws:iam::<consumer account id>:user/<IAM user>" }, "Action": "sts:AssumeRole" }] }</pre> Por último, conceda permisos a los usuarios para que asuman el rol de IAM adjuntando la misma política al grupo de usuarios al que pertenecen.	

Tarea	Descripción	Habilidades requeridas
(Si es necesario) Conceda acceso a la clave de cifrado de datos al rol de IAM en la cuenta del consumidor.	Si el bucket de S3 está cifrado mediante una clave de AWS KMS, conceda el permiso `kms:Decrypt` sobre la clave al rol de IAM en la cuenta de consumidor adjuntándole la siguiente política: `{ "Effect": "Allow", "Action": "kms:Decrypt", "Resource": "arn:aws:kms:<region>:<data account id>:key/<key id>" }`	Administrador de la nube
Cambie al rol de IAM en la cuenta del consumidor para acceder a los datos.	Cambie al rol de IAM en la cuenta del consumidor para acceder a los datos.	Consumidor de datos

Tarea	Descripción	Habilidades requeridas
Acceda a los datos.	Realizar consultas mediante Athena. Por ejemplo, abra el editor de consultas de Athena y ejecute la siguiente consulta: `SELECT * FROM <shared catalog name>.<database name>.<table name>` En lugar de utilizar una referencia de catálogo con nombre, también puede hacer referencia al catálogo por su nombre de recurso de Amazon (ARN). Nota: Si utiliza una referencia de catálogo dinámica en una consulta o vista, ponga la referencia entre comillas dobles escapadas (\"). Por ejemplo: `SELECT * FROM \"glue:arn:aws:glue:<region>:<data account id>:catalog\".<database name>.<table name>` Para obtener más información, consulte Acceso entre cuentas a los catálogos de datos de	Consumidor de datos

Tarea	Descripción	Habilidades requeridas
	AWS Glue en la Guía del usuario de Amazon Athena.	

Recursos relacionados

- Acceso entre cuentas a los catálogos de datos de AWS Glue (documentación de Athena)
- (AWS CLI) create-data-catalog (Referencia de comandos de la CLI de AWS)
- Acceso entre cuentas al catálogo de datos de AWS Glue con Amazon Athena (blog sobre macrodatos de AWS)
- Prácticas recomendadas de seguridad en IAM (documentación de IAM)

Información adicional

Uso de Lake Formation como alternativa para compartir entre cuentas

También puede usar AWS Lake Formation para compartir el acceso a los objetos del catálogo de AWS Glue entre cuentas. Lake Formation proporciona un control de acceso detallado a nivel de columnas y filas, control de acceso basado en etiquetas, tablas gobernadas para transacciones ACID y otras funciones. Aunque Lake Formation está bien integrado con Athena, requiere una configuración adicional en comparación con el enfoque exclusivo de IAM de este patrón. Recomendamos que considere la decisión de utilizar los controles de acceso exclusivos de Lake Formation o IAM en el contexto más amplio de la arquitectura general de su solución. Las consideraciones incluyen qué otros servicios están involucrados y cómo se integran con ambos enfoques.

Automatización del intercambio de datos entre cuentas

Creado por Issam Habibi (AWS), Louis Hourcade (AWS) y Madalena Calvo (AWS)

Entorno: PoC o piloto	Tecnologías: lagos de datos; análisis	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: AWS Glue; AWS Lake Formation; AWS RAM; Amazon Athena		

Resumen

Tener varias unidades de negocio (BUs) independientes dentro de una organización significa que el control estricto de los permisos de acceso al lago de datos debe ser una prioridad absoluta y que cada BU debe acceder solo a sus propios datos. Sin embargo, las cargas de trabajo de una BU pueden interesar a otra BU con fines analíticos, lo que suscita interés en torno al tema del intercambio de datos entre distintas BU, con un control de permisos detallado.

En esta página, suponemos que una BU está asignada a una cuenta de AWS que aloja sus datos (Glue rastreó las bases de datos desde S3) y, por lo tanto, el intercambio de datos entre BU se convierte en un problema de intercambio de datos entre cuentas de AWS. Proporcionaremos una forma automatizada de compartir tablas específicas de una base de datos de Glue con el director de una cuenta externa de AWS mediante Lake Formation. Esta automatización permitirá a los propietarios de los datos conceder a las BUs externas el derecho a ejecutar consultas de análisis (utilizando Athena, por ejemplo) en tablas definidas.

Puede utilizar esta solución automatizada para cumplir con un caso de uso típico, como:

El equipo de datos de recursos humanos estará alojado en una cuenta de AWS de origen que compartirá la tabla de sueldos con la cuenta de AWS de destino del equipo de analistas de datos para realizar consultas adicionales con Athena.

Requisitos previos y limitaciones

Requisitos previos

Para esta implementación, necesitará:

- dos cuentas de AWS (cuenta de origen y cuenta de destino) con permisos suficientes para implementar los recursos de AWS incluidos en este código
- aws-cdk: instalado globalmente (npm install -g aws-cdk)
- cliente git
- Al menos una base de datos de Glue rastreada con tablas.
- En la sección de epopeyas se muestran pocas configuraciones manuales de Lake Formation

Limitaciones

- Esta solución requiere que las bases de datos de Glue ya estén rastreadas en la cuenta de origen de AWS.

- Esta solución aún no proporciona una forma automática de revocar los permisos concedidos. Una vez que compartas los datos de una cuenta de origen con una cuenta de destino, la revocación del acceso debe hacerse manualmente en la consola de Lake Formation.

Arquitectura

Descripción general de la solución

Este código CDK implementa la arquitectura que se resume en el siguiente diagrama

En particular, incluye:

Pila de cuentas de origen:

- DynamoDb tabla: esta tabla contiene las definiciones de permisos de uso compartido que carga un usuario. Tiene las DynamoDb transmisiones activadas y activa una lambda para cada elemento de permisos de uso compartido que se añada a la tabla.
- Una función lambda: concede los permisos especificados en una tabla a un principal externo.

Pila de cuentas de destino:

- Resource Access Manager (RAM): recibe invitaciones de Lake Formation. Se debe aceptar una invitación para poder acceder a los datos compartidos.
- Amazon SQS: recibe mensajes de la cuenta de origen que indican que se ha iniciado un procedimiento de compartición
- EventBridge regla: esta regla se activa una vez que se acepta una invitación de RAM.
- Dos funciones Lambda: una activada por la cola de SQS que acepta automáticamente las invitaciones de RAM y una segunda función activada por la EventBridge regla que crea la base de datos compartida local y los enlaces de recursos a los recursos compartidos. Esos enlaces de recursos se pueden consultar más a fondo con Athena.

El proceso podría resumirse en los siguientes pasos:

1: un usuario carga el elemento de definición del recurso compartido en la tabla de DynamoDB de la cuenta de origen.

2- DynamoDb Streams activa la cuenta de origen lambda, que comparte la tabla de la base de datos especificada en el elemento de definición de acciones con la cuenta de destino mediante la formación de lagos. Al compartir, se envía automáticamente una invitación de RAM a la cuenta de destino.

3- La cuenta de origen lambda también envía un mensaje a una cola de SQS de la cuenta de destino para avisarla del inicio del procedimiento de uso compartido.

4- En la cuenta de destino, la cola SQS activa una lambda que acepta la invitación de RAM recibida.

5- Tras aceptar la invitación, una EventBridge regla activa una lamdba que crea una base de datos local y un enlace de recursos que contendrá la tabla compartida. Esta lambda también otorga permisos sobre los datos compartidos al principal de destino.

6- el director puede consultar datos con Athena.

Herramientas

Repositorio de códigos

El código de este patrón está disponible en Gitlab

Prácticas recomendadas

- Como se mencionó anteriormente, es obligatorio que ya tengas una base de datos rastreada por Glue en tu cuenta.
- Los nombres de las bases de datos y de las tablas deben coincidir con los de la base de datos rastreada por Glue.
- El elemento de entrada para compartir que se insertará en DynamoDB tendrá el siguiente aspecto:

Epics

Clona el repositorio y configura la implementación

Tarea	Descripción	Habilidades requeridas
Clone el repositorio	Clona el repositorio de gitlab en tu máquina `git clone git@ssh.gitlab.aws.dev:ihabibi/cross-account-data-sharing.git` `cd cross-account-data-sharing`	AWS general
Configura tu despliegue	Edite el `resources.py` archivo con información sobre la región, las cuentas de origen/destino que está utilizando y el arn principal de destino `AWS_REGION = 'eu-west-1'` `AWS_SOURCE_ACCOUNT_ID = '111111111111'`	AWS general

Tarea	Descripción	Habilidades requeridas
	`AWS_TARGET_ACCOUNT_ID = '222222222222' TARGET_PRINCIPAL_ARN = 'arn:aws:iam::222222222222:role/admin'`	

Inicie su cuenta de AWS e implemente el código

Tarea	Descripción	Habilidades requeridas
Inicie su cuenta de AWS de origen	Si aún no lo ha hecho, debe iniciar su entorno de AWS antes de implementar esta aplicación de CDK. Ejecute los siguientes comandos con las credencia les de AWS de su cuenta de AWS de origen: `cdk bootstrap aws://<source-account-id>/<aws-region>`	AWS general
Implemente la pila de CDK de origen	Ahora que su cuenta de AWS de origen está iniciada y que ha configurado la implement ación, puede implementar la aplicación CDK con el siguiente comando: (asegúrese de estar en el cross-account-data-sharing directorio/)	AWS general

Tarea	Descripción	Habilidades requeridas
	`cdk deploy SourceAccountStack`	
Inicie su cuenta de AWS de destino	Si aún no lo ha hecho, debe iniciar su entorno de AWS antes de implementar esta aplicación de CDK. Ejecute los siguientes comandos con las credenciales de AWS de su cuenta de AWS de destino: `cdk bootstrap aws://<target-account-id>/<aws-region>`	AWS general
Implemente la pila de CDK de destino	Ahora que su cuenta de AWS de destino está iniciada y que ha configurado la implementación, puede implementar la aplicación CDK con el siguiente comando: (asegúrese de estar en el cross-account-data-sharing directorio/) `cdk deploy TargetAccountStack`	AWS general

Configura Lake Formation en la cuenta de origen

Tarea	Descripción	Habilidades requeridas
Configura Lake Formation en la cuenta de origen	• En la cuenta de origen, inicie sesión en la consola de Lake Formation y vaya a Registrar e ingerir -> Ubicaciones de lagos de datos. Registre la ubicación S3 de sus datos. • vaya a Permisos -> Permisos del lago de datos. Revoca todos los permisos de IAMAllowedGroup .	

Pruebe el uso compartido de cuentas cruzadas

Tarea	Descripción	Habilidades requeridas
Comparta una tabla de la cuenta de origen a la de destino	• Inicia sesión en la consola de tu cuenta de origen, busca la tabla «permissi ons_table» e inserta un elemento siguiendo este esquema. DynamoDb También puede usar AWS CLI `{ "share_id": "1", "table_name": "sample_data", "database_name": "database-ohio", "permissions": "DESCRIBE,SELECT",`	AWS general

Tarea	Descripción	Habilidades requeridas
	<pre>"source_acc_id": "111111111111", "target_acc_id": "222222222222" }</pre> Una vez insertado el elemento en la tabla, se desencadena todo el proceso y la tabla estará lista para ser consultada en cuestión de segundos en la cuenta de destino. • Tenga en cuenta que los permisos posibles son DESCRIBIR y SELECCIONAR. Deben estar separados por una coma.	
Consulta la tabla de la cuenta de destino	• Inicia sesión en la consola de tu cuenta objetivo y verás que Lake Formation ya reconoce la tabla compartida y puedes consultarla con Athena.	

Recursos relacionados

Codifica en Gitlab

Información adicional

Documentación de los principales servicios utilizados:

Amazon DynamoDb

AWS Lambda

AWS Lake Formation

AWS Glue

AWS Resource Access Manager

Amazon SQS

Implementar y administrar un lago de datos sin servidor en la nube de AWS mediante el uso de la infraestructura como código

Entorno: producción	Tecnologías: lagos de datos; análisis; sin servidor; DevOps	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon S3; Amazon SQS; AWS CloudFormation; AWS Glue; Amazon; AWS Lambda CloudWatch; AWS Step Functions; Amazon DynamoDB		

Resumen

Este patrón describe cómo utilizar la computación sin servidor y la infraestructura como código (IaC) para implementar y administrar un lago de datos en la nube de Amazon Web Services (AWS). Este patrón se basa en el taller sobre el marco de lago de datos sin servidor (SDLF) desarrollado por AWS.

El SDLF es un conjunto de recursos reutilizables que aceleran la entrega de lagos de datos empresariales en la nube de AWS y permiten una implementación más rápida en la producción. Se utiliza para implementar la estructura fundamental de un lago de datos siguiendo las prácticas recomendadas.

SDLF implementa un proceso de integración e implementación continuas (CI/CD) durante todo el despliegue del código y la infraestructura mediante servicios de AWS como AWS, CodePipeline AWS CodeBuild y AWS. CodeCommit

Este patrón utiliza varios servicios sin servidor de AWS para simplificar la administración de los lagos de datos. Entre ellas se incluyen Amazon Simple Storage Service (Amazon S3) y Amazon DynamoDB para el almacenamiento, AWS Lambda y AWS Glue para la informática, y Amazon Events, Amazon Simple Queue Service (Amazon SQS) CloudWatch y AWS Step Functions para la orquestación.

AWS CloudFormation y los servicios de código de AWS actúan como capa IaC para proporcionar implementaciones rápidas y reproducibles con operaciones y administración sencillas.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada.
- Un cliente Git, instalado y configurado.
- El taller de SDLF, abierto en la ventana de un navegador web y listo para usar.

Arquitectura

El diagrama de arquitectura ilustra un proceso basado en eventos con los siguientes pasos.

1. Tras añadir un archivo al bucket de datos sin procesar de S3, se coloca una notificación de evento de Amazon S3 en una cola de SQS. Cada notificación se entrega como un archivo JSON, que contiene metadatos como el nombre del bucket de S3, la clave del objeto o la marca de tiempo.
2. Esta notificación la consume una función de Lambda que enruta el evento al proceso correcto de extracción, transformación y carga (ETL) en función de los metadatos. La función de Lambda también puede usar configuraciones contextuales almacenadas en una tabla de Amazon DynamoDB. Este paso permite desacoplar y escalar múltiples aplicaciones en el lago de datos.
3. El evento se dirige a la primera función de Lambda del proceso ETL, que transforma y mueve los datos del área de datos sin procesar al área de almacenamiento del lago de datos. El primer paso es actualizar el catálogo completo. Se trata de una tabla de DynamoDB que contiene todos los metadatos de archivos del lago de datos. Cada fila de esta tabla contiene metadatos operativos sobre un único objeto almacenado en Amazon S3. Se realiza una llamada sincrónica a una función de Lambda que realiza una ligera transformación, que es una operación económica desde el punto de vista computacional (como convertir un archivo de un formato a otro), en el objeto S3. Como se ha agregado un objeto nuevo al bucket provisional de S3, se actualiza el catálogo completo y se envía un mensaje a la cola de SQS a la espera de la siguiente fase de ETL.

4. Una regla de CloudWatch eventos activa una función Lambda cada 5 minutos. Esta función comprueba si los mensajes de la fase ETL anterior se enviaron a la cola de SQS. Si se ha entregado un mensaje, la función de Lambda inicia la segunda función desde AWS Step Functions en el proceso ETL.
5. A continuación, se aplica una transformación profunda a un lote de archivos. Esta importante transformación es una operación costosa desde el punto de vista computacional, como una llamada sincrónica a un trabajo de AWS Glue, una tarea de AWS Fargate, un paso de Amazon EMR o un bloc de notas de Amazon. SageMaker Los metadatos de las tablas se extraen de los archivos de salida mediante un rastreador de AWS Glue, que actualiza el catálogo de AWS Glue. Los metadatos de los archivos también se añaden a la tabla de catálogo completa de DynamoDB. Por último, también se ejecuta un paso de calidad de datos aprovechando Deequ.

Pila de tecnología

- CloudWatch Eventos de Amazon
- AWS CloudFormation
- AWS CodePipeline
- AWS CodeBuild
- AWS CodeCommit
- Amazon DynamoDB
- AWS Glue
- AWS Lambda
- Amazon S3
- Amazon SQS
- AWS Step Functions

Herramientas

- Amazon CloudWatch Events — CloudWatch Events ofrece una transmisión casi en tiempo real de los eventos del sistema que describen los cambios en los recursos de AWS.
- AWS CloudFormation: CloudFormation ayuda a crear y aprovisionar las implementaciones de infraestructura de AWS de forma predecible y repetitiva.

- AWS CodeBuild: CodeBuild es un servicio de compilación totalmente gestionado que compila el código fuente, ejecuta pruebas unitarias y produce artefactos listos para su implementación.
- AWS CodeCommit: CodeCommit es un servicio de control de versiones hospedado por AWS que puede usar para almacenar y administrar activos de forma privada (como código fuente y archivos binarios).
- AWS CodePipeline: CodePipeline es un servicio de entrega continua que puede utilizar para modelar, visualizar y automatizar los pasos necesarios para publicar los cambios de software de forma continua.
- Amazon DynamoDB: DynamoDB es un servicio de base de datos NoSQL totalmente administrado que ofrece un rendimiento rápido y predecible, así como escalabilidad.
- AWS Glue: AWS Glue es un servicio ETL totalmente gestionado que facilita la preparación y la carga de datos para su análisis.
- AWS Lambda: Lambda admite la ejecución de código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos altamente escalable. Amazon S3 se puede utilizar para una amplia gama de soluciones de almacenamiento, incluyendo sitios web, aplicaciones móviles, copias de seguridad y lagos de datos.
- AWS Step Functions: AWS Step Functions es un orquestador de funciones sin servidor que facilita la secuenciación de las funciones de AWS Lambda y varios servicios de AWS en aplicaciones esenciales desde el punto de vista empresarial.
- Amazon SQS: Amazon Simple Queue Service (Amazon SQS) es un servicio de cola de mensajes totalmente gestionado que le permite desacoplar y escalar microservicios, sistemas distribuidos y aplicaciones sin servidor.
- Deequ: Deequ es una herramienta que le ayuda a calcular las métricas de calidad de los datos para conjuntos de datos de gran tamaño, a definir y verificar las limitaciones de calidad de los datos y a mantenerse informado sobre los cambios en la distribución de los datos.

Código

El código fuente y los recursos del SDLF están disponibles en el GitHub repositorio de AWS Labs.

Epics

Configurar la canalización de CI/CD para aprovisionar la IaC

Tarea	Descripción	Habilidades requeridas
Configure la canalización de CI/CD para administrar la IaC para el lago de datos.	Inicie sesión en la consola de administración de AWS y siga los pasos de la sección de Configuración inicial del taller de SDLF. Esto crea los recursos de CI/CD iniciales , como los CodeCommit repositorios, los CodeBuild entornos y las CodePipeline canalizaciones que aprovisio nan y administran la IaC para el lago de datos.	DevOps ingeniero

Control de versiones de la IaC

Tarea	Descripción	Habilidades requeridas
Clona el CodeCommit repositorio en tu máquina local.	Siga los pasos de la sección Implementación de los fundamentos del taller sobre el SDLF. Esto le ayuda a clonar el repositorio de Git que aloja la IaC en su entorno local. Para obtener más informaci ón, consulte Conectarse a CodeCommit repositorios en la CodeCommit documenta ción.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Modifique las CloudFormation plantillas.	Utilice su estación de trabajo local y un editor de código para modificar las CloudFormation plantillas según sus casos de uso o requisitos. Configúrelos en el repositorio de Git clonado localmente. Para obtener más información, consulte Trabajar con CloudFormation plantillas de AWS en la CloudFormation documentación de AWS.	DevOps ingeniero
Envía los cambios al CodeCommit repositorio.	Su código de infraestructura está ahora bajo control de versiones y se realiza un seguimiento de las modificaciones de su base de código. Cuando introduce un cambio en el CodeCommit repositorio, lo aplica CodePipeline automáticamente a su infraestructura y lo envía allí CodeBuild. Importante: Si utiliza la CLI de AWS SAM CodeBuild, ejecute los `sam deploy` comandos `sam package` y. Si usa la CLI de AWS, ejecute los comandos `aws cloudformation package` y `aws cloudformation deploy` .	DevOps ingeniero

Recursos relacionados

Configurar la canalización de CI/CD para aprovisionar la IaC

- Taller sobre el SDLF: Configuración inicial

Control de versiones de la IaC

- Taller sobre SDLF: Implementando las bases
- Conectarse a CodeCommit repositorios
- Trabajar con CloudFormation plantillas de AWS

Otros recursos

- Arquitectura de referencia de la canalización de análisis de datos sin servidor de AWS
- Documentación de SDLF

Capturar datos de IoT directamente en Amazon S3 de forma rentable con AWS IoT Greengrass

Creado por Sebastian Viviani (AWS) y Rizwan Syed (AWS)

Entorno: PoC o piloto	Tecnologías: lagos de datos; análisis; IoT	Carga de trabajo: código abierto
Servicios de AWS: AWS IoT Greengrass; Amazon S3; Amazon Athena		

Resumen

Este patrón le muestra cómo incorporar datos de Internet de las cosas (IoT) de forma rentable directamente en un depósito de Amazon Simple Storage Service (Amazon S3) mediante un dispositivo AWS IoT Greengrass versión 2. El dispositivo ejecuta un componente personalizado que lee los datos de IoT y los guarda en un almacenamiento persistente (es decir, un disco o volumen local). A continuación, el dispositivo comprime los datos de IoT en un archivo de Apache Parquet y los carga periódicamente en un bucket de S3.

La cantidad y la velocidad de los datos de IoT que ingiere están limitadas únicamente por las capacidades de su hardware periférico y el ancho de banda de la red. Puede utilizar Amazon Athena para analizar de forma rentable los datos ingeridos. Athena admite archivos comprimidos de Apache Parquet y la visualización de datos mediante el uso de Amazon Managed Grafana.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una puerta de enlace perimetral que se ejecuta en AWS IoT Greengrass versión 2 y recopila datos de los sensores (las fuentes de datos y el proceso de recopilación de datos están fuera del alcance de este patrón, pero puede usar casi cualquier tipo de datos de sensores). Este patrón utiliza un intermediario MQTT local con sensores o puertas de enlace que publican los datos de forma local.
- Componentes, roles y dependencias del SDK de AWS IoT Greengrass

- Un componente de administrador de transmisiones para cargar los datos al bucket de S3
- AWS SDK para Java, AWS SDK para JavaScript o AWS SDK para Python (Boto3) para ejecutar las API

Limitaciones

- Los datos de este patrón no se cargan en tiempo real en el bucket de S3. Hay un período de retraso y puede configurarlo. Los datos se almacenan temporalmente en el dispositivo perimetral y, una vez transcurrido el período, se cargan.
- El SDK está disponible en Java, Node.js o Python.

Arquitectura

Pila de tecnología de destino

- Amazon S3
- AWS IoT Greengrass
- Intermediario MQTT
- Componente Stream Manager

Arquitectura de destino

El siguiente diagrama muestra una arquitectura diseñada para capturar datos de sensores de IoT y almacenarlos en un bucket de S3.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Las actualizaciones de varios sensores (por ejemplo, de temperatura y válvula) se publican en un agente de MQTT local.
2. El compresor de archivos Parquet que está suscrito a estos sensores actualiza los temas y recibe estas actualizaciones.
3. El compresor de archivos Parquet almacena las actualizaciones de forma local.
4. Una vez transcurrido el período, los archivos almacenados se comprimen en archivos Parquet y se pasan al administrador de flujos para cargarlos en el bucket de S3 especificado.

5. El administrador de transmisión carga los archivos de Parquet en el bucket de S3.

Nota: el administrador de transmisiones (`StreamManager`) es un componente administrado. Para ver ejemplos de cómo exportar datos a Amazon S3, consulte Stream Manager en la documentación de AWS IoT Greengrass. Puede utilizar un bróker MQTT local como componente u otro bróker como Eclipse Mosquitto.

Herramientas

Herramientas de AWS

- Amazon Athena es un servicio de consultas interactivo que facilita el análisis de datos en Amazon S3 con SQL estándar.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS IoT Greengrass es un servicio en la nube y de tiempo de ejecución de borde de IoT de código abierto que lo ayuda a crear, implementar y administrar aplicaciones de IoT en los dispositivos.

Otras herramientas

- Apache Parquet es un formato de almacenamiento de archivos de código abierto diseñado originalmente para Hadoop.
- El MQTT (Message Queuing Telemetry Transport) es un protocolo de mensajería ligero diseñado para dispositivos restringidos.

Prácticas recomendadas

Utilice el formato de partición adecuado para los datos cargados

No hay requisitos específicos para los nombres de los prefijos raíz del bucket de S3 (por ejemplo, `"myAwesomeDataSet/"` o`"dataFromSource"`), pero le recomendamos que utilice una partición y un prefijo significativos para que sea fácil entender el propósito del conjunto de datos.

También le recomendamos que utilice la partición correcta en Amazon S3 para que las consultas se ejecuten de forma óptima en el conjunto de datos. En el siguiente ejemplo, los datos se dividen en

formato HIVE para optimizar la cantidad de datos escaneados por cada consulta de Athena. Esto puede mejorar el rendimiento y reducir los costos.

`s3://<ingestionBucket>/<rootPrefix>/year=YY/month=MM/day=DD/HHMM_<suffix>.parquet`

Epics

Configure su entorno

Tarea	Descripción	Habilidades requeridas
Crear un bucket de S3.	1. Crear un bucket de S3 o utilice uno existente. 2. Cree un prefijo significativo para el depósito de S3 en el que desee capturar los datos de IoT (por ejemplo,`s3:\\<bucket>\<prefix>`). 3. Registre su prefijo para usarlo más adelante.	Desarrollador de aplicaciones
Añada permisos de IAM al bucket de S3.	Para conceder a los usuarios acceso de escritura al bucket y al prefijo de S3 que creó anteriormente, añada la siguiente política de IAM a su rol de AWS IoT Greengrass: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "S3DataUpload", "Effect": "Allow",`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	<pre>"Action": ["s3:List*", "s3:Put*"], "Resource": ["arn:aws:s3:::<ingestionBucket>", "arn:aws:s3:::<ingestionBucket>/<prefix>/*"] }] }</pre> Para obtener más información, consulte Creación de una política de IAM para acceder a los recursos de Amazon S3 en la documentación de Aurora. A continuación, actualice la política de recursos (si es necesario) del bucket de S3 para permitir el acceso de escritura con los principios de AWS correctos.	

Cree e implemente el componente AWS IoT Greengrass

Tarea	Descripción	Habilidades requeridas
Actualizar la receta del componente.	Actualice la configuración del componente al crear una implementación según el siguiente ejemplo: `{ "region": "<region>", "parquet_period": <period>, "s3_bucket": "<s3Bucket>", "s3_key_prefix": "<s3prefix>" }` `<region>`Sustitúyalo por su región `<period>` de AWS, su intervalo periódico, `<s3Bucket>` su bucket de S3 y `<s3prefix>` por su prefijo.	Desarrollador de aplicaciones
Crear el componente.	Realice una de las acciones siguientes: • Crear un componente. • Añada el componente a la canalización de CI/CD (si existe). Asegúrese de copiar el artefacto del repositorio de artefactos al depósito de artefactos de AWS IoT Greengrass. A continuac ión, cree o actualice su	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	componente AWS IoT Greengrass. • Añada el agente MQTT como componente o agréguelo manualmente más adelante. Nota: esta decisión afecta al esquema de autenticación que puede utilizar con el bróker. Al añadir manualmente un agente, se desvincula el agente de AWS IoT Greengrass y se habilita cualquier esquema de autenticación compatible del agente. Los componentes de agente proporcionados por AWS tienen esquemas de autenticación predefinidos. Para obtener más información, consulte el agente MQTT 3.1.1 (Moquette) y el agente MQTT 5 (EMQX).	

Tarea	Descripción	Habilidades requeridas
Actualice el cliente MQTT.	El código de ejemplo no utiliza la autenticación porque el componente se conecta localmente al intermediario. Si su situación es diferente , actualice la sección del cliente de MQTT según sea necesario. Además, realice lo siguiente: 1. Actualice los temas de MQTT de la suscripción. 2. Actualice el analizador de mensajes MQTT según sea necesario, ya que los mensajes de cada fuente pueden diferir.	Desarrollador de aplicaciones

Añada el componente al dispositivo principal de AWS IoT Greengrass versión 2

Tarea	Descripción	Habilidades requeridas
Actualice la implementación del dispositivo principal.	Si la implementación del dispositivo principal de AWS IoT Greengrass versión 2 ya existe, revise la implement ación. Si la implementación no existe, cree una nueva. Para asignar al componente el nombre correcto, actualice la configuración del administr ador de registros para el nuevo componente (si es	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	necesario) en función de lo siguiente: `{ "logsUploaderConfiguration": { "systemLogsConfiguration": { ... }, "componentLogsConfigurationMap": { "<com.iot.ingest.parquet>": { "minimumLogLevel": "INFO", "diskSpaceLimit": "20", "diskSpaceLimitUnit": "MB", "deleteLogFileAfterCloudUpload": "false" } ... } }, "periodicUploadIntervalSec": "300" }` Por último, complete la revisión de la implementación de su dispositivo principal AWS IoT Greengrass.	

Verifique la captura de datos en el depósito de S3

Tarea	Descripción	Habilidades requeridas
Compruebe los registros del volumen de AWS IoT Greengrass.	Compruebe lo siguiente: • El cliente MQTT se ha conectado correctamente al agente MQTT local. • El cliente MQTT está suscrito a los temas correctos. • Están llegando al bróker mensajes de actualización de sensores sobre temas relacionados con el MQTT. • La compresión de parquet se produce en cada intervalo periódico.	Desarrollador de aplicaciones
Compruebe el bucket de S3.	Compruebe si los datos se cargan en el bucket de S3. Puede ver los archivos que se están cargando en cada período. También puede comprobar si los datos se han cargado en el depósito de S3 consultan do los datos en la siguiente sección.	Desarrollador de aplicaciones

Configurar consultas desde Athena

Tarea	Descripción	Habilidades requeridas
Crear una base de datos y tabla.	1. Cree una base de datos de AWS Glue (si es necesario). 2. Cree una tabla en AWS Glue manualmente o ejecute un rastreador en AWS Glue.	Desarrollador de aplicaciones
Concede a Athena acceso a los datos.	1. Actualice los permisos para permitir que Athena acceda al bucket de S3. Para obtener más información, consulte Acceso detallado a bases de datos y tablas en el catálogo de datos de AWS Glue en la documentación de Athena. 2. Consulte la tabla en su base de datos.	Desarrollador de aplicaciones

Solución de problemas

Problema	Solución
El cliente MQTT no se puede conectar	• Validar los permisos en el bróker MQTT. Si tiene un bróker MQTT de AWS, consulte Broker MQTT 3.1.1 (Moquette) y MQTT 5 Broker (EMQX). • Validar las credenciales en el cliente MQTT. Si tiene un bróker MQTT de AWS, consulte

Problema	Solución
	Broker MQTT 3.1.1 (Moquette) y MQTT 5 Broker (EMQX).
El cliente MQTT no se suscribe	Validar los permisos en el bróker MQTT. Si tiene un bróker MQTT de AWS, consulte Broker MQTT 3.1.1 (Moquette) y MQTT 5 Broker (EMQX).
Los archivos Parquet no se crean	• Compruebe que los temas de MQTT son correctos. • Compruebe que los mensajes de MQTT de los sensores tengan el formato correcto.
Los objetos no se cargan en el bucket de S3	• Compruebe que dispone de conectividad a Internet y de un punto de conexión. • Compruebe que la política de recursos de su bucket de S3 sea correcta. • Compruebe los permisos para la función de dispositivo principal de AWS IoT Greengrass versión 2.

Recursos relacionados

- DataFrame(documentación de Pandas)
- Documentación de Apache Parquet (documentación de Parquet)
- Desarrollo de componentes de AWS IoT Greengrass (Guía para desarrolladores de AWS IoT Greengrass, versión 2)
- Implemente componentes de AWS IoT Greengrass en dispositivos (Guía para desarrolladores de AWS IoT Greengrass, versión 2)
- Interactúe con dispositivos de IoT locales (Guía para desarrolladores de AWS IoT Greengrass, versión 2)
- Broker MQTT 3.1.1 (Moquette) (Guía para desarrolladores de AWS IoT Greengrass, versión 2)
- Broker MQTT 5 (EMQX) (Guía para desarrolladores de AWS IoT Greengrass, versión 2)

Información adicional

Análisis de costos

El siguiente escenario de análisis de costos demuestra cómo el enfoque de captura de datos incluido en este patrón puede afectar los costos de captura de datos en la nube de AWS. Los ejemplos de precios de este escenario se basan en los precios vigentes en el momento de la publicación. Los precios están sujetos a cambios. Además, los costos pueden variar en función de la región de AWS, las Service quotas de AWS y otros factores relacionados con el entorno de nube.

Conjunto de señales de entrada

Este análisis utiliza el siguiente conjunto de señales de entrada como base para comparar los costos de captura de IoT con otras alternativas disponibles.

Número de señales	Frecuencia	Datos por señal
125	25 Hz	8 bytes

En este escenario, el sistema recibe 125 señales. Cada señal es de 8 bytes y se produce cada 40 milisegundos (25 Hz). Estas señales pueden venir individualmente o agrupadas en una carga útil común. Tiene la opción de dividir y empaquetar estas señales según sus necesidades. También puede determinar la latencia. La latencia consiste en el período de tiempo para recibir, acumular y capturar los datos.

A modo de comparación, la operación de captura de este escenario se basa en la región de AWS de `us-east-1`. La comparación de costos se aplica únicamente a los servicios de AWS. Otros costos, como el hardware o la conectividad, no se tienen en cuenta en el análisis.

Comparaciones de costos

La siguiente tabla muestra el coste mensual en dólares estadounidenses (USD) de cada método de ingestión.

Método	Coste mensual
AWS SiteWise IoT*	331,77 USD

AWS IoT SiteWise Edge con paquete de procesamiento de datos (mantiene todos los datos en el borde)	200 USD
Reglas de AWS IoT Core y Amazon S3 para acceder a datos sin procesar	84,54 USD
Compresión de archivos Parquet en el borde y carga a Amazon S3	0,5 USD

*Los datos se deben reducir para cumplir con las Service quotas. Esto significa que se pierden algunos datos con este método.

Métodos alternativos

En esta sección se muestran los costos equivalentes de los siguientes métodos alternativos:

- AWS IoT SiteWise: cada señal debe cargarse en un mensaje individual. Por lo tanto, la cantidad total de mensajes por mes es de 125 × 25 × 3600 × 24 × 30, o sea, 8 100 millones de mensajes por mes. Sin embargo, AWS IoT solo SiteWise puede gestionar 10 puntos de datos por segundo por propiedad. Suponiendo que los datos se reduzcan a 10 Hz, la cantidad de mensajes por mes se reduce a 125 × 10 × 3600 × 24 × 30, o sea, 3,24 mil millones. Si utiliza el componente de publicación que agrupa las medidas en grupos de 10 (a 1 USD por millón de mensajes), el coste mensual será de 324 USD al mes. Suponiendo que cada mensaje tenga 8 bytes (1 Kb/125), se trata de 25,92 GB de almacenamiento de datos. Esto añade un coste mensual de 7,77 USD. El coste total del primer mes es de 331,77 USD y aumenta 7,77 USD cada mes.
- AWS IoT SiteWise Edge con paquete de procesamiento de datos, que incluye todos los modelos y señales completamente procesados en el borde (es decir, sin ingesta de nubes): puede usar el paquete de procesamiento de datos como alternativa para reducir los costos y configurar todos los modelos que se calculan en el borde. Esto puede funcionar solo para el almacenamiento y la visualización, incluso si no se realiza ningún cálculo real. En este caso, es necesario utilizar un hardware potente para la puerta de enlace perimetral. Hay un coste fijo de 200 USD al mes.
- Ingesta directa a AWS IoT Core por parte de MQTT y una regla de IoT para almacenar los datos sin procesar en Amazon S3: suponiendo que todas las señales se publiquen en una carga útil común, el número total de mensajes publicados en AWS IoT Core es de 25 × 3600 × 24 × 30, es decir, 64,8 millones por mes. A 1 USD por millón de mensajes, se trata de un coste mensual de 64,8 USD al mes. A 0,15 USD por millón de activaciones de reglas y con una regla

por mensaje, esto añade un coste mensual de 19,44 USD. Con un coste de 0,023 USD por GB de almacenamiento en Amazon S3, se añaden otros 1,5 USD al mes (aumentando cada mes para reflejar los nuevos datos). El coste total del primer mes es de 84,54 USD y aumenta 1,5 USD cada mes.

- Comprimir los datos en el borde de un archivo Parquet y subirlos a Amazon S3 (método propuesto): la relación de compresión depende del tipo de datos. Con los mismos datos industriales probados para MQTT, el total de datos de salida de un mes completo es de 1,2 Gb. Esto cuesta 0,03 USD al mes. Los índices de compresión (que utilizan datos aleatorios) descritos en otros puntos de referencia son del orden del 66 por ciento (lo que se acerca más al peor de los casos). El total de datos es de 21 Gb y cuesta 0,5 USD al mes.

Generador de archivos de parquet

El siguiente ejemplo de código muestra la estructura de un generador de archivos Parquet escrito en Python. El ejemplo de código es solo para fines ilustrativos y no funcionará si se pega en su entorno.

```
import queue
import paho.mqtt.client as mqtt
import pandas as pd

#queue for decoupling the MQTT thread
messageQueue = queue.Queue()
client = mqtt.Client()
streammanager = StreamManagerClient()

def feederListener(topic, message):
    payload = {
        "topic" : topic,
        "payload" : message,
    }
    messageQueue.put_nowait(payload)

def on_connect(client_instance, userdata, flags, rc):
    client.subscribe("#",qos=0)

def on_message(client, userdata, message):
    feederListener(topic=str(message.topic),
 message=str(message.payload.decode("utf-8")))


filename = "tempfile.parquet"
```

```
streamname = "mystream"
destination_bucket= "mybucket"
keyname="mykey"
period= 60

client.on_connect = on_connect
client.on_message = on_message
streammanager.create_message_stream(
            MessageStreamDefinition(name=streamname,
 strategy_on_full=StrategyOnFull.OverwriteOldestData)
       )


while True:
   try:
       message = messageQueue.get(timeout=myArgs.mqtt_timeout)
   except (queue.Empty):
       logger.warning("MQTT message reception timed out")

   currentTimestamp = getCurrentTime()
   if currentTimestamp >= nextUploadTimestamp:
       df = pd.DataFrame.from_dict(accumulator)
       df.to_parquet(filename)
       s3_export_task_definition = S3ExportTaskDefinition(input_url=filename,
 bucket=destination_bucket, key=key_name)
       streammanager.append_message(streamname,
 Util.validate_and_serialize_to_json_bytes(s3_export_task_definition))
       accumulator = {}
       nextUploadTimestamp += period
   else:
        accumulator.append(message)
```

Migre los datos de Hadoop a Amazon S3 mediante WanDisco Migrator LiveData

Origen: clúster Hadoop en las instalaciones	Destino: Amazon S3	Tipo R: volver a alojar
Entorno: producción	Tecnologías: lagos de datos; Macrodatos; Nube híbrida; Migración	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon S3		

Resumen

Este patrón describe el proceso de migración de datos de Apache Hadoop desde un Hadoop Distributed File System (HDFS) a Amazon Simple Storage Service (Amazon S3). Utiliza WanDisco LiveData Migrator para automatizar el proceso de migración de datos.

Requisitos previos y limitaciones

Requisitos previos

- Nodo perimetral del clúster Hadoop donde se instalará LiveData Migrator. El nodo debe cumplir con los siguientes requisitos:
  - Especificación mínima: 4 CPU, 16 GB de RAM, 100 GB de almacenamiento.
  - Red mínima de 2 Gbps.
  - Se puede acceder al puerto 8081 en su nodo perimetral para acceder a la interfaz de usuario de WanDisco.
  - Java 1.8 de 64 bits.
  - Bibliotecas cliente de Hadoop instaladas en el nodo perimetral.
  - Capacidad para autenticarse como superusuario de HDFS (por ejemplo, "hdfs").
  - Si Kerberos está activado en su clúster de Hadoop, debe haber disponible en el nodo perimetral un keytab válido que contenga una entidad principal adecuada para el superusuario de HDFS.

  - Consulte las notas de publicación para obtener una lista de los sistemas operativos compatibles.
- Una cuenta de AWS activa con acceso a un bucket de S3.
- Un enlace de AWS Direct Connect establecido entre su clúster de Hadoop local (específicamente el nodo perimetral) y AWS.

Versiones de producto

- LiveData Migrator 1.8.6
- de usuario de SanDisco (OneUI) 5.8.0

Arquitectura

Pila de tecnología de origen

- Clúster Hadoop en las instalaciones

Pila de tecnología de destino

- Amazon S3

Arquitectura

El siguiente diagrama muestra la arquitectura de la solución LiveData Migrator.

El flujo de trabajo consta de cuatro componentes principales para la migración de datos de HDFS en las instalaciones a Amazon S3.

- LiveData Migrator: automatiza la migración de datos de HDFS a Amazon S3 y reside en un nodo perimetral del clúster de Hadoop.
- HDFS: un sistema de archivos distribuido que proporciona un acceso de alto rendimiento a los datos de las aplicaciones.
- Amazon S3: un servicio de almacenamiento de objetos de AWS que ofrece escalabilidad, disponibilidad de datos, seguridad y rendimiento.
- AWS Direct Connect: un servicio que establece una conexión de red dedicada entre los centros de datos en las instalaciones y AWS.

Automatizar y escalar

Por lo general, se crean varias migraciones para poder seleccionar contenido específico del sistema de archivos de origen por ruta o directorio. También puede migrar datos a varios sistemas de archivos independientes al mismo tiempo definiendo varios recursos de migración.

Epics

Configurar el almacenamiento de Amazon S3 en su cuenta de AWS

Tarea	Descripción	Habilidades requeridas
Inicie sesión en su cuenta de AWS.	Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.	Experiencia de AWS
Cree un bucket de S3.	Si aún no tiene un bucket de S3 existente para usarlo como almacenamiento de destino, elija la opción “Crear bucket” en la consola de Amazon S3 y especifique el nombre del bucket, la región de AWS y la configuración del bucket para bloquear el acceso público. AWS y wanDisco recomiendan habilitar las opciones de bloqueo de acceso público para el bucket de S3 y configurar las políticas de acceso al bucket y permisos de usuario para cumplir con los requisitos de su organización. Puede encontrar un ejemplo de AWS en https://docs.aws.amazon.com/	Experiencia de AWS

Tarea	Descripción	Habilidades requeridas
	AmazonS3/latest/dev/example-walkthroughs-managing-access-example1.html.	

Instale Migrator LiveData

Tarea	Descripción	Habilidades requeridas
Descargue el instalador de Migrator LiveData .	Descargue el LiveData instalador de Migrator y cárguelo en el nodo perimetral de Hadoop. Puede descargar una versión de prueba gratuita de LiveData Migrator en https://www2.wandisco.com/ldm-trial. También puede obtener acceso a LiveData Migrator desde AWS Marketplace, en https://aws.amazon.com/marketplace/pp/B07B8SZND9.	Administrador de Hadoop, propietario de la aplicación
Instale LiveData Migrator.	Utilice el instalador descargado e instale LiveData Migrator como superusuario de HDFS en un nodo perimetral de su clúster de Hadoop. Consulte la sección “Información adicional ” para ver los comandos de instalación.	Administrador de Hadoop, propietario de la aplicación
Compruebe el estado de Migrator y otros servicios LiveData .	Compruebe el estado de LiveData Migrator, Hive Migrator y WanDisco UI mediante los comandos que	Administrador de Hadoop, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	se proporcionan en la sección «Información adicional».	

Configure el almacenamiento mediante la interfaz de usuario de WanDisco

Tarea	Descripción	Habilidades requeridas
Registre su LiveData cuenta de Migrator.	Inicie sesión en la interfaz de usuario de WanDisco a través de un navegador web en el puerto 8081 (en el nodo perimetral de Hadoop) y proporcione sus datos para registrarse. Por ejemplo, si ejecuta LiveData Migrator en un host llamado myldmhost .example.com, la URL sería: http://myldmhost.example.com:8081	Propietario de la aplicación
Configure el almacenamiento HDFS de origen.	Proporcione los detalles de configuración necesarios para el almacenamiento HDFS de origen. Esto incluirá el valor "fs.defaultFS" y un nombre de almacenamiento definido por el usuario. Si Kerberos está habilitado, proporcione la ubicación principal y la ubicación de las pestañas clave para que las utilice Migrator. LiveData Si NameNode HA está habilitado en el clúster, proporcione una ruta a los archivos core-site	Administrador de Hadoop, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	.xml y hdfs-site.xml del nodo perimetral.	
Configure el almacenamiento de Amazon S3 de destino.	Añada su almacenamiento de destino como del tipo S3a. Proporcione el nombre de almacenamiento definido por el usuario y el nombre del bucket de S3. Introduzca «org.apache.hadoop.fs.s3a.SimpleAWSCredentialsProvider» en la opción Proveedor de credenciales y proporcione las claves secretas y de acceso de AWS para el depósito de S3. También se necesitarán propiedades de S3a adicionales. Para obtener más información, consulte la sección «Propiedades del S3a» de la documentación de Migrator en https://docs.wandisco.com/live-data-migrator/docs/command-reference/#filesystem-add-s3a. LiveData	AWS, propietario de la aplicación

Preparación para la migración

Tarea	Descripción	Habilidades requeridas
Añada exclusiones (si es necesario).	Si desea excluir conjuntos de datos específicos de la migración, añada exclusiones para el almacenamiento HDFS de origen. Estas exclusiones	Administrador de Hadoop, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	pueden basarse en el tamaño del archivo, los nombres de los archivos (según los patrones de expresiones regulares) y la fecha de modificación.	

Crear e iniciar la migración

Tarea	Descripción	Habilidades requeridas
Cree y configure la migración.	Cree una migración en el panel de control de la interfaz de usuario de WanDisco. Elija su fuente (HDFS) y su destino (el bucket de S3). Añada las nuevas exclusion es que ha definido en el paso anterior. Seleccione la opción "Sobrescribir" u "Omitir si el tamaño coincide". Cree la migración cuando todos los campos estén completos.	Administrador de Hadoop, propietario de la aplicación
Inicie la migración.	En el panel de control, seleccione la migración que ha creado. Haga clic para iniciar la migración. También puede iniciar una migración automáticamente si seleccion a la opción de inicio automátic o al crear la migración.	Propietario de la aplicación

Administrar ancho de banda

Tarea	Descripción	Habilidades requeridas
Establezca un límite de ancho de banda de la red entre el origen y el destino.	En la lista de almacenamientos del panel de control, seleccione su almacenamiento de origen y seleccione "Administración del ancho de banda" en la lista de agrupamiento. Desactive la opción ilimitada y defina el límite y la unidad de ancho de banda máximos. Seleccione “Aplicar”.	Propietario de la aplicación, Networking

Monitorear y gestionar migraciones

Tarea	Descripción	Habilidades requeridas
Vea la información de migración mediante la interfaz de usuario de WanDisco.	Utilice la interfaz de usuario de WanDisco para ver la información sobre licencias, ancho de banda, almacenamiento y migración. La interfaz de usuario también proporciona un sistema de notificaciones para que pueda recibir notificaciones sobre errores, advertencias o hitos importantes en su uso.	Administrador de Hadoop, propietario de la aplicación
Detenga, reanude y elimine las migraciones.	Puede impedir que una migración transfiera contenido a su destino colocándola en el estado STOPPED.	Administrador de Hadoop, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	Las migraciones detenidas se pueden reanudar. Las migraciones en estado STOPPED también se pueden eliminar.	

Recursos relacionados

- LiveData Documentación sobre el migrador
- LiveData Migrator en AWS Marketplace
- Comunidad de soporte de WanDisco
- Demostración de WanDisco LiveData Migrator (vídeo)

Información adicional

Instalación de Migrator LiveData

Puede usar los siguientes comandos para instalar LiveData Migrator, suponiendo que el instalador esté dentro de su directorio de trabajo:

```
su - hdfs
chmod +x livedata-migrator.sh && sudo ./livedata-migrator.sh
```

Comprobar el estado de LiveData Migrator y otros servicios después de la instalación

Usa los siguientes comandos para comprobar el estado de LiveData Migrator, Hive migrator y WanDisco UI:

```
service livedata-migrator status
service hivemigrator status
service livedata-ui status
```

Más patrones

- Cree una canalización de servicios de ETL para cargar datos de forma incremental desde Amazon S3 a Amazon Redshift mediante AWS Glue
- ???
- Asegúrese de que el clúster de Amazon Redshift esté cifrado en el momento de su creación
- Genere datos de prueba con un trabajo de AWS Glue y Python
- Migre datos a la nube de AWS mediante Starburst
- Optimice la incorporación ETL del tamaño del archivo de entrada en AWS
- Orqueste un proceso de ETL con validación, transformación y particionamiento mediante AWS Step Functions
- ???
- Transfiera datos de Db2 z/OS a gran escala a Amazon S3 en archivos CSV
- Compruebe que los nuevos clústeres de Amazon Redshift tengan puntos de conexión SSL necesarios
- Visualice los registros de auditoría de Amazon Redshift con Amazon Athena y Amazon QuickSight

Bases de datos

Temas

- Acceso a tablas en las instalaciones de Microsoft SQL Server desde Microsoft SQL Server en Amazon EC2 mediante servidores vinculados
- Agregue HA a Oracle PeopleSoft en Amazon RDS Custom mediante una réplica de lectura
- Evaluar el rendimiento de las consultas para migrar bases de datos de SQL Server a MongoDB Atlas en AWS
- Automatice la conmutación por error y la conmutación por recuperación entre regiones mediante DR Orchestrator Framework
- Automatice la replicación de las instancias de Amazon RDS en todas las cuentas de AWS
- Realice copias de seguridad automáticas de las bases de datos de SAP HANA mediante Systems Manager y EventBridge
- Bloquee el acceso público a Amazon RDS mediante Cloud Custodian
- Configure el enrutamiento de solo lectura en un grupo de disponibilidad Always On en SQL Server en AWS
- Conectar mediante un túnel SSH en pgAdmin
- Convertir consultas JSON de Oracle en SQL de bases de datos PostgreSQL
- Copiar tablas de Amazon DynamoDB entre cuentas mediante una implementación personalizada
- Copiar tablas de Amazon DynamoDB entre cuentas mediante AWS Backup
- Crear informes detallados de costos y uso para Amazon RDS y Amazon Aurora
- Emule cargas de trabajo de Oracle RAC mediante puntos de conexión personalizados en Aurora PostgreSQL
- Habilite conexiones cifradas para instancias de base de datos de PostgreSQL en Amazon RDS
- Cifrar una instancia de base de datos de Amazon RDS para PostgreSQL existente
- Imponga el etiquetado automático de las bases de datos de Amazon RDS en el lanzamiento
- Estime el costo de una tabla de DynamoDB para la capacidad bajo demanda
- Costos de almacenamiento estimados para una tabla de Amazon DynamoDB
- Calcule el tamaño del motor de Amazon RDS para una base de datos de Oracle mediante informes de AWR
- Exporte tablas de Amazon RDS para SQL Server a un bucket S3 mediante AWS DMS

- Gestionar bloques anónimos en instrucciones SQL dinámicas en Aurora PostgreSQL
- Gestionar las sobrecargadas funciones de Oracle en Aurora PostgreSQL
- Ayudar a reforzar el etiquetado en DynamoDB
- Implemente recuperación de desastres entre regiones con AWS DMS y Amazon Aurora
- Migre funciones y procedimientos de Oracle con más de 100 argumentos a PostgreSQL
- Migrar las instancias de base de datos de Amazon RDS para Oracle a otras cuentas que usen AMS
- Migrar las variables de enlace OUT de Oracle a una base de datos PostgreSQL
- Migración de SAP HANA a AWS mediante SAP HSR con el mismo nombre de host
- Migrar SQL Server a AWS mediante grupos de disponibilidad distribuidos
- Migre de Oracle 8i o 9i a Amazon RDS para Oracle con AWS DMS SharePlex
- Supervisar Amazon Aurora en busca de instancias sin cifrado
- Supervise GoldenGate los registros de Oracle mediante Amazon CloudWatch
- Redefina la plataforma de Oracle Database Enterprise Edition a Standard Edition 2 en Amazon RDS para Oracle
- Replicar bases de datos de unidades centrales en AWS mediante Precisely Connect
- Programe trabajos para Amazon RDS para PostgreSQL y Aurora PostgreSQL mediante Lambda y Secrets Manager
- Proteja y optimice el acceso de los usuarios a una base de datos de federación DB2 en AWS mediante contextos de confianza
- Envíe notificaciones para una instancia de base de datos de Amazon RDS para SQL Server mediante un servidor SMTP en las instalaciones y el Correo de base de datos
- Configurar la recuperación de desastres para SAP en IBM Db2 en AWS
- Configure una arquitectura HA/DR para Oracle E-Business Suite en Amazon RDS Custom con una base de datos en espera activa
- Configure la replicación de datos entre Amazon RDS para MySQL y MySQL en Amazon EC2 mediante GTID
- Funciones de transición para una PeopleSoft aplicación de Oracle en Amazon RDS Custom for Oracle
- Patrones de migración de bases de datos según la carga
- Más patrones

Acceso a tablas en las instalaciones de Microsoft SQL Server desde Microsoft SQL Server en Amazon EC2 mediante servidores vinculados

Creado por Tirumala Dasari (AWS) y Eduardo Valentim (AWS)

Entorno: PoC o piloto	Tecnologías: Bases de datos	Carga de trabajo: Microsoft

Resumen

Este patrón describe cómo acceder a las tablas de bases de datos en las instalaciones de Microsoft SQL Server que se ejecutan en Microsoft Windows, desde bases de datos de Microsoft SQL Server que se ejecutan o alojan en instancias Windows o Linux de Amazon Elastic Compute Cloud (Amazon EC2) mediante servidores vinculados.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Amazon EC2 con Microsoft SQL Server ejecutándose en la AMI (Imagen de máquina de Amazon) de Amazon Linux
- AWS Direct Connect entre el servidor Microsoft SQL Server (Windows) en las instalaciones y la instancia EC2 de Windows o Linux

Versiones de producto

- Servidor SQL 2016 o posterior

Arquitectura

Pila de tecnología de origen

- Base de datos Microsoft SQL Server en las instalaciones que se ejecuta en Windows

- Amazon EC2 con Microsoft SQL Server que se ejecuta en una AMI de Windows o una AMI de Linux

Pila de tecnología de destino

- Amazon EC2 con Microsoft SQL Server que se ejecuta en la AMI de Amazon Linux
- Amazon EC2 con Microsoft SQL Server ejecutando Windows AMI

Arquitectura de base de datos de origen y destino

Herramientas

- Microsoft SQL Server Management Studio (SSMS) es un entorno integrado para administrar infraestructuras de SQL Server. Proporciona una interfaz de usuario y un grupo de herramientas con editores de scripts enriquecidos que interactúan con SQL Server.

Epics

Cambiar el modo de autenticación a Windows para SQL Server en Windows SQL Server

Tarea	Descripción	Habilidades requeridas
Conéctese a Windows SQL Server mediante SSMS.		Administrador de base de datos
Cambie el modo de autenticación a Windows en SQL Server desde el menú contextual (haga clic con el botón derecho) de la instancia de Windows SQL Server.		Administrador de base de datos

Reiniciar el servicio Windows MSSQL

Tarea	Descripción	Habilidades requeridas
Reinicie el servicio SQL.	1. En el Explorador de objetos de SSMS, seleccione la instancia de SQL Server. 2. Abra el menú contextual (con el botón derecho). 3. Elija Reiniciar.	Administrador de base de datos

Crear un nuevo inicio de sesión y seleccionar las bases de datos a las que acceder en Windows SQL Server

Tarea	Descripción	Habilidades requeridas
En la pestaña Seguridad, abra el menú contextual (haga clic con el botón derecho) de Inicio de sesión y seleccione un nuevo inicio de sesión.		Administrador de base de datos
En la pestaña General, seleccione la autenticación de SQL Server, introduzca un nombre de usuario, introduzc a la contraseña y, a continuac ión, confirme la contraseñ a y desactive la opción de cambiarla la próxima vez que inicie sesión.		Administrador de base de datos
En la pestaña Funciones del servidor, seleccione Público.		Administrador de base de datos
En la pestaña de asignacio nes de usuario, seleccione la	Seleccione public y db_datare ader para acceder a los datos	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
base de datos y el esquema a los que desee acceder y, a continuación, resalte la base de datos para seleccionar los roles de la base de datos.	de las tablas de la base de datos.	
Pulse Aceptar para crear un usuario.		Administrador de base de datos

Agregue la IP de Windows SQL Server al archivo host de Linux SQL Server

Tarea	Descripción	Habilidades requeridas
Conéctese a la caja de Linux SQL Server a través de la ventana del terminal.		Administrador de base de datos
Abra el archivo /etc/hosts y añada la dirección IP del equipo Windows con SQL Server.		Administrador de base de datos
Guarde el archivo de hosts.		Administrador de base de datos

Crear un servidor vinculado en Linux SQL Server

Tarea	Descripción	Habilidades requeridas
Cree un servidor vinculado mediante los procedimientos almacenados master.sy s.sp_addlinkedserver y	Para obtener más informaci ón sobre el uso de estos procedimientos almacenad os, consulte la sección de Información adicional.	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
master.dbo.sp_addlinkedsrvlogin.		

Verifique el servidor vinculado y las bases de datos creados en SSMS

Tarea	Descripción	Habilidades requeridas
En Linux SQL Server en SSMS, vaya a servidores vinculados y actualice.		Administrador de base de datos
Expanda los servidores y catálogos vinculados creados en el panel izquierdo.	Verá las bases de datos de SQL Server seleccionadas con tablas y vistas.	Administrador de base de datos

Verificar que puede acceder a las tablas de bases de datos de Windows SQL Server

Tarea	Descripción	Habilidades requeridas
En la ventana de consulta de SSMS, ejecute la siguiente consulta: "seleccionar los primeros 3 * de [sqllin]. dms_sample_win.dbo .mlb_data".	Tenga en cuenta que la cláusula FROM (de) utiliza una sintaxis de cuatro partes: computer.database. schema.table (por ejemplo, SELECCIONAR el nombre "SQL2 databases" DE [sqllin] .master.sys.databases). En nuestro ejemplo, creamos un alias para SQL2 en el archivo de hosts, por lo que no es necesario introducir el nombre real de NetBIOS entre corchetes. Si utiliza los nombres de NetBIOS	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
	reales, tenga en cuenta que AWS utiliza de forma predeterminada los nombres de NetBIOS, como Win-xxxx, y SQL Server requiere corchetes para los nombres con guiones.	

Recursos relacionados

- Notas de la versión de SQL Server en Linux

Información adicional

Uso de procedimientos almacenados para crear servidores vinculados

SSMS no admite la creación de servidores vinculados para Linux SQL Server, por lo que debe usar estos procedimientos almacenados para crearlos:

```
EXEC master.sys.sp_addlinkedserver @server= N'SQLLIN' , @srvproduct= N'SQL Server'
EXEC master.dbo.sp_addlinkedsrvlogin
 @rmtsrvname=N'SQLLIN',@useself=N'False',@locallogin=NULL,@rmtuser=N'username',@rmtpassword='Te
```

Nota 1: Introduzca las credenciales de inicio de sesión que creó anteriormente en Windows SQL Server en el procedimiento almacenado `master.dbo.sp_addlinkedsrvlogin`.

Nota 2: el nombre `@server`, `SQLLIN` y el nombre de la entrada del archivo host `172.12.12.4 SQLLIN` deben ser los mismos.

Puede utilizar este proceso para crear servidores vinculados en los siguientes casos:

- De Linux SQL Server a Windows SQL Server a través de un servidor vinculado (como se especifica en este patrón)
- De Windows SQL Server a Linux SQL Server a través de un servidor vinculado

- De Linux SQL Server a otro servidor SQL de Linux a través de un servidor vinculado

Agregue HA a Oracle PeopleSoft en Amazon RDS Custom mediante una réplica de lectura

Creado por sampath kathirvel (AWS)

Entorno: producción	Tecnologías: bases de datos; infraestructura	Carga de trabajo: Oracle
Servicios de AWS: Amazon RDS		

Resumen

Para ejecutar la solución de planificación de recursos PeopleSoft empresariales (ERP) de Oracle en Amazon Web Services (AWS), puede utilizar Amazon Relational Database Service (Amazon RDS) o Amazon RDS Custom for Oracle, que admite aplicaciones heredadas, personalizadas y empaquetadas que requieren acceso al sistema operativo y al entorno de base de datos subyacentes. Para conocer los factores clave a tener en cuenta durante la planificación de una migración, consulte Estrategias de migración de bases de datos Oracle en Recomendaciones de AWS.

En el momento de escribir este artículo, RDS Custom para Oracle no admite la opción Multi-AZ, que está disponible para Amazon RDS para Oracle como una solución de alta disponibilidad que utiliza la replicación del almacenamiento. En su lugar, este patrón logra la alta disponibilidad mediante el uso de una base de datos en espera que crea y mantiene una copia física de la base de datos principal. El patrón se centra en los pasos para ejecutar una base de datos de PeopleSoft aplicaciones en Amazon RDS Custom with HA mediante Oracle Data Guard para configurar una réplica de lectura.

Este patrón también cambia la réplica de lectura al modo de solo lectura. Tener la réplica de lectura en modo de solo lectura ofrece ventajas adicionales:

- Descargar las cargas de trabajo de solo lectura de la base de datos principal
- Permitir la reparación automática de los bloques dañados mediante la recuperación de bloques en buen estado de la base de datos en espera mediante la característica Oracle Active Data Guard
- Uso de la capacidad Far Sync para mantener sincronizada la base de datos remota en espera sin la sobrecarga de rendimiento asociada a la transmisión de redo log a larga distancia.

El uso de una réplica en modo de solo lectura requiere la opción Oracle Active Data Guard, que tiene un costo adicional, ya que se trata de una característica de Oracle Database Enterprise Edition con licencia independiente.

Requisitos previos y limitaciones

Requisitos previos

- Una PeopleSoft aplicación existente en Amazon RDS Custom. Si no tiene una aplicación, consulte el patrón Migrate Oracle PeopleSoft to Amazon RDS Custom.
- Un único nivel PeopleSoft de aplicación. Sin embargo, puede adaptar este patrón para que funcione con varios niveles de aplicación.
- Amazon RDS Custom está configurado con al menos 8 GB de espacio de intercambio.
- Una licencia de base de datos Oracle Active Data Guard para convertir la réplica de lectura en modo de solo lectura y utilizarla para transferir las tareas de elaboración de informes al modo de espera. Para obtener más información, consulte la Lista de precios de Oracle Technology Commercial.

Limitaciones

- Limitaciones generales y configuraciones no compatibles con RDS Custom para Oracle
- Limitaciones asociadas a las Réplicas de lectura de Amazon RDS Custom para Oracle

Versiones de producto

- Para ver las versiones de la base de datos Oracle compatibles con Amazon RDS Custom, consulte RDS Custom para Oracle.
- Para ver las clases de instancias de la base de datos Oracle compatibles con Amazon RDS Custom, consulte Compatibilidad de clases de instancias de base de datos con RDS Custom para Oracle.

Arquitectura

Pila de tecnología de destino

- Amazon RDS Custom para Oracle

- AWS Secrets Manager
- Oracle Active Data Guard
- PeopleSoft Aplicación Oracle

Arquitectura de destino

El siguiente diagrama muestra una instancia de base de datos de Amazon RDS Custom y una réplica de lectura de Amazon RDS Custom. La réplica de lectura utiliza Oracle Active Data Guard para replicar en otra zona de disponibilidad. También puede usar la réplica de lectura para descargar el tráfico de lectura en la base de datos principal y para generar informes.

Para ver una arquitectura representativa con Oracle PeopleSoft en AWS, consulte Configurar una PeopleSoft arquitectura de alta disponibilidad en AWS.

Herramientas

Servicios de AWS

- Amazon RDS Custom para Oracle es un servicio de base de datos administrado para aplicaciones heredadas, personalizadas y empaquetadas que requieren acceso al sistema operativo y al entorno de base de datos subyacentes.
- AWS Secrets Manager ayuda a reemplazar las credenciales codificadas en el código, incluidas las contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación. En este patrón, recupera las contraseñas de usuario de la base de datos de Secrets Manager para `RDS_DATAGUARD` con el nombre secreto `do-not-delete-rds-custom-+<<RDS Resource ID>>+-dg`.

Otras herramientas

- Oracle Data Guard le ayuda a crear, mantener, gestionar y supervisar las bases de datos en espera.

Prácticas recomendadas

Para lograr un objetivo de cero pérdidas de datos (RPO=0), utilice el modo de protección Data Guard `MaxAvailability`, con la configuración `SYNC+NOAFFIRM` redo transport para mejorar el

rendimiento. Para obtener más información sobre cómo seleccionar el modo de protección de la base de datos, consulte la sección Información adicional.

Epics

Crear la réplica de lectura

Tarea	Descripción	Habilidades requeridas
Crear la réplica de lectura.	Para crear una réplica de lectura de la instancia de base de datos de Amazon RDS Custom, siga las instrucciones de la documentación de Amazon RDS y utilice la instancia de base de datos de Amazon RDS Custom que creó (consulte la sección Requisitos previos) como base de datos de origen. De forma predeterminada, la réplica de lectura de Amazon RDS Custom se crea como una copia física en espera y se encuentra montada. Esto tiene la intención de garantizar el cumplimiento de la licencia de Oracle Active Data Guard. Este patrón incluye código para configurar una base de datos de contenedores multiusuario (CDB) o una instancia que no sea de CDB.	Administrador de base de datos

Cambie el modo de protección de Oracle Data Guard a MaxAvailability

Tarea	Descripción	Habilidades requeridas
Acceda a la configuración del agente Data Guard en la base de datos principal.	En este ejemplo, la réplica de lectura de Amazon RDS Custom es `RDS_CUSTOM_ORCL_D` para la instancia que no es de CDB y `RDS_CUSTOM_RDSCDB_B` para la instancia de CDB. Las bases de datos que no son de CDB son `orcl_a` (principal) y `orcl_d` (en espera). Los nombres de las bases de datos para CDB son `rdscdb_a` (principal) y `rdscdb_b` (en espera). Puede conectarse a la réplica de lectura personalizada de RDS directamente o a través de la base de datos principal . Puede encontrar el nombre del servicio de red de su base de datos en el archivo `tnsnames.ora` ubicado en el directorio `$ORACLE_HOME/network/admin` . RDS Custom para Oracle rellena automáticamente estas entradas para su base de datos principal y sus réplicas de lectura. La contraseña del usuario `RDS_DATAGUARD` se	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	guarda en AWS Secrets Manager, con el nombre secreto `do-not-delete-rds-custom-+<<RDS Resource ID>>+-dg`. Para obtener más información sobre cómo conectarse a una instancia personalizada de RDS mediante la clave SSH (Secure Shell) recuperada de Secrets Manager, consulte Conexión a una instancia de base de datos personalizada de RDS mediante SSH. Para acceder a la configuración del agente de Oracle Data Guard a través de la línea de comandos de Data Guard (`dgmgrl`), utilice el siguiente código. No CDB `$ dgmgrl RDS_DATAGUARD@RDS_CUSTOM_ORCL_D` `DGMGRL for Linux: Release 19.0.0.0.0 - Production on Fri Sep 30 22:44:49 2022` `Version 19.10.0.0.0` `Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved.`	

Tarea	Descripción	Habilidades requeridas
	Welcome to DGMGRL, type "help" for informati on. Password: Connected to "ORCL_D" Connected as SYSDG. DGMGRL> DGMGRL> show database orcl_d Database - orcl_d Role: PHYSICAL STANDBY Intended State: APPLY-ON Transport Lag: 0 seconds (computed 0 seconds ago) Apply Lag: 0 seconds (computed 0 seconds ago) Average Apply Rate: 11.00 KByte/s Instance(s): ORCL SUCCESS DGMGRL> CDB -bash-4.2$ dgmgrl C##RDS_DATAGUARD@R DS_CUSTOM_RDSCDB_B DGMGRL for Linux: Release 19.0.0.0.0 - Production on Wed Jan 11 20:24:11 2023 Version 19.16.0.0.0 Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved.	

Tarea	Descripción	Habilidades requeridas
	Welcome to DGMGRL, type "help" for informati on. Password: Connected to "RDSCDB_B " Connected as SYSDG. DGMGRL> DGMGRL> show database rdscdb_b Database - rdscdb_b Role: PHYSICAL STANDBY Intended State: APPLY-ON Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 0 seconds (computed 1 second ago) Average Apply Rate: 2.00 KByte/s Real Time Query: OFF Instance(s): RDSCDB Database Status: SUCCESS DGMGRL>	

Tarea	Descripción	Habilidades requeridas
Cambie la configuración de transporte de registros conectándose a DGMGRL desde el nodo principal.	Cambie el modo de transporte de registros a `FastSync`, correspondiente a la configuración redo transport `SYNC +NOAFFIRM` . Para asegurarse de que tiene una configuración válida después del cambio de rol, cámbiela tanto para la base de datos principal como para la base de datos en espera. No CDB `DGMGRL>` `DGMGRL> edit database orcl_d set property logxptmode=fastsync;` `Property "logxptmode" updated` `DGMGRL> show database orcl_d LogXptMode;` `LogXptMode = 'fastsync'` `DGMGRL> edit database orcl_a set property logxptmode=fastsync;` `Property "logxptmode" updated` `DGMGRL> show database orcl_a logxptmode;` `LogXptMode = 'fastsync'` `DGMGRL>` CDB	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`DGMGRL> edit database rdscdb_b set property logxptmode=fastsyn c;DGMGRL> edit database rdscdb_b set property logxptmode=fastsync; Property "logxptmode" updated DGMGRL> show database rdscdb_b LogXptMode; LogXptMode = 'fastsync' DGMGRL> edit database rdscdb_a set property logxptmode=fastsync; Property "logxptmode" updated DGMGRL> show database rdscdb_a logxptmode; LogXptMode = 'fastsync' DGMGRL>`	

Tarea	Descripción	Habilidades requeridas
Cambie el modo de protección a MaxAvailability.	Cambie el modo de protección a `MaxAvailability` mediante una conexión a `DGMGRL` desde el nodo principal. No CDB `DGMGRL> edit configuration set protection mode as maxavailability;` `Succeeded.` `DGMGRL> show configuration;` `Configuration - rds_dg` `Protection Mode: MaxAvailability` `Members:` `orcl_a - Primary database` `orcl_d - Physical standby database` `Fast-Start Failover: Disabled` `Configuration Status:` `SUCCESS (status updated 38 seconds ago)` `DGMGRL>` CDB `DGMGRL> show configuration` `Configuration - rds_dg` `Protection Mode: MaxAvailability` `Members:`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	<pre> rdscdb_a - Primary database rdscdb_b - Physical standby database Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 57 seconds ago) DGMGRL></pre>	

Cambie el estado de la réplica de montada a de solo lectura y habilite redo apply.

Tarea	Descripción	Habilidades requeridas
Detenga redo apply para la base de datos en espera.	La réplica de lectura se crea en modo `MOUNT` de forma predeterminada. Para abrirla en modo de solo lectura, primero debe desactivar redo apply conectándose a `DGMGRL` desde el nodo principal o en espera. No CDB <pre>DGMGRL> show database orcl_dDGMGRL> show database orcl_d Database - orcl_d Role: PHYSICAL STANDBY Intended State: APPLY- ON Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 0 seconds (computed 1 second ago)</pre>	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`Average Apply Rate: 11.00 KByte/s` `Real Time Query: OFF` `Instance(s):` `ORCL` `Database Status:` `SUCCESS` `DGMGRL> edit database orcl_d set state=apply-off;` `Succeeded.` `DGMGRL> show database orcl_d` `Database - orcl_d` `Role: PHYSICAL STANDBY` `Intended State: APPLY-OFF` `Transport Lag: 0 seconds (computed 1 second ago)` `Apply Lag: 42 seconds (computed 1 second ago)` `Average Apply Rate: (unknown)` `Real Time Query: OFF` `Instance(s):` `ORCL` `Database Status:` `SUCCESS` `DGMGRL>` CDB `DGMGRL> show configurationDGMGRL> show configuration` `Configuration - rds_dg` `Protection Mode: MaxAvailability` `Members:`	

Tarea	Descripción	Habilidades requeridas
	rdscdb_a - Primary database rdscdb_b - Physical standby database Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 57 seconds ago) DGMGRL> show database rdscdb_b; Database - rdscdb_b Role: PHYSICAL STANDBY Intended State: APPLY-ON Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 0 seconds (computed 1 second ago) Average Apply Rate: 2.00 KByte/s Real Time Query: OFF Instance(s): RDSCDB Database Status: SUCCESS DGMGRL> edit database rdscdb_b set state=apply-off; Succeeded. DGMGRL> show database rdscdb_b; Database - rdscdb_b Role: PHYSICAL STANDBY Intended State: APPLY-OFF	

Tarea	Descripción	Habilidades requeridas
	<pre> Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 0 seconds (computed 1 second ago) Average Apply Rate: (unknown) Real Time Query: OFF Instance(s): RDSCDB Database Status: SUCCESS</pre>	

Tarea	Descripción	Habilidades requeridas
Abra la instancia de réplica de lectura en modo de solo lectura.	Conéctese a la base de datos en espera mediante la entrada TNS y ábrala en modo de solo lectura conectándose a ella desde el nodo principal o en espera. No CDB `$ sqlplus RDS_DATAG UARD@RDS_CUSTOM_OR CL_D as sysdg -bash-4.2$ sqlplus RDS_DATAGUARD@RDS_ CUSTOM_ORCL_D as sysdg SQL*Plus: Release 19.0.0.0.0 - Productio n on Fri Sep 30 23:00:14 2022 Version 19.10.0.0.0 Copyright (c) 1982, 2020, Oracle. All rights reserved. Enter password: Last Successful login time: Fri Sep 30 2022 22:48:27 +00:00 Connected to: Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production Version 19.10.0.0.0 SQL> select open_mode from v$database; OPEN_MODE -------------------- MOUNTED SQL> alter database open read only;`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

```
Database altered.
SQL> select open_mode
 from v$database;
OPEN_MODE
--------------------
READ ONLY
SQL>
```

CDB

```
-bash-4.2$ sqlplus
 C##RDS_DATAGUARD@R
DS_CUSTOM_RDSCDB_B as
 sysdg
SQL*Plus: Release
 19.0.0.0.0 - Productio
n on Wed Jan 11
 21:14:07 2023
Version 19.16.0.0.0
Copyright (c) 1982,
 2022, Oracle.  All
 rights reserved.
Enter password:
Last Successful login
 time: Wed Jan 11 2023
 21:12:05 +00:00
Connected to:
Oracle Database 19c
 Enterprise Edition
 Release 19.0.0.0.0 -
 Production
Version 19.16.0.0.0
SQL> select name,open
_mode from v$database;
NAME   OPEN_MODE
--------- ---------
-----------
RDSCDB   MOUNTED
SQL> alter database
 open read only;
Database altered.
```

Tarea	Descripción	Habilidades requeridas
	SQL> select name,open _mode from v$database; NAME OPEN_MODE --------- --------- ----------- RDSCDB READ ONLY SQL>	

Tarea	Descripción	Habilidades requeridas
Active redo apply en la instancia de réplica de lectura.	Active redo apply en la instancia de réplica de lectura mediante DGMGR L desde el nodo principal o en espera. No CDB `$ dgmgrl RDS_DATAG UARD@RDS_CUSTOM_OR CL_D DGMGRL for Linux: Release 19.0.0.0.0 - Production on Fri Sep 30 23:02:16 2022 Version 19.10.0.0.0 Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved. Welcome to DGMGRL, type "help" for informati on. Password: Connected to "ORCL_D" Connected as SYSDG. DGMGRL> edit database orcl_d set state=apply-on; DGMGRL> edit database orcl_d set state=app ly-on; Succeeded. DGMGRL> show database orcl_d Database - orcl_d Role: PHYSICAL STANDBY Intended State: APPLY-ON`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Transport Lag: 0 seconds (computed 0 seconds ago) Apply Lag: 0 seconds (computed 0 seconds ago) Average Apply Rate: 496.00 KByte/s Real Time Query: ON Instance(s): ORCL Database Status: SUCCESS DGMGRL> CDB -bash-4.2$ dgmgrl C##RDS_DATAGUARD@RDS_CUSTOM_RDSCDB_B -bash-4.2$ dgmgrl C##RDS_DATAGUARD@RDS_CUSTOM_RDSCDB_B DGMGRL for Linux: Release 19.0.0.0.0 - Production on Wed Jan 11 21:21:11 2023 Version 19.16.0.0.0 Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved. Welcome to DGMGRL, type "help" for information. Password: Connected to "RDSCDB_B" Connected as SYSDG.	

Tarea	Descripción	Habilidades requeridas
	DGMGRL> edit database rdscdb_b set state=app ly-on; Succeeded. DGMGRL> show database rdscdb_b Database - rdscdb_b Role: PHYSICAL STANDBY Intended State: APPLY-ON Transport Lag: 0 seconds (computed 0 seconds ago) Apply Lag: 0 seconds (computed 0 seconds ago) Average Apply Rate: 35.00 KByte/s Real Time Query: ON Instance(s): RDSCDB Database Status: SUCCESS DGMGRL> show database rdscdb_b Database - rdscdb_b Role: PHYSICAL STANDBY Intended State: APPLY-ON Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 0 seconds (computed 1 second ago) Average Apply Rate: 16.00 KByte/s Real Time Query: ON Instance(s): RDSCDB	

Tarea	Descripción	Habilidades requeridas
	`Database Status: SUCCESS DGMGRL>`	

Recursos relacionados

- Configuración de Amazon RDS como una PeopleSoft base de datos de Oracle (documento técnico de AWS)
- Guía de agente de Oracle Data Guard (documentación de referencia de Oracle)
- Oracle Data Guard Concepts and Administration(documentación de referencia de Oracle)

Información adicional

Seleccionar el modo de protección de su base de datos

Oracle Data Guard ofrece tres modos de protección para configurar su entorno de Data Guard en función de sus requisitos de disponibilidad, protección y rendimiento. Estos tres modos se resumen en la tabla siguiente:

Modo de protección	Configuración redo transport	Descripción
MÁXIMO RENDIMIENTO	ASYNC	En el caso de las transacciones que se realizan en la base de datos principal, los datos de redo se transmiten de forma asíncrona y se escriben en el redo log de la base de datos en espera. Por lo tanto, el impacto en el rendimiento es mínimo. `MaxPerformance` no puede proporcionar RPO=0 debido al envío asincrónico de registros.

MÁXIMA PROTECCIÓN	SYNC+AFFIRM	En el caso de las transacciones de la base de datos principal, los datos de redo se transmiten de forma sincrónica y se escriben en el disco de la base de datos en espera redo log antes de que se confirme la transacción. Si la base de datos en espera deja de estar disponible, la base de datos principal se cierra automáticamente para garantizar la protección de las transacciones.
MÁXIMA DISPONIBILIDAD	SYNC+AFFIRM	Es similar al modo `MaxProtection` , excepto cuando no se recibe ningún acuse de recibo de la base de datos en espera. En ese caso, funciona como si estuviera en modo `MaxPerformance` para preservar la disponibilidad de la base de datos principal hasta que pueda volver a escribir su redo stream en una base de datos en espera sincronizada.

SYNC+NOAFFIRM	En el caso de las transacciones de la base de datos principal, el redo se transmite de forma sincrónica a la base de datos en espera, y la principal solo espera una confirmación de acuse de recibo del redo en la base de datos en espera, no a que se haya escrito en el disco en espera. Este modo, también conocido como `FastSync`, puede proporcionar una ventaja en el rendimiento a costa de la posible exposición a la pérdida de datos en un caso especial de varios fallos simultáneos.

Las réplicas de lectura en RDS Custom para Oracle se crean con el modo de protección del máximo rendimiento, que también es el modo de protección predeterminado de Oracle Data Guard. El modo de rendimiento máximo proporciona el menor impacto en el rendimiento de la base de datos principal, lo que puede ayudarle a cumplir el requisito del objetivo de punto de recuperación (RPO) medido en segundos.

Para lograr el objetivo de cero pérdidas de datos (RPO=0), puede personalizar el modo de protección de Oracle Data Guard a `MaxAvailability` con la configuración `SYNC+NOAFFIRM` redo transport para mejorar el rendimiento. Como las confirmaciones en la base de datos principal solo se reconocen después de que los vectores redo correspondientes se hayan transmitido correctamente a la base de datos en espera, la latencia de la red entre la instancia principal y la réplica puede ser crucial para las cargas de trabajo sensibles a las confirmaciones. Recomendamos realizar pruebas de carga de la carga de trabajo para evaluar el impacto en el rendimiento cuando la réplica de lectura esté personalizada para ejecutarse en modo `MaxAvailability`.

La implementación de la réplica de lectura en la misma zona de disponibilidad que la base de datos principal proporciona una latencia de red más baja en comparación con la implementación de la

réplica de lectura en una zona de disponibilidad diferente. Sin embargo, es posible que implementar las réplicas principal y de lectura en la misma zona de disponibilidad no cumpla con los requisitos de alta disponibilidad porque, en el improbable caso de que la zona de disponibilidad no esté disponible, tanto la instancia principal como la instancia de réplica de lectura se ven afectadas.

Evaluar el rendimiento de las consultas para migrar bases de datos de SQL Server a MongoDB Atlas en AWS

Creado por Battulga Purevragchaa (AWS), Krishnakumar Sathyanarayana (US Inc) y Babu Srinivasan (PeerIslands MongoDB)

Entorno: PoC o piloto	Origen: Microsoft SQL Server	Destino: MongoDB Atlas o MongoDB Enterprise Advanced
Tipo R: redefinir la plataforma	Carga de trabajo: Microsoft	Tecnologías: Bases de datos; migración

Resumen

Este patrón proporciona una guía para cargar MongoDB con datos casi reales y evaluar el rendimiento de las consultas de MongoDB que sea lo más parecido posible al escenario de producción. La evaluación proporciona información para ayudar a planificar la migración a MongoDB desde una base de datos relacional. El patrón utiliza PeerIslands el generador de datos de prueba y el analizador de rendimiento para probar el rendimiento de las consultas.

Este patrón es particularmente útil para la migración de Microsoft SQL Server a MongoDB, ya que realizar transformaciones de esquemas y cargar datos de las instancias actuales de SQL Server a MongoDB puede resultar muy complejo. En lugar de esto, puede cargar datos prácticamente reales en MongoDB, conocer el rendimiento de MongoDB y ajustar el diseño del esquema antes de iniciar la migración propiamente dicha.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Familiaridad con MongoDB Atlas
- Esquema de MongoDB de destino
- Patrones típicos de consulta

Limitaciones

- Los tiempos de carga de datos y el rendimiento estarán limitados por el tamaño de la instancia del clúster de MongoDB. Se recomienda seleccionar instancias que estén recomendadas para uso en producción a fin de comprender el rendimiento en el mundo real.
- PeerIslands Actualmente, Test Data Generator y Performance Analyzer solo admiten consultas y cargas de datos en línea. Aún no se admite el procesamiento por lotes sin conexión (por ejemplo, cargar datos en MongoDB mediante conectores Spark).
- PeerIslands El generador de datos de prueba y el analizador de rendimiento admiten las relaciones de campo dentro de una colección. No admite relaciones entre colecciones.

Ediciones de producto

- Este patrón es compatible con MongoDB Atlas y MongoDB Enterprise Advanced.

Arquitectura

Pila de tecnología de destino

- MongoDB Atlas o MongoDB Enterprise Advanced

Arquitectura

PeerIslands El generador de datos de prueba y el analizador de rendimiento se crean con Java y Angular, y almacenan los datos generados en Amazon Elastic Block Store (Amazon EBS). La herramienta consta de dos flujos de trabajo: la generación de datos de prueba y las pruebas de rendimiento.

- En la generación de datos de prueba, se crea una plantilla, que es la representación en JSON del modelo de datos que se debe generar. Después de crear la plantilla, se pueden generar los datos en una colección de destino, tal y como se define en la configuración de generación de carga.
- En las pruebas de rendimiento, se crea un perfil. Un perfil es un escenario de prueba en varias etapas en el que se pueden configurar las operaciones de creación, lectura, actualización y eliminación (CRUD), los procesos de agregación, la ponderación de cada operación y la duración

de cada etapa. Tras crear el perfil, puede realizar pruebas de rendimiento en la base de datos de destino, en función de la configuración.

PeerIslands El generador de datos de prueba y el analizador de rendimiento almacenan sus datos en Amazon EBS, por lo que puede conectar Amazon EBS a MongoDB mediante cualquier mecanismo de conexión compatible con MongoDB, incluidos el emparejamiento, las listas de permisos y los puntos de enlace privados. De forma predeterminada, la herramienta no incluye componentes operativos; sin embargo, se puede configurar con Amazon Managed Service for Prometheus, Amazon Managed Grafana CloudWatch, Amazon y AWS Secrets Manager si es necesario.

Herramientas

- PeerIslands El generador de datos de prueba y el analizador de rendimiento incluyen dos componentes. El componente generador de datos de prueba ayuda a generar datos del mundo real altamente específicos del cliente, basados en el esquema de MongoDB. La herramienta está totalmente basada en la interfaz de usuario, con una rica biblioteca de datos, y se puede utilizar para generar rápidamente miles de millones de registros en MongoDB. La herramienta también proporciona capacidades para implementar relaciones entre campos en el esquema de MongoDB. El componente analizador del rendimiento ayuda a generar consultas y agregaciones altamente específicas para el cliente y a realizar pruebas de rendimiento realistas en MongoDB. Se puede usar el analizador de rendimiento para probar el rendimiento de MongoDB con perfiles de carga enriquecidos y consultas parametrizadas para un caso de uso específico.

Prácticas recomendadas

Consulte los siguientes recursos:

- MongoDB Schema Design Best Practices (Prácticas recomendadas de diseño de esquemas de MongoDB) (sitio web para desarrolladores de MongoDB)
- Best Practices of Deploying MongoDB Atlas on AWS (Prácticas recomendadas para implementar MongoDB Atlas en AWS) (sitio web de MongoDB)
- Conexión segura de aplicaciones a un plano de datos de MongoDB Atlas con AWS PrivateLink (entrada del blog de AWS)
- Best Practices Guide for MongoDB Performance (Guía de prácticas recomendadas para el rendimiento de MongoDB) (sitio web de MongoDB)

Epics

Comprender los datos de origen

Tarea	Descripción	Habilidades requeridas
Conozca el tamaño de la base de datos de origen actual de SQL Server.	Conozca su huella actual de SQL Server. Para este fin, se pueden ejecutar consultas en el esquema `INFORMATION` de la base de datos. Determine el número de tablas y el tamaño de cada tabla. Analice el índice asociado a cada tabla. Para obtener más información sobre el análisis de SQL, consulte la entrada del blog SQL2Mongo: Data Migration Journey en el sitio web. PeerIslands	Administrador de base de datos
Comprenda el esquema de origen.	Determine el esquema de la tabla y la representación empresarial de los datos (por ejemplo, códigos postales, nombres y moneda). Utilice el diagrama de relaciones entre entidades (ER) existente o genere el diagrama ER a partir de la base de datos existente. Para obtener más información, consulte la entrada del blog SQL2Mongo: Data Migration Journey en el sitio web. PeerIslands	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Comprenda los patrones de consulta.	Documente las 10 consultas SQL principales que utiliza. Puede utilizar las tablas performance_schema .events_statements _summary_by_digest, disponibles en la base de datos, para comprender las consultas principales. Para obtener más información, consulte la entrada del blog SQL2Mongo: Data Migration Journey en el sitio web. PeerIslands	Administrador de base de datos
Comprenda los compromisos de SLA.	Documente los acuerdos de nivel de servicio (SLA) previstos para las operacion es de bases de datos. Las medidas habituales incluyen la latencia de las consultas y las consultas por segundo. Las medidas y sus objetivos suelen estar disponibles en los documentos de requisitos no funcionales (NFR).	Administrador de base de datos

Definir el esquema de MongoDB

Tarea	Descripción	Habilidades requeridas
Defina el esquema de origen.	Defina varias opciones para el esquema de MongoDB de destino. Para obtener	Ingeniero de MongoDB

Tarea	Descripción	Habilidades requeridas
	más información, consulte Schemas (Esquemas) en la documentación de MongoDB Atlas. Tenga en cuenta las prácticas recomendables y los patrones de diseño basados en las relacione s de las tablas. Consulte Data Model Examples and Patterns (Ejemplos y patrones de modelos de datos) en la documentación de MongoDB para obtener más información.	
Defina los patrones de consulta de destino.	Defina las consultas de MongoDB y las canalizac iones de agregación. Estas consultas equivalen a las consultas principales que capturó para su carga de trabajo de SQL Server. Para saber cómo construir canalizaciones de agregació n de MongoDB, consulte la documentación de MongoDB.	Ingeniero de MongoDB
Defina el tipo de instancia de MongoDB.	Determine el tamaño de la instancia que planea utilizar para las pruebas. Para obtener orientación, consulte la documentación de MongoDB.	Ingeniero de MongoDB

Prepare la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Configure el clúster de MongoDB Atlas.	Para configurar un clúster de MongoDB en AWS, siga las instrucciones de la documentación de MongoDB.	Ingeniero de MongoDB
Cree usuarios en la base de datos de destino.	Configure el clúster de MongoDB Atlas para el acceso y la seguridad de la red siguiendo las instrucciones de la documentación de MongoDB.	Ingeniero de MongoDB
Cree los roles adecuados en AWS y configure el control de acceso basado en roles para Atlas.	Si es necesario, configure usuarios adicionales siguiendo las instrucciones de la documentación de MongoDB. Configure la autenticación y la autorización mediante los roles de AWS.	Ingeniero de MongoDB
Configure Compass para el acceso a MongoDB Atlas.	Configure el programa de utilidad GUI MongoDB Compass para facilitar la navegación y el acceso.	Ingeniero de MongoDB

Configurar la carga base mediante el generador de datos de prueba

Tarea	Descripción	Habilidades requeridas
Instale el generador de datos de prueba.	Instale PeerIsland Test Data Generator en su entorno.	Ingeniero de MongoDB

Tarea	Descripción	Habilidades requeridas
Configure el generador de datos de prueba para generar los datos adecuados.	Cree una plantilla mediante la biblioteca de datos para generar datos específicos para cada campo del esquema de MongoDB. Para obtener más información, consulte MongoDB Data Generator & Perf. Vídeo del analizador.	Ingeniero de MongoDB
Generador de datos de prueba con escala horizontal para generar la carga requerida.	Utilice la plantilla que creó para iniciar la generación de cargas con respecto a la colección de destino; para ello, configure el paralelismo requerido. Determine los plazos y la escala para generar los datos necesarios.	Ingeniero de MongoDB
Valide la carga en MongoDB Atlas.	Compruebe los datos cargados en MongoDB Atlas.	Ingeniero de MongoDB
Genere los índices necesarios en MongoDB.	Defina los índices según sea necesario, en función de los patrones de consulta. Para conocer las prácticas recomendadas, consulte la documentación de MongoDB.	Ingeniero de MongoDB

Llevar a cabo pruebas de rendimiento

Tarea	Descripción	Habilidades requeridas
Configure los perfiles de carga en Performance Analyzer.	Cree un perfil de pruebas de rendimiento en Performance	Ingeniero de MongoDB

Tarea	Descripción	Habilidades requeridas
	Analyzer; para ello, configure consultas específicas y sus correspondientes ponderación, duración de la prueba y etapas. Para obtener más información, consulte MongoDB Data Generator & Perf. Vídeo del analizador.	
Ejecute las pruebas de rendimiento.	Utilice el perfil de prueba de rendimiento que creó para iniciar la prueba con respecto a la colección de destino; para ello, configure el paralelismo requerido. Escale horizontalmente la herramienta de prueba de rendimiento para ejecutar consultas en MongoDB Atlas.	Ingeniero de MongoDB
Registre los resultados de la prueba.	Registre la latencia P95 y P99 para las consultas.	Ingeniero de MongoDB
Ajuste su esquema y sus patrones de consulta.	Modifique los índices y los patrones de consulta para solucionar cualquier problema de rendimiento.	Ingeniero de MongoDB

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cerrar los recursos temporales de AWS.	Elimine todos los recursos temporales que utilizó para el	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	generador de datos de prueba y el analizador de rendimiento.	
Actualice los resultados de las pruebas de rendimiento.	Comprenda el rendimiento de las consultas de MongoDB y compárelo con sus SLA. Si es necesario, ajuste el esquema de MongoDB y vuelva a ejecutar el proceso.	Ingeniero de MongoDB
Finalice el proyecto.	Cerrar el proyecto y enviar comentarios.	Ingeniero de MongoDB

Recursos relacionados

- GitHub repositorio: S3toAtlas
- Esquema: MongoDB Schema design (Diseño de esquema de MongoDB)
- Canalizaciones de agregación: MongoDB aggregation pipelines (Canalizaciones de agregación de MongoDB)
- Dimensionamiento de MongoDB Atlas: Sizing tier selection (Selección de capa de dimensionamiento)
- Vídeo: MongoDB Data Generator & Perf. Analizador
- Referencias: documentación de MongoDB
- Tutorialws: MongoDB developer guide, MongoDB Jumpstart
- AWS Marketplace: MongoDB Atlas en AWS Marketplace
- Soluciones de socios de AWS: MongoDB Atlas on AWS Reference Deployment (Implementación de referencia de MongoDB Atlas en AWS)

Recursos adicionales:

- Análisis de SQL
- MongoDB Developer Community forums (Foros de la comunidad de desarrolladores de MongoDB)

- MongoDB Performance Tuning Questions (Preguntas sobre el ajuste del rendimiento de MongoDB)
- Operational Analytics with Atlas and Redshift (Análisis operativo con Atlas y Redshift)
- Application modernization with MongoDB Atlas and AWS Elastic Beanstalk (Modernización de aplicaciones con MongoDB Atlas y AWS Elastic Beanstalk)

Automatice la conmutación por error y la conmutación por recuperación entre regiones mediante DR Orchestrator Framework

Creado por Jitendra Kumar (AWS), Oliver Francis (AWS) y Pavithra Balasubramanian (AWS)

aws-cross-region-drRepositorio de código: -databases	Entorno: producción	Tecnologías: bases de datos; infraestructura; migración; modernización
Servicios de AWS: Amazon Aurora; AWS CloudFormation; Amazon ElastiCache; Amazon RDS; AWS Step Functions		

Resumen

Este patrón describe cómo utilizar DR Orchestrator Framework para organizar y automatizar los pasos manuales, propensos a errores, para realizar la recuperación ante desastres en todas las regiones de Amazon Web Services ().AWS El patrón cubre las siguientes bases de datos:

- Amazon Relational Database Service (Amazon RDS) para MySQL, Amazon RDS para PostgreSQL o Amazon RDS para MariaDB
- Edición compatible con Amazon Aurora MySQL o Amazon Aurora compatible con PostgreSQL (mediante un archivo centralizado)
- Amazon ElastiCache para Redis

Para demostrar la funcionalidad de DR Orchestrator Framework, debe crear dos instancias o clústeres de bases de datos. El principal está en y Región de AWS `us-east-1` el secundario está dentro. `us-west-2` Para crear estos recursos, utilice las AWS CloudFormation plantillas de la `App-Stack` carpeta del GitHub repositorio aws-cross-region-dr-databases.

Requisitos previos y limitaciones

Requisitos previos generales

- El marco DR Orchestrator se implementó tanto en el sistema primario como en el secundario Regiones de AWS
- Dos depósitos de Amazon Simple Storage Service
- Una nube privada virtual (VPC) con dos subredes y un grupo de seguridad AWS

Requisitos previos específicos del motor

- Amazon Aurora: debe haber al menos una base de datos global de Aurora disponible en dos Regiones de AWS. Puede utilizarla `us-east-1` como región principal y utilizarla `us-west-2` como región secundaria.
- Amazon ElastiCache for Redis: un almacén de datos ElastiCache global debe estar disponible en dos. Regiones de AWS Puede `use us-east-1` utilizarla como región principal y usarla `us-west-2` como región secundaria.

Limitaciones de Amazon RDS

- DR Orchestrator Framework no comprueba el retraso de la replicación antes de realizar una conmutación por error o una conmutación por recuperación. El retraso de la replicación debe comprobarse manualmente.
- Esta solución se probó con una instancia de base de datos principal con una réplica de lectura. Si desea utilizar más de una réplica de lectura, pruebe la solución minuciosamente antes de implementarla en un entorno de producción.

Limitaciones de Aurora

- La disponibilidad y el soporte de las funciones varían según las versiones específicas de cada motor de base de datos y entre ellas Regiones de AWS. Para obtener más información sobre la disponibilidad de funciones y regiones para la replicación entre regiones, consulte Réplicas de lectura entre regiones.
- Las bases de datos globales de Aurora tienen requisitos de configuración específicos para las clases de instancias de base de datos Aurora compatibles y el número máximo de Regiones de AWS. Para obtener más información, consulte Requisitos de configuración de una base de datos global de Amazon Aurora.

- Esta solución se probó con una instancia de base de datos principal con una réplica de lectura. Si desea utilizar más de una réplica de lectura, pruebe la solución minuciosamente antes de implementarla en un entorno de producción.

ElastiCache limitaciones

- Para obtener información sobre la disponibilidad regional del almacén de datos global y los requisitos de ElastiCache configuración, consulte los requisitos previos y las limitaciones en la documentación. ElastiCache

Versiones de productos Amazon RDS Up

Amazon RDS es compatible con las siguientes versiones de motor:

- MySQL: Amazon RDS admite instancias de base de datos que ejecutan las siguientes versiones de MySQL: MySQL 8.0 y MySQL 5.7
- PostgreSQL: para obtener información sobre las versiones compatibles de Amazon RDS para PostgreSQL, consulte Versiones de bases de datos PostgreSQL disponibles.
- MariaDB: Amazon RDS admite instancias de base de datos que ejecutan las siguientes versiones de MariaDB:
  - MariaDB 10.11
  - MariaDB 10.6
  - MariaDB 10.5

Versiones de productos Aurora

- El cambio de base de datos global de Amazon Aurora requiere que Aurora sea compatible con MySQL y MySQL 5.7, versión 2.09.1 y superior

  Para obtener más información, consulte Limitaciones de las bases de datos globales de Amazon Aurora.

ElastiCache para las versiones de los productos de Redis

Amazon ElastiCache for Redis es compatible con las siguientes versiones de Redis:

- Redis 7.1 (mejorada)

- Redis 7.0 (mejorada)
- Redis 6.2 (mejorada)
- Redis 6.0 (mejorada)
- Redis 5.0.6 (mejorada)

Para obtener más información, consulte las versiones compatibles con ElastiCache Redis.

Arquitectura

Arquitectura Amazon RDS

La arquitectura de Amazon RDS incluye los siguientes recursos:

- La instancia de base de datos de Amazon RDS principal creada en la región principal (`us-east-1`) con acceso de lectura y escritura para los clientes
- Una réplica de lectura de Amazon RDS creada en la región secundaria (`us-west-2`) con acceso de solo lectura para los clientes
- El marco DR Orchestrator se implementó tanto en la región principal como en la secundaria

En el diagrama se muestra lo siguiente:

1. Replicación asíncrona entre la instancia principal y la instancia secundaria
2. Acceso de lectura y escritura para los clientes de la región principal
3. Acceso de solo lectura para los clientes de la región secundaria

Arquitectura Aurora

La arquitectura Amazon Aurora incluye los siguientes recursos:

- El clúster de base de datos Aurora principal creado en la región principal (`us-east-1`) con un punto final de escritura activa
- Un clúster de base de datos Aurora creado en la región secundaria (`us-west-2`) con un punto final de escritura inactivo
- El marco DR Orchestrator se implementó tanto en la región principal como en la secundaria

En el diagrama se muestra lo siguiente:

1. Replicación asíncrona entre el clúster principal y el clúster secundario
2. El clúster de base de datos principal con un punto final de escritura activa
3. El clúster de base de datos secundario con un punto final de escritura inactiva

ElastiCache para la arquitectura Redis

La arquitectura Amazon ElastiCache for Redis incluye los siguientes recursos:

- Un almacén de datos global ElastiCache para Redis creado con dos clústeres:
  1. El clúster principal de la región principal () `us-east-1`
  2. El clúster secundario de la región secundaria (`us-west-2`)
- Un enlace entre regiones de Amazon con cifrado TLS 1.2 entre los dos clústeres
- El marco DR Orchestrator se implementó en las regiones principal y secundaria

Automatizar y escalar

DR Orchestrator Framework es escalable y admite la conmutación por error o la conmutación por recuperación de más de una base de datos AWS en paralelo.

Puede utilizar el siguiente código de carga útil para conmutar por error varias AWS bases de datos de su cuenta. En este ejemplo, tres AWS bases de datos (dos bases de datos globales, como Aurora MySQL o Aurora PostgreSQL, y una instancia de Amazon RDS for MySQL) se conmutan por error a la región DR:

```
{
  "StatePayload": [
    {
      "layer": 1,
      "resources": [
        {
          "resourceType": "PlannedFailoverAurora",
          "resourceName": "Switchover (planned failover) of Amazon Aurora global
 databases (MySQL)",
```

```
          "parameters": {
            "GlobalClusterIdentifier": "!Import dr-globaldb-cluster-mysql-global-
identifier",
            "DBClusterIdentifier": "!Import dr-globaldb-cluster-mysql-cluster-
identifier"
          }
        },
        {
          "resourceType": "PlannedFailoverAurora",
          "resourceName": "Switchover (planned failover) of Amazon Aurora global
 databases (PostgreSQL)",
          "parameters": {
            "GlobalClusterIdentifier": "!Import dr-globaldb-cluster-postgres-global-
identifier",
            "DBClusterIdentifier": "!Import dr-globaldb-cluster-postgres-cluster-
identifier"
          }
        },
        {
          "resourceType": "PromoteRDSReadReplica",
          "resourceName": "Promote RDS for MySQL Read Replica",
          "parameters": {
            "RDSInstanceIdentifier": "!Import rds-mysql-instance-identifier",
            "TargetClusterIdentifier": "!Import rds-mysql-instance-global-arn"
          }
        }
      ]
    }
  ]
}
```

Herramientas

AWS servicios

- Amazon Aurora es un motor de base de datos relacional completamente administrado diseñado para la nube y compatible con MySQL y PostgreSQL.
- Amazon le ElastiCache ayuda a configurar, gestionar y escalar los entornos de caché en memoria distribuidos en. Nube de AWS Este patrón usa Amazon ElastiCache for Redis.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que

utilice. En este patrón, las funciones Lambda se utilizan AWS Step Functions para realizar los pasos.

- Amazon Relational Database Service (Amazon RDS) le ayuda a configurar, operar y escalar una base de datos relacional en. Nube de AWS Este patrón es compatible con Amazon RDS para MySQL, Amazon RDS para PostgreSQL y Amazon RDS para MariaDB.
- AWS SDK for Python (Boto3)le ayuda a integrar su aplicación, biblioteca o script de Python con Servicios de AWS. En este patrón, las API de Boto3 se utilizan para comunicarse con las instancias de la base de datos o las bases de datos globales.
- AWS Step Functionses un servicio de organización sin servidor que le ayuda a combinar AWS Lambda funciones y otras Servicios de AWS para crear aplicaciones críticas para la empresa. En este patrón, las máquinas de estado Step Functions se utilizan para organizar y ejecutar la conmutación por error y la conmutación por recuperación entre regiones de las instancias de bases de datos o las bases de datos globales.

Repositorio de código

El código de este patrón está disponible en el repositorio -databases deaws-cross-region-dr. GitHub

Epics

Instale DR Orchestrator Framework

Tarea	Descripción	Habilidades requeridas
Clona el GitHub repositorio.	Para clonar el repositorio, ejecute el siguiente comando: `git clone https://github.com/aws-samples/aws-cross-region-dr-databases.git`	AWS DevOps, administrador de AWS
Package el código de las funciones de Lambda en un archivo de archivos.zip.	Cree los archivos de almacenamiento para las funciones de Lambda para incluir las dependencias de DR Orchestrator Framework:	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	`cd <YOUR-LOCAL-GIT-FOLDER>/DR-Orchestration-artifacts` `bash scripts/deploy-orchestrator-sh.sh`	
Cree depósitos de S3.	Los cubos S3 son necesarios para almacenar DR Orchestrator Framework junto con la configuración más reciente. Cree dos depósitos de S3, uno en la región principal (`us-east-1`) y otro en la región secundaria (): `us-west-2` • `dr-orchestrator-xxxxxx-us-east-1` • `dr-orchestrator-xxxxxx-us-west-2` `xxxxxx`Sustitúyalo por un valor aleatorio para que los nombres de los cubos sean únicos.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Cree subredes y grupos de seguridad.	Tanto en la región principal (`us-east-1`) como en la región secundaria (`us-west-2`), cree dos subredes y un grupo de seguridad para implementar la función Lambda en la VPC: • `subnet-XXXXXXX` • `subnet-YYYYYYY` • `sg-XXXXXXXXXXX`	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Actualice los archivos de parámetros de DR Orchestrator.	En la `<YOUR-LOCAL-GIT-FOLDER>/DR-Orchestration-artifacts/cloudformation` carpeta, actualice los siguientes archivos de parámetros de DR Orchestrator: • `Orchestrator-Deployer-parameters-us-east-1.json` • `Orchestrator-Deployer-parameters-us-west-2.json` Utilice los siguientes valores de parámetros, sustituyendo x y por y los nombres de sus recursos: `[ { "ParameterKey": "TemplateStoreS3BucketName", "ParameterValue": "dr-orchestrator-xxxxxx-us-east-1" }, { "ParameterKey": "TemplateVPCId", "ParameterValue": "vpc-xxxxxx" }, {`	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	`"ParameterKey": "TemplateLambdaSubnetID1", "ParameterValue": "subnet-xxxxx" }, { "ParameterKey": "TemplateLambdaSubnetID2", "ParameterValue": "subnet-yyyyy" }, { "ParameterKey": "TemplateLambdaSecurityGroupID", "ParameterValue": "sg-xxxxxxxxxx" } ]`	

Tarea	Descripción	Habilidades requeridas
Cargue el código de DR Orchestrator Framework en el bucket de S3.	El código estará más seguro en un bucket de S3 que en el directorio local. Cargue el `DR-Orchestration-artifacts` directorio, incluidos todos los archivos y subcarpetas, en los cubos de S3. Para cargar el código, haga lo siguiente: 1. Inicie sesión en AWS Management Console. 2. Vaya a la consola de Amazon IVS. 3. Seleccione la `dr-orchestrator-xxxxxx-us-east-1 bucket` . 4. Selecciona Cargar y, a continuación, selecciona Añadir carpeta. 5. Seleccione la carpeta `DR-Orchestration-artifacts` . 6. Seleccione Cargar. 7. Selecciona el `dr-orchestrator-xxxxxx-us-west-2` depósito. 8. Repita los pasos 4 a 7.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Implemente DR Orchestrator Framework en la región principal.	Para implementar DR Orchestrator Framework en la región principal (`us-east-1`), ejecuta los siguientes comandos: `cd <YOUR-LOCAL-GIT-FOLDER>/DR-Orchestration-artifacts/cloudformation` `aws cloudformation deploy \` `--region us-east-1 \` `--stack-name dr-orchestrator \` `--template-file Orchestrator-Deployer.yaml \` `--parameter-overrides file://Orchestrator-Deployer-parameters-us-east-1.json \` `--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \` `--disable-rollback`	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Implemente DR Orchestrator Framework en la región secundaria.	En la región secundaria (`us-west-2`), ejecute los siguientes comandos: `cd <YOUR-LOCAL-GIT-FOLDER>/DR-Orchestration-artifacts/cloudformation` `aws cloudformation deploy \` `--region us-west-2 \` `--stack-name dr-orchestrator \` `--template-file Orchestrator-Deployer.yaml \` `--parameter-overrides file://Orchestrator-Deployer-parameters-us-west-2.json \` `--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \` `--disable-rollback`	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Comprobar la implementación.	Si el AWS CloudFormation comando se ejecuta correctamente, devuelve el siguiente resultado: `Successfully created/ updated stack - dr-orchestrator` Como alternativa, puede ir a la AWS CloudFormation consola y verificar el estado de la `dr-orchestrator` pila.	Administrador de AWS

Cree las instancias o los clústeres de la base de datos

Tarea	Descripción	Habilidades requeridas
Cree las subredes y los grupos de seguridad de la base de datos.	En su VPC, cree dos subredes y un grupo de seguridad para la instancia de base de datos o la base de datos global en las regiones principal (`us-east-1`) y secundaria (`us-west-2`): • `subnet-XXXXXX` • `subnet-XXXXXX` • `sg-XXXXXXXXXX`	Administrador de AWS
Actualice el archivo de parámetros de la instancia de base de datos o el clúster principal.	En la `<YOUR LOCAL GIT FOLDER>/App-Stack` carpeta, actualice el archivo	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	de parámetros de la región principal. Amazon RDS En el `RDS-MySQL-parameter-us-east-1.json` archivo, actualice `SubnetIds` y `DBSecurityGroup` con los nombres de los recursos que creó: `{ "Parameters": { "SubnetIds": "subnet-xxxxxx,subnet-xxxxxx", "DBSecurityGroup": "sg-xxxxxxxxxx", "MySqlGlobalIdentifier":"rds-mysql-instance", "InitialDatabaseName": "mysqldb", "DBPortNumber": "3789", "PrimaryRegion": "us-east-1", "SecondaryRegion": "us-west-2", "KMSKeyAliasName": "rds/rds-mysql-instance-KmsKeyId" } }` Amazon Aurora	

Tarea	Descripción	Habilidades requeridas
	En el `Aurora-MySQL-parameter-us-east-1.json` archivo, actualice `SubnetIds` y `DBSecurityGroup` con los nombres de los recursos que creó: `{ "Parameters": { "SubnetIds": "subnet1-xxxxxx,subnet2-xxxxxx", "DBSecurityGroup": "sg-xxxxxxxxxx", "GlobalClusterIdentifier":"dr-globaldb-cluster-mysql", "DBClusterName":"dbcluster-01", "SourceDBClusterName":"dbcluster-02", "DBPortNumber": "3787", "DBInstanceClass": "db.r5.large", "InitialDatabaseName": "sampledb", "PrimaryRegion": "us-east-1", "SecondaryRegion": "us-west-2", "KMSKeyAliasName": "rds/dr-globaldb-cluster-mysql-KmsKeyId" } }`	

Tarea	Descripción	Habilidades requeridas
	Amazon ElastiCache para Redis En el `ElastiCache-parameter-us-east-1.json` archivo, actualice `SubnetIds` y `DBSecurityGroup` con los nombres de los recursos que creó. `{ "Parameters": { "CacheNodeType": "cache.m5.large", "DBSecurityGroup": "sg-xxxxxxxxxx", "SubnetIds": "subnet-xxxxxx,subnet-xxxxxx", "EngineVersion": "5.0.6", "GlobalReplicationGroupIdSuffix": "demo-redis-global-datastore", "NumReplicas": "1", "NumShards": "1", "ReplicationGroupId": "demo-redis-cluster", "DBPortNumber": "3788", "TransitEncryption": "true", "KMSKeyAliasName": "elasticache/demo-redis-global-datastore-KmsKeyId",`	

Tarea	Descripción	Habilidades requeridas
	<pre>"PrimaryRegion": "us-east-1", "SecondaryRegion": "us-west-2" } }</pre>	

Tarea	Descripción	Habilidades requeridas
Implemente su instancia de base de datos o clúster en la región principal.	Para implementar la instancia o el clúster en la región principal (`us-east-1`), ejecute los siguientes comandos en función del motor de base de datos. Amazon RDS `cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack` `aws cloudformation deploy \` `--region us-east-1 \` `--stack-name rds-mysql-app-stack \` `--template-file RDS-MySQL-Primary.yaml \` `--parameter-overrides file://RDS-MySQL-parameter-us-east-1.json \` `--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \` `--disable-rollback` Amazon Aurora `cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack` `aws cloudformation deploy \` `--region us-east-1 \`	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	`--stack-name aurora-mysql-app-stack \ --template-file Aurora-MySQL-Primary.yaml \ --parameter-overrides file://Aurora-MySQL-parameter-us-east-1.json \ --capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \ --disable-rollback` Amazon ElastiCache para Redis `cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack` `aws cloudformation deploy \ --region us-east-1 --stack-name elasticache-ds-app-stack \ --template-file ElastiCache-Primary.yaml \ --parameter-overrides file://ElastiCache-parameter-us-east-1.json \ --capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \ --disable-rollback`	

Tarea	Descripción	Habilidades requeridas
	Compruebe que los AWS CloudFormation recursos se han desplegado correctam ente.	

Tarea	Descripción	Habilidades requeridas
Actualice el archivo de parámetros de la instancia de base de datos secundaria o del clúster.	En la <YOUR LOCAL GIT FOLDER>/App-Stack carpeta, actualice el archivo de parámetros de la región secundaria. Amazon RDS En el RDS-MySQL-parameter-us-west-2.json archivo, actualice SubnetIDs y DBSecurityGroup con los nombres de los recursos que creó. Actualice el valor PrimaryRegionKMSKeyArn con el valor MySQLKmsKeyId obtenido de la sección de resultados de la AWS CloudFormation pila de la instancia de base de datos principal: `{ "Parameters": { "SubnetIds": "subnet-aaaaaaaaa, subnet-bbbbbbbbb", "DBSecurityGroup": "sg-ccccccccc", "MySqlGlobalIdentifier":"rds-mysql-instance", "InitialDatabaseName": "mysqldb", "DBPortNumber": "3789",`	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	<pre> "PrimaryRegion": "us-east-1", "SecondaryRegion": "us-west-2", "KMSKeyAliasName": "rds/rds-mysql-ins tance-KmsKeyId", "PrimaryRegionKMSK eyArn":"arn:aws:km s:us-east-1:xxxxxx xxx:key/mrk-xxxxxx xxxxxxxxxxxxxx" } }</pre>	
	Amazon Aurora En el `Aurora-MySQL-parameter-us-west-2.json` archivo, actualice `SubnetIDs` y `DBSecurityGroup` con los nombres de los recursos que creó. Actualice el valor `PrimaryRegionKMSKeyArn` con el valor `AuroraKmsKeyId` obtenido de la sección de resultados de la AWS CloudFormation pila de la instancia de base de datos principal: <pre>{ "Parameters": { "SubnetIds": "subnet1-aaaaaaaaa ,subnet2-bbbbbbbbb",</pre>	

Tarea	Descripción	Habilidades requeridas
	"DBSecurityGroup": "sg-ccccccccc", "GlobalClusterIdentifier":"dr-globaldb-cluster-mysql", "DBClusterName":"dbcluster-01", "SourceDBClusterName":"dbcluster-02", "DBPortNumber": "3787", "DBInstanceClass": "db.r5.large", "InitialDatabaseName": "sampledb", "PrimaryRegion": "us-east-1", "SecondaryRegion": "us-west-2", "KMSKeyAliasName": "rds/dr-globaldb-cluster-mysql-KmsKeyId" } } Amazon ElastiCache para Redis En el `ElastiCache-parameter-us-west-2.json` archivo, actualice `SubnetIDs` y `DBSecurityGroup` con los nombres de los recursos que creó. Actualice el valor `PrimaryRegionKMSKeyArn` con el valor `ElastiCacheKmsKeyI`	

Tarea	Descripción	Habilidades requeridas
	d obtenido de la sección de resultados de la AWS CloudFormation pila de la instancia de base de datos principal: `{ "Parameters": { "CacheNodeType": "cache.m5.large", "DBSecurityGroup": "sg-cccccccccc", "SubnetIds": "subnet-aaaaaaaaa, subnet-bbbbbbbbb", "EngineVersion": "5.0.6", "GlobalReplicationGroupIdSuffix": "demo-redis-global-datastore", "NumReplicas": "1", "NumShards": "1", "ReplicationGroupId": "demo-redis-cluster", "DBPortNumber": "3788", "TransitEncryption": "true", "KMSKeyAliasName": "elasticache/demo-redis-global-datastore-KmsKeyId", "PrimaryRegion": "us-east-1", "SecondaryRegion": "us-west-2" } }`	

Tarea	Descripción	Habilidades requeridas
Implemente su instancia de base de datos o clúster en la región secundaria.	Ejecute los siguientes comandos, en función del motor de base de datos. Amazon RDS `cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack` `aws cloudformation deploy \` `--region us-west-2 \` `--stack-name rds-mysql-app-stack \` `--template-file RDS-MySQL-DR.yaml \` `--parameter-overrides file://RDS-MySQL-parameter-us-west-2.json \` `--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \` `--disable-rollback` Amazon Aurora `cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack` `aws cloudformation deploy \` `--region us-west-2 \` `--stack-name aurora-mysql-app-stack \` `--template-file Aurora-MySQL-DR.yaml \`	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	`--parameter-overrides file://Aurora-MySQL-parameter-us-west-2.json \ --capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \ --disable-rollback`	
	Amazon ElastiCache para Redis	
	`cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack` `aws cloudformation deploy \ --region us-west-2 \ --stack-name elasticache-ds-app-stack \ --template-file ElastiCache-DR.yaml \ --parameter-overrides file://ElastiCache-parameter-us-west-2.json \ --capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \ --disable-rollback`	
	Compruebe que los AWS CloudFormation recursos se han desplegado correctamente.	

Recursos relacionados

- Estrategia de recuperación ante desastres para bases de datos en AWS vigor (estrategia de orientación AWS prescriptiva)
- Automatice su solución de recuperación ante desastres para bases de datos relacionales en AWS(guía de orientación AWS prescriptiva)
- Uso de bases de datos globales de Amazon Aurora
- Replicación Regiones de AWS mediante el uso de almacenes de datos globales
- Automatice su solución de DR para bases de datos relacionales en AWS (guía de orientación AWS prescriptiva)

Automatice la replicación de las instancias de Amazon RDS en todas las cuentas de AWS

Creado por Parag Nagwekar (AWS) y Arun Chandapillai (AWS)

Entorno: producción	Tecnologías: bases de datos; sin servidor; infraestructura DevOps	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: AWS Lambda; Amazon RDS; AWS SDK para Python (Boto3); AWS Step Functions; Amazon SNS		

Resumen

Este patrón le muestra cómo automatizar el proceso de replicación, seguimiento y restauración de sus instancias de base de datos de Amazon Relational Database Service (Amazon RDS) en distintas cuentas de AWS mediante AWS Step Functions y AWS Lambda. Puede utilizar esta automatización para realizar una replicación a gran escala de instancias de base de datos de RDS sin que ello afecte al rendimiento ni a los gastos operativos adicionales, independientemente del tamaño de su organización. También puede usar este patrón para ayudar a su organización a cumplir con las estrategias de gobernanza de datos obligatorias o los requisitos de conformidad que exigen que sus datos se repliquen y sean redundantes en diferentes cuentas y regiones de AWS. La replicación entre cuentas de los datos de Amazon RDS a escala es un proceso manual ineficiente y propenso a errores que puede resultar costoso y llevar mucho tiempo, pero la automatización de este patrón puede ayudarle a conseguir la replicación entre cuentas de forma segura, eficaz y eficiente.

Requisitos previos y limitaciones

Requisitos previos

- Dos cuentas de AWS
- Una instancia de base de datos de RDS, activa y en ejecución en la cuenta de AWS de origen

- Un grupo de subredes para la instancia de base de datos de RDS en la cuenta de AWS de destino
- Una clave de AWS Key Management Service (AWS KMS) creada en la cuenta de AWS de origen y compartida con la cuenta de destino (para obtener más información sobre los detalles de la política, consulte la sección Additional information (Información adicional) de este patrón).
- Una clave de AWS KMS en la cuenta de AWS de destino para cifrar la base de datos en la cuenta de destino

Versiones de producto

- Python 3.9 (con AWS Lambda)
- PostgreSQL 11.3, 13.x y 14.x

Arquitectura

Pila de tecnología

- Amazon Relational Database Service (Amazon RDS)
- Amazon Simple Notification Service (Amazon SNS)
- AWS Key Management Service (AWS KMS)
- AWS Lambda
- AWS Secrets Manager
- AWS Step Functions

Arquitectura de destino

El siguiente diagrama muestra una arquitectura para usar Step Functions para orquestar la replicación programada y bajo demanda de instancias de base de datos de RDS desde una cuenta de origen (cuenta A) a una cuenta de destino (cuenta B).

En la cuenta de origen (cuenta A en el diagrama), la máquina de estados Step Functions realiza lo siguiente:

1. Crea una instantánea de la instancia de base de datos de RDS en la cuenta A.

2. Copia y cifra la instantánea con una clave de AWS KMS de la cuenta A. Para garantizar el cifrado en tránsito, la instantánea se cifra independientemente de que la instancia de base de datos esté cifrada o no.
3. Comparte la instantánea de base de datos con la cuenta B al permitir que la cuenta B acceda a la instantánea.
4. Envía una notificación al tema de SNS y, a continuación, el tema de SNS invoca la función de Lambda en la cuenta B.

En la cuenta de destino (cuenta B en el diagrama), la función de Lambda ejecuta la máquina de estados Step Functions para orquestar lo siguiente:

1. Copiar la instantánea compartida de la cuenta A a la cuenta B y, al mismo tiempo, utilizar la clave de AWS KMS de la cuenta A para descifrar primero los datos y, a continuación, cifrarlos con la clave de AWS KMS de la cuenta B.
2. Leer el secreto de Secrets Manager para capturar el nombre de la instancia de base de datos actual.
3. Restaurar la instancia de base de datos de la instantánea con un nombre nuevo y una clave de AWS KMS predeterminada para Amazon RDS.
4. Leer el punto de conexión de la nueva base de datos y actualizar el secreto de Secrets Manager con el nuevo punto de conexión de la base de datos y, a continuación, etiquetar la instancia de base de datos anterior para poder eliminarla más adelante.
5. Conservar las N instancias más recientes de las bases de datos y eliminar todas las demás instancias.

Herramientas

Herramientas de AWS

- Amazon Relational Database Service (Amazon RDS) lo ayuda a configurar, utilizar y escalar una base de datos relacional en la Nube de AWS.
- Amazon Simple Notification Service (Amazon SNS) permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.

- AWS Key Management Service (AWS KMS) facilita poder crear y controlar claves criptográficas para proteger los datos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS SDK para Python (Boto3) es un kit de desarrollo de software que permite integrar su aplicación, biblioteca o script de Python con los servicios de AWS.
- AWS Secrets Manager le permite reemplazar las credenciales codificadas en el código, incluidas las contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación.
- AWS Step Functions es un servicio de orquestación sin servidor que le permite combinar funciones de Lambda y otros servicios de AWS para crear aplicaciones esenciales desde el punto de vista empresarial.

Code

El código de este patrón está disponible en el repositorio GitHub Crossaccount RDS Replication.

Epics

Automatice la replicación de instancias de bases de datos de RDS en todas las cuentas de AWS con un solo clic

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation pila en la cuenta de origen.	1. Inicie sesión en la consola de administración de AWS de la cuenta de origen (cuenta A) y abra la CloudFormation consola. 2. En el panel de navegación, seleccione Stacks (Pilas). 3. Elija Create stack (Crear pila) y, a continuación, seleccione With existing	Administrador de la nube, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	resources (import resources) (Con recursos existentes (importar recursos)). 4. En la página Identific ar recursos, seleccione Siguiente. 5. En la página Specify Template (Especificar plantilla), seleccione Upload a template (Subir una plantilla). 6. Elija Elegir archivo, seleccione el **`Cloudform ation-SourceAccoun tRDS.yaml`** archivo del repositorio de GitHub Crossaccount RDS Replication y, a continuac ión, elija Siguiente. 7. En Stack name (Nombre de pila), escriba un nombre para su pila. 8. En la sección Parameter s (Parámetros), especifiq ue los parámetros que se definen en la plantilla de la pila: • Para DestinationAccount Number, introduzca el número de cuenta de la instancia de base de datos de RDS de destino.	

Tarea	Descripción	Habilidades requeridas
	• Para KeyName, introduzca su clave de AWS KMS. • Para ScheduleExpression, introduzca una expresión cron (el valor predeterminado es a las 12:00 de la mañana todos los días). • En SourceDBIdentifier (Identificador de la base de datos de origen), escriba el nombre de la base de datos de origen. • Para SourceDBSnapshotName, introduzca el nombre de la instantánea o acepte el nombre predeterminado. 9. Elija Next (Siguiente). 10. En la página Configure stack options (Configurar opciones de la pila), mantenga las opciones predeterminadas y elija Next (Siguiente). 11. Revise la configuración de la pila y seleccione Submit (Enviar). 12. Seleccione la pestaña Resources (Recursos) para su pila y, a continuación, anote el Nombre de recurso	

Tarea	Descripción	Habilidades requeridas
	de Amazon (ARN) del tema de SNS.	

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation pila en la cuenta de destino.	1. Inicie sesión en la consola de administración de AWS de la cuenta de destino (cuenta B) y abra la CloudFormation consola. 2. En el panel de navegación, seleccione Stacks (Pilas). 3. Elija Create stack (Crear pila) y, a continuación, seleccione With existing resources (import resources) (Con recursos existentes (importar recursos)). 4. En la página Identific ar recursos, seleccione Siguiente. 5. En la página Specify Template (Especificar plantilla), seleccione Upload a template (Subir una plantilla). 6. Elija un archivo, selección elo del **`Cloudform ation-DestinationA ccountRDS.yaml`** repositorio de GitHub Crossaccount RDS Replication y, a continuac ión, elija Siguiente. 7. En Stack name (Nombre de pila), escriba un nombre para su pila.	Arquitecto, DevOps ingeniero y administrador de la nube

Tarea	Descripción	Habilidades requeridas
	8. En la sección Parameters (Parámetros), especifique los parámetros que se definen en la plantilla de la pila: • Para DatabaseName, introduzca un nombre para la base de datos. • En Engine (Motor), introduzca el tipo de motor de base de datos que coincida con la base de datos fuente. • Para DB InstanceClass, introduzca el tipo de instancia de base de datos preferido o acepte el predeterminado. • En Subnetgrups (Grupos de subredes), introduzca el grupo de subredes de VPC existente. Para obtener instrucciones sobre cómo crear un grupo de subredes, consulte el paso 2: Crear un grupo de subredes de base de datos en la Guía del usuario de Amazon RDS. • Para SecretName, introduzca la ruta y el nombre secreto o acepte	

Tarea	Descripción	Habilidades requeridas
	los valores predeterm inados. • Para SGID, introduzca el ID del grupo de seguridad del clúster de destino. • Para KMSKey (Clave KMS), introduzca el ARN de la clave KMS en su cuenta de destino. • Para NoOfOlderInstances ello, introduzca el número de copias antiguas de las instancias de base de datos de RDS que desea conservar para la reversión. 9. Elija Next (Siguiente). 10. En la página Configure stack options (Configur ar opciones de la pila), mantenga las opciones predeterminadas y elija Next (Siguiente). 11. Revise la configuración de la pila y seleccione Submit (Enviar). 12. Elija la pestaña Resources (Recursos) para su pila y, a continuación, anote el ID físico y el ARN de `InvokeStepFunction` .	

Tarea	Descripción	Habilidades requeridas
Compruebe la creación de la instancia de base de datos de RDS en la cuenta de destino.	1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon RDS. 2. En el panel de navegación, elija Databases (Bases de datos) y, a continuación, compruebe que la nueva instancia de base de datos de RDS aparece en el nuevo clúster.	Administrador de nube, arquitecto de nube, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Suscriba la función de Lambda al tema de SNS.	Debe ejecutar los siguiente s comandos de la interfaz de la línea de comandos de AWS (AWS CLI) para suscribir la función de Lambda de la cuenta de destino (cuenta B) al tema de SNS de la cuenta de origen (cuenta A). En la cuenta A, ejecute el siguiente comando: `aws sns add-permission \ --label lambda-access --aws-account-id <DestinationAccount> \ --topic-arn <Arn of SNSTopic > \ --action-name Subscribe ListSubscriptionsB yTopic` En la cuenta B, ejecute el siguiente comando: `aws lambda add-permi ssion \ --function-name <Name of InvokeStepFunction > \ --source-arn <Arn of SNSTopic > \ --statement-id function-with-sns \ --action lambda:In vokeFunction \`	Administrador de la nube, arquitecto de la nube y administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	`--principal sns.amazonaws.com` En la cuenta B, ejecute el siguiente comando: `aws sns subscribe \ --protocol "lambda" \ --topic-arn <Arn of SNSTopic> \ --notification-endpoint <Arn of InvokeStepFunction>`	

Tarea	Descripción	Habilidades requeridas
Sincronice la instancia de base de datos de RDS de la cuenta de origen con la cuenta de destino.	Inicie la replicación de la base de datos bajo demanda iniciando la máquina de estados Step Functions en la cuenta de origen. 1. Abra la consola Step Functions. 2. En el panel de navegación, elija State machines (Máquinas de estado). 3. Elija su máquina de estado. 4. En la pestaña Executions (Ejecuciones), seleccione la función y, a continuación, elija Start execution (Iniciar ejecución) para iniciar el flujo de trabajo. Nota: Hay un programador para ayudarlo a ejecutar la replicación automáticamente según lo programado, pero el programador está desactivado de forma predeterminada. Puedes encontrar el nombre de la CloudWatch regla de Amazon para el programador en la pestaña Recursos de la CloudFormation pila de la cuenta de destino. Para obtener instrucciones sobre cómo modificar la regla de CloudWatch eventos, consulte	Arquitecto de nube, DevOps ingeniero y administrador de nube

Tarea	Descripción	Habilidades requeridas
	Eliminar o deshabilitar una regla de CloudWatch eventos en la Guía del CloudWatch usuario.	
Restaure su base de datos a cualquiera de las copias anteriores cuando sea necesario.	1. Abra la consola de Secrets Manager. 2. De la lista de secretos, elige el secreto que creaste con la CloudFormation plantilla anterior. Su aplicación usa el secreto para acceder a la base de datos del clúster de destino. 3. Para actualizar el valor secreto desde la página de detalles, en la sección Secret value (Valor del secreto), elija Retrieve secret value (Recupera r valor del secreto) y, a continuación, Edit (Editar). 4. Introduzca los detalles del punto de conexión de la base de datos.	Administrador de la nube, administrador de bases de datos, ingeniero DevOps

Recursos relacionados

- Réplicas de lectura entre regiones (Guía de usuario de Amazon RDS)
- Implementaciones azules/verdes (Guía del usuario de Amazon RDS)

Información adicional

Usted puede usar el siguiente ejemplo de política para compartir su clave de AWS KMS en todas las cuentas de AWS.

```
{
    "Version": "2012-10-17",
    "Id": "cross-account-rds-kms-key",
    "Statement": [
        {
            "Sid": "Enable user permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::<SourceAccount>:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow administration of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::<DestinationAccount>:root"
            },
            "Action": [
                "kms:Create*",
                "kms:Describe*",
                "kms:Enable*",
                "kms:List*",
                "kms:Put*",
                "kms:Update*",
                "kms:Revoke*",
                "kms:Disable*",
                "kms:Get*",
                "kms:Delete*",
                "kms:ScheduleKeyDeletion",
                "kms:CancelKeyDeletion"
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow use of the key",
            "Effect": "Allow",
```

```
            "Principal": {
                "AWS": [
                    "arn:aws:iam::<DestinationAccount>:root",
                    "arn:aws:iam::<SourceAccount>:root"
                ]
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey",
                "kms:CreateGrant"
            ],
            "Resource": "*"
        }
    ]
}
```

Realice copias de seguridad automáticas de las bases de datos de SAP HANA mediante Systems Manager y EventBridge

Creado por Ambarish Satarkar (AWS) y Gaurav Rath (AWS)

Repositorio de código: HDB_Backup_SSM_Document	Entorno: producción	Tecnologías: bases de datos; almacenamiento y copia de seguridad
Carga de trabajo: SAP	Servicios de AWS: Amazon EC2; Amazon EventBridge; Amazon S3; AWS Systems Manager	

Resumen

Este patrón describe cómo automatizar las copias de seguridad de bases de datos de SAP HANA mediante AWS Systems Manager EventBridge, Amazon, Amazon Simple Storage Service (Amazon S3) y AWS Backint Agent para SAP HANA.

Este patrón proporciona un enfoque basado en script de intérprete de comandos utilizando el comando `BACKUP DATA` y elimina la necesidad de mantener scripts y configuraciones de trabajo para cada instancia de sistema operativo (OS) a través de numerosos sistemas.

Nota: A partir de abril de 2023, AWS Backup anunció compatibilidad con las bases de datos de SAP HANA en Amazon Elastic Compute Cloud (Amazon EC2). Para obtener más información, consulte Copia de seguridad de bases de datos de SAP HANA en instancias de Amazon EC2.

Según las necesidades de su organización, puede utilizar el servicio AWS Backup para hacer copias de seguridad automáticas de sus bases de datos de SAP HANA o puede utilizar este patrón.

Requisitos previos y limitaciones

Requisitos previos

- Una instancia de SAP HANA con una versión compatible en estado de ejecución en una instancia de Amazon Elastic Compute Cloud (Amazon EC2) gestionada que esté configurada para Systems Manager
- Debe contar con la versión 2.3.274.0 de Systems Manager Agent (Agente de SSM) instalada o una posterior
- Un bucket de S3 que no tiene habilitado el acceso público
- Una clave hdbuserstore llamada SYSTEM
- Un rol de IAM de AWS Identity and Access Management para que el manual de procedimientos se ejecute según lo programado
- Las políticas AmazonSSMManagedInstanceCore y ssm:StartAutomationExecution están asociadas al rol de servicio de automatización de Systems Manager.

Limitaciones

- AWS Backint Agent para SAP HANA no admite la deduplicación.
- AWS Backint Agent para SAP HANA no admite la compresión de datos.

Versiones de producto

AWS Backint Agent es compatible con los siguientes sistemas operativos:

- SUSE Linux Enterprise Server
- SUSE Linux Enterprise Server para SAP
- Red Hat Enterprise Linux para SAP

AWS Backint Agent es compatible con las siguientes bases de datos:

- SAP HANA 1.0 SP12 (nodo único y varios nodos)
- SAP HANA 2.0 y versiones posteriores (nodo único y varios nodos)

Arquitectura

Pila de tecnología de destino

- AWS Backint Agent

- Amazon S3
- AWS Systems Manager
- Amazon EventBridge
- SAP HANA

Arquitectura de destino

El siguiente diagrama muestra los scripts de instalación que instalan AWS Backint Agent, el bucket S3 y Systems Manager EventBridge, y que utilizan un documento de comandos para programar copias de seguridad periódicas.

Automatizar y escalar

- Se pueden instalar varios AWS Backint Agents mediante un manual de procedimientos de Systems Manager Automation.
- Cada ejecución del manual de procedimientos de Systems Manager puede escalarse hasta un número n de instancias de SAP HANA, en función de la selección de objetivos.
- EventBridge puede automatizar las copias de seguridad de SAP HANA.

Herramientas

- AWS Backint Agent para SAP HANA es una aplicación independiente que se integra con sus flujos de trabajo existentes para hacer copias de seguridad de la base de datos de SAP HANA en un bucket de S3 que especifique en el archivo de configuración. AWS Backint Agent admite copias de seguridad completas, incrementales y diferenciales de bases de datos de SAP HANA. Se ejecuta en un servidor de bases de datos SAP HANA, donde las copias de seguridad y los catálogos se transfieren de la base de datos de SAP HANA a AWS Backint Agent.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que puede utilizar para conectar sus aplicaciones con datos de diversas fuentes. EventBridge ofrece un flujo de datos en tiempo real desde sus aplicaciones, aplicaciones de software como servicio (SaaS) y servicios de AWS a objetivos como las funciones de AWS Lambda, los puntos de enlace de invocación HTTP que utilizan destinos de API o los buses de eventos de otras cuentas.

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos. Puede utilizar Amazon S3 para almacenar y recuperar cualquier cantidad de datos en cualquier momento y desde cualquier parte de la web.
- AWS Systems Manager le ayuda a ver y controlar la infraestructura en AWS. Mediante la consola de Systems Manager, puede ver los datos operativos de varios servicios de AWS y automatizar las tareas operativas en sus recursos de AWS.

Código

El código de este patrón está disponible en el repositorio. aws-backint-automated-backup GitHub

Epics

Cree un SISTEMA de claves hdbuserstore

Tarea	Descripción	Habilidades requeridas
Cree una clave hdbuserstore.	1. Vaya a `/usr/sap/<SID>/HDB<InstNo>/exe`. 2. Ejecute el siguiente comando, con XX como número instancia de la base de datos SAP HANA. `hdbuserstore -i set SYSTEM <hostname>:3XX13@SYSTEMDB SYSTEM` Por ejemplo, para un host de SAP HANA `saphanadb` con número de instancia `00`, ejecute el siguiente comando. `hdbuserstore -i set SYSTEM saphanadb`	Administrador de AWS, administrador de SAP HANA

Tarea	Descripción	Habilidades requeridas
	`:30013@SYSTEMDB SYSTEM`	

Instalación de AWS Backint Agent

Tarea	Descripción	Habilidades requeridas
Instalación de AWS Backint Agent.	Siga las instrucciones de Instalación y configuración de AWS Backint Agent para SAP HANA en la documentación de AWS Backint Agent.	Administrador de AWS, administrador de SAP HANA

Cree un documento de comandos de Systems Manager

Tarea	Descripción	Habilidades requeridas
Cree un documento de comandos de Systems Manager.	1. Inicie sesión en la consola de administración de AWS y abra la consola de AWS Systems Manager. 2. Seleccione Documents (Documentos) y seleccione Owned by me (De mi propiedad). 3. Confirme que se encuentra en la misma región de AWS que su base de datos de SAP HANA. 4. Seleccione Create document (Crear documento), Command or session (Comando	Administrador de AWS, administrador de SAP HANA

Tarea	Descripción	Habilidades requeridas
	o sesión) para crear su documento. 5. Utilice un nombre único y descriptivo, sin espacios (por ejemplo, SAP HANA-Backup). 6. Asegúrese de que el Document type (Tipo de documento) esté configura do como Command document (Documento de comando). 7. En el encabezado de Content (Contenido), hay un código de ejemplo. Asegúrese de elegir el tipo de código JSON y sustituya el código por el código del `HDB_Backup_SSM_Doc ument.json` archivo del GitHub repositorio. 8. Elija Create document (Crear documento). 9. Consulte su documento en la sección De mi propiedad.	

Programe las copias de seguridad con una frecuencia periódica

Tarea	Descripción	Habilidades requeridas
Programa copias de seguridad periódicas con Amazon EventBridge.	1. Abre la EventBridge consola de Amazon,	Administrador de AWS, administrador de SAP HANA

Tarea	Descripción	Habilidades requeridas
	selecciona Reglas y selecciona Crear regla. 2. En la pantalla Define rule detail (Definir detalles de la regla), introduzca un nombre y una descripci ón únicos para la regla y utilice el bus de eventos predeterminado. 3. En Rule type (Tipo de regla), seleccione Schedule (Programar) y, a continuac ión, Next (Siguiente). 4. En la pantalla Define schedule (Definir programación), elija el patrón de programación apropiado y la expresión cron o expresión de frecuencia en función de la frecuencia requerida. 5. En la pantalla Select targets (Seleccionar destinos), en Target type (Tipo de destino), elija AWS service (Servicio de AWS). En Select a target (Seleccione un destino), elija Systems Manager Run Command. 6. Elija el documento que creó anteriormente. 7. En Target key (Clave de destino) y Target value (Valor objetivo), proporcio	

Tarea	Descripción	Habilidades requeridas
	ne el ID de la instancia. Puede utilizar nombres y valores de etiquetas para agregar varias instancias. 8. En Configure automation parameters (Configurar los parámetros de automatiz ación), seleccione Constant (Constante) para las copias de seguridad incrementales o diferenciales. Si desea una copia de seguridad completa, seleccione No Parameters (Sin parámetro s). 9. Elija si desea crear una nueva función o utilizar una función existente. Si utiliza un rol existente, asegúrese de que tenga las políticas necesarias para invocar el objetivo. 10. Conserve la configuración adicional predeterminada y seleccione Next (Siguiente). 11. La pantalla Configure tags (Configurar etiquetas) es opcional. Elija Next (Siguiente). 12. En la pantalla Review and create (Revisar y crear), revise la configuración de la regla y seleccione Create	

Tarea	Descripción	Habilidades requeridas
	(Crear). La regla debe crearse correctamente. Puede verificar el éxito de la copia de seguridad desde la ruta del bucket de S3. `s3:/<your_bucket_name>/<target folder>/<SID>/usr/sap/<SID>/SYS/global/hdb/backint/DB_<SID>/` También puede verificar las copias de seguridad desde el catálogo de copias de seguridad de SAP HANA.	

Recursos relacionados

- AWS Backint Agent para SAP HANA
- Instalación y configuración de AWS Backint Agent para SAP HANA

Bloquee el acceso público a Amazon RDS mediante Cloud Custodian

Creado por abhay kumar (AWS) y Dwarika Patra (AWS)

Entorno: Producción	Tecnologías: bases de datos, seguridad, identidad, cumplimiento	Carga de trabajo: todas las demás cargas de trabajo; código abierto
Servicios de AWS: Amazon RDS		

Resumen

Muchas organizaciones ejecutan sus cargas de trabajo y servicios en múltiples proveedores de nube. En estos entornos de nube híbrida, la infraestructura de nube necesita un gobierno estricto, además de la seguridad proporcionada por los proveedores de nube individuales. Una base de datos en la nube, como Amazon Relational Database Service (Amazon RDS), es un servicio importante que debe supervisarse para detectar cualquier vulnerabilidad de acceso y permisos. Si bien puede restringir el acceso a la base de datos de Amazon RDS configurando un grupo de seguridad, también puede añadir un segundo nivel de protección para prohibir acciones como el acceso público. Garantizar el bloqueo del acceso público le ayudará a cumplir con el Reglamento General de Protección de Datos (RGPD), la Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA), el Instituto Nacional de Estándares y Tecnología (NIST) y el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS).

Cloud Custodian es un motor de reglas de código abierto que puede usar para imponer restricciones de acceso a los recursos de Amazon Web Services (AWS), como Amazon RDS. Cloud Custodian le permite establecer reglas que validen el entorno según los estándares de seguridad y conformidad definidos. Puede usar Cloud Custodian para administrar sus entornos de nube y así garantizar el cumplimiento de las políticas de seguridad, las políticas de etiquetado, la recopilación de elementos no utilizados y la administración de costos. Con Cloud Custodian puede usar una única interfaz para implementar la gobernanza en su entorno de nube híbrida. Por ejemplo, puede usar la interfaz de Cloud Custodian para interactuar con AWS y Microsoft Azure, lo que reduce el esfuerzo de trabajar con mecanismos como AWS Config, los grupos de seguridad de AWS y las políticas de Azure.

Este patrón proporciona instrucciones para usar Cloud Custodian en AWS e imponer restricciones de accesibilidad pública en las instancias de Amazon RDS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un par de claves
- AWS Lambda instalado

Arquitectura

Pila de tecnología de destino

- Amazon RDS
- AWS CloudTrail
- AWS Lambda
- Cloud Custodian

Arquitectura de destino

En el siguiente diagrama, se muestra a Cloud Custodian implementando la política en Lambda, CloudTrail AWS iniciando `CreateDBInstance` el evento y `PubliclyAccessible` configurando la función Lambda en false en Amazon RDS.

Herramientas

Servicios de AWS

- AWS le CloudTrail ayuda a auditar la gobernanza, el cumplimiento y el riesgo operativo de su cuenta de AWS.
- La Interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que permite interactuar con los servicios de AWS mediante comandos en el intérprete de comandos de línea de comandos.

- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Relational Database Service (Amazon RDS) le ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS.

Otras herramientas

- Cloud Custodian unifica las herramientas y scripts que emplean muchas organizaciones para administrar sus cuentas de nube pública en una sola herramienta de código abierto. Emplea un motor de reglas sin estado para la definición y aplicación de las políticas con métricas, resultados estructurados e informes detallados de la infraestructura de la nube. Se integra perfectamente con tiempos de ejecución sin servidor para proporcionar soluciones y respuestas en tiempo real con una baja sobrecarga operativa.

Epics

Configurar AWS CLI.

Tarea	Descripción	Habilidades requeridas
Instalar AWS CLI.	Para instalar la CLI de AWS, siga las instrucciones de la documentación de AWS.	Administrador de AWS
Configuración de credenciales de AWS	Configure los ajustes que permiten a la CLI de AWS interactuar con AWS, incluida la región de AWS y el formato de salida que desee usar. `$>aws configure`	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	`AWS Access Key ID [None]: <your_access_key_id>` `AWS Secret Access Key [None]: <your_secret_access_key>` `Default region name [None]:` `Default output format [None]:` Para obtener más información, consulte la documentación de AWS.	
Crear un rol de IAM.	Para crear un rol de IAM con el rol de ejecución de Lambda, ejecute el siguiente comando. `aws iam create-role --role-name lambda-ex --assume-role-policy-document '{"Version": "2012-10-17","Statement": [{ "Effect": "Allow", "Principal": {"Service": "lambda.amazonaws.com"}, "Action": "sts:AssumeRole"}]}`	AWS DevOps

Configure Cloud Custodian

Tarea	Descripción	Habilidades requeridas
Instale Cloud Custodian.	Para instalar Cloud Custodian en su sistema operativo y	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	entorno, siga las instrucciones de la documentación de Cloud Custodian.	
Consulte el esquema de Cloud Custodian.	Para ver una lista completa de los recursos de Amazon RDS con los que puede ejecutar políticas, introduzca el siguiente comando. `custodian schema aws.rds`	DevOps ingeniero
Cree la política de Cloud Custodian.	Guarda el código que se encuentra en el archivo de políticas de Cloud Custodian en la sección de Información adicional con una extensión YAML.	DevOps ingeniero
Defina las acciones de Cloud Custodian para cambiar el indicador de acceso público.	1. Localice el código de Custodian (por ejemplo, `/Users/abcd/custodian/lib/python3.9/site-packages/c7n/resources/rds.py`). 2. Localice la clase `RDSSetPublicAvailability` en `rds.py` y modifíquela introduciendo el código que se encuentra en el archivo rds.py de recursos de c7n, en la sección de Información adicional.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Ejecute una prueba.	(Opcional) Para comprobar qué recursos identifica la política sin ejecutar ninguna acción en ellos, emplee el siguiente comando. `custodian run -dryrun <policy_name>.yaml -s <output_directory>`	DevOps ingeniero

Implemente la política

Tarea	Descripción	Habilidades requeridas
Implemente la política mediante Lambda.	Para crear la función de Lambda que ejecutará la política, introduzca el siguiente comando. `custodian run -s policy.yaml` A continuación, el CloudTrail `CreateDBInstance` evento de AWS iniciará esta política. De este modo, AWS Lambda establecerá el indicador de acceso público como false en aquellas instancias que cumplan los criterios.	DevOps ingeniero

Recursos relacionados

- AWS Lambda
- Amazon RDS
- Cloud Custodian

Información adicional

Archivo YAML de política de Cloud Custodian

```
policies:
  - name: "block-public-access"
    resource: rds
    description: |
      This Enforcement blocks public access for RDS instances.
    mode:
      type: cloudtrail
      events:
        - event: CreateDBInstance # Create RDS instance cloudtrail event
          source: rds.amazonaws.com
          ids: requestParameters.dBInstanceIdentifier
      role: arn:aws:iam::1234567890:role/Custodian-compliance-role
    filters:
      - type: event
        key: 'detail.requestParameters.publiclyAccessible'
        value: true
    actions:
      - type: set-public-access
        state: false
```

Archivo rds.py de recursos de c7n

```
@actions.register('set-public-access')
 class RDSSetPublicAvailability(BaseAction):

     schema = type_schema(
         "set-public-access",
         state={'type': 'boolean'})
     permissions = ('rds:ModifyDBInstance',)

     def set_accessibility(self, r):
```

```
        client = local_session(self.manager.session_factory).client('rds')
        waiter = client.get_waiter('db_instance_available')
        waiter.wait(DBInstanceIdentifier=r['DBInstanceIdentifier'])
        client.modify_db_instance(
            DBInstanceIdentifier=r['DBInstanceIdentifier'],
            PubliclyAccessible=self.data.get('state', False))


    def process(self, rds):
        with self.executor_factory(max_workers=2) as w:
            futures = {w.submit(self.set_accessibility, r): r for r in rds}
            for f in as_completed(futures):
                if f.exception():
                    self.log.error(
                        "Exception setting public access on %s  \n %s",
                        futures[f]['DBInstanceIdentifier'], f.exception())
        return rds
```

Integración de Security Hub

Cloud Custodian se puede integrar con AWS Security Hub para enviar resultados de seguridad y tratar de adoptar medidas correctivas. Para obtener más información, consulte Anuncio de la integración de Cloud Custodian con AWS Security Hub.

Configure el enrutamiento de solo lectura en un grupo de disponibilidad Always On en SQL Server en AWS

Creado por Subhani Shaik (AWS)

Entorno: PoC o piloto	Tecnologías: bases de datos; infraestructura	Carga de trabajo: Microsoft
Servicios de AWS: AWS Managed Microsoft AD; Amazon EC2		

Resumen

Este patrón explica cómo usar la réplica secundaria en espera en SQL Server Always On descargando las cargas de trabajo de solo lectura de la réplica principal a la réplica secundaria.

La duplicación de bases de datos tiene one-to-one mapeo. No puede leer la base de datos secundaria directamente, por lo que debe crear instantáneas. La característica de grupo de disponibilidad Always On se introdujo en Microsoft SQL Server 2012. En versiones posteriores se han introducido importantes funcionalidades, incluido el enrutamiento de solo lectura. En los grupos de disponibilidad de Always On, puede leer los datos directamente desde la réplica secundaria cambiando el modo de réplica a uno de solo lectura.

La solución de grupos de disponibilidad Always On ofrece alta disponibilidad (HA), recuperación de desastres (DR) y una alternativa a la duplicación de bases de datos. Los grupos de disponibilidad Always On funcionan a nivel de base de datos, y maximizan la disponibilidad de un conjunto de bases de datos de usuarios.

SQL Server emplea el mecanismo de enrutamiento de solo lectura para redirigir las conexiones entrantes de solo lectura a la réplica de lectura secundaria. Para ello, debe agregar los siguientes parámetros y valores en la cadena de conexión:

- `ApplicationIntent=ReadOnly`
- `Initial Catalog=<database name>`

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa con una nube privada virtual (VPC), dos zonas de disponibilidad, subredes privadas y un grupo de seguridad
- Dos máquinas Amazon Elastic Compute Cloud (Amazon EC2) con imágenes de máquina de Amazon SQL Server 2019 Enterprise Edition, clústeres de conmutación por error de Windows Server (WSFC) configurados a nivel de instancia y un grupo de disponibilidad Always On configurado a nivel de SQL Server entre el nodo principal (`WSFCNODE1`) y el nodo secundario (`WSFCNODE2`), que forman parte del directorio de AWS Directory Service para Microsoft Active Directory denominado `tagechtalk.com`
- Uno o más nodos configurados para aceptar `read-only` en la réplica secundaria
- Un oyente con el nombre `SQLAG1` para el grupo de disponibilidad Always On
- SQL Server Database Engine en ejecución con la misma cuenta de servicio en dos nodos
- SQL Server Management Studio (SSMS)
- Una base de datos de prueba llamada `test`

Versiones de producto

- SQL Server 2014 y versiones posteriores

Arquitectura

Pila de tecnología de destino

- Amazon EC2
- AWS Managed Microsoft AD
- Amazon FSx

Arquitectura de destino

El siguiente diagrama muestra cómo el oyente del grupo de disponibilidad (AG) Always On redirige las consultas que contienen el parámetro `ApplicationIntent` en la conexión al nodo secundario correspondiente.

1. Se envía una solicitud al oyente del grupo de disponibilidad Always On.
2. Si la cadena de conexión no tiene el parámetro `ApplicationIntent`, la solicitud se envía a la instancia principal.
3. Si la cadena de conexión contiene `ApplicationIntent=ReadOnly`, la solicitud se envía a la instancia secundaria con una configuración de enrutamiento de solo lectura. Con un grupo de disponibilidad Always On, es WSFC.

Herramientas

Servicios de AWS

- AWS Directory Service para Microsoft Active Directory permite que las cargas de trabajo compatibles con un directorio y los recursos de AWS utilicen Active Directory de Microsoft administrado en la nube de AWS.
- Amazon Elastic Compute Cloud (Amazon EC2) brinda capacidad de computación escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon FSx proporciona sistemas de archivos que admiten los protocolos de conectividad estándares del sector y ofrecen alta disponibilidad y replicación en todas las regiones de AWS.

Otros servicios

- SQL Server Management Studio (SSMS) es una herramienta para conectar, gestionar y administrar instancias de SQL Server.
- sqlcmd es una utilidad de línea de comandos.

Prácticas recomendadas

Para obtener más información sobre los grupos de disponibilidad Always On, consulte la documentación de SQL Server.

Epics

Configure el enrutamiento de solo lectura

Tarea	Descripción	Habilidades requeridas
Actualice las réplicas a solo lectura.	Para actualizar la réplica principal y la secundaria a solo lectura, conéctese a la réplica principal desde SSMS y ejecute el código del Paso 1 que encontrará en la sección de Información adicional.	Administrador de base de datos
Cree la URL de enrutamiento.	Para crear la URL de enrutamiento para ambas réplicas, ejecute el código del Paso 2 que encontrará en la sección de Informaci ón adicional. En este código, `tagechtalk.com` es el nombre del directorio de AWS Managed Microsoft AD.	Administrador de base de datos
Cree la lista de enrutamiento.	Para crear la lista de enrutamiento para ambas réplicas, ejecute el código del Paso 3 que encontrará en la sección de Información adicional.	Administrador de base de datos
Valide la lista de enrutamiento.	Conéctese a la instancia principal desde SQL Server Management Studio y ejecute el código del Paso 4 que encontrará en la sección de Información adicional para	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	validar la lista de enrutamie nto.	

Pruebe el enrutamiento de solo lectura

Tarea	Descripción	Habilidades requeridas
Connect mediante el Applicati onIntent parámetro.	1. Desde SSMS, conéctese al nombre de oyente del grupo de disponibilidad Always On con `Applicati onIntent=ReadOnly; Initial Catalog=t est` . 2. Se establecerá una conexión con la réplica secundaria. Para realizar la prueba, ejecute el siguiente comando para mostrar el nombre del servidor conectado. `SELECT SERVERPRO PERTY('Computernam ePhysicalNetBios')` El resultado devolverá el nombre de la réplica secundaria actual (`WSFCN0DE2`).	Administrador de base de datos
Realice una conmutación por error.	1. Desde SSMS, conéctese al nombre de oyente del grupo de disponibilidad Always On.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	2. Compruebe que las bases de datos principal y secundaria estén sincronizadas y que no se pierdan datos. 3. Realice una conmutación por error para que la réplica principal actual pase a ser la réplica secundaria, y la réplica secundaria pase a ser la réplica principal. 4. Desde SSMS, conéctese al nombre de oyente del grupo de disponibilidad Always On con `ApplicationIntent=ReadOnly; Initial Catalog=test` . 5. Se establecerá una conexión con la réplica secundaria. Para realizar la prueba, ejecute el siguiente comando para mostrar el nombre del servidor conectado. `SELECT SERVERPROPERTY('ComputerNamePhysicalNetBios')` Se mostrará el nombre de la réplica secundaria actual (`WSFCNODE1`).	

Conéctese mediante la utilidad de línea de comandos sqlcmd

Tarea	Descripción	Habilidades requeridas
Conéctese mediante sqlcmd.	Para conectarse desde sqlcmd, ejecute el código del Paso 5 que encontrará en la sección de Informaci ón adicional en la línea de comandos. Después de conectarse, ejecute el siguiente comando para mostrar el nombre del servidor conectado. `SELECT SERVERPRO PERTY('Computernam ePhysicalNetBios') .` El resultado devolverá el nombre de la réplica secundari a actual (`WSFCNODE1`).	Administrador de base de datos

Solución de problemas

Problema	Solución
No se puede crear el oyente y aparece el mensaje “El clúster WSFC no ha podido poner en línea el recurso Nombre de red”.	Para mayor información, consulte el blog de Microsoft La creación del oyente dio el mensaje de error: “el clúster WSFC no ha podido poner en línea el recurso Nombre de red”.
Posibles problemas, incluidos otros problemas con los oyentes o problemas de acceso a la red.	Consulte Solución de problemas de configura ción de grupos de disponibilidad Always On (SQL Server) en la documentación de Microsoft .

Recursos relacionados

- Configure el enrutamiento de solo lectura en un grupo de disponibilidad Always On
- Consulte Solución de problemas de configuración de grupos de disponibilidad Always On (SQL Server)

Información adicional

Paso 1. Actualice las réplicas a solo lectura

```
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE1' WITH (SECONDARY_ROLE
 (ALLOW_CONNECTIONS = READ_ONLY))
GO
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE2' WITH (SECONDARY_ROLE
 (ALLOW_CONNECTIONS = READ_ONLY))
GO
```

Paso 2. Cree la URL de enrutamiento

```
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE1' WITH (SECONDARY_ROLE
 (READ_ONLY_ROUTING_URL = N'TCP://WSFCNode1.tagechtalk.com:1433'))
GO
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE2' WITH (SECONDARY_ROLE
 (READ_ONLY_ROUTING_URL = N'TCP://WSFCNode2.tagechtalk.com:1433'))
GO
```

Paso 3. Cree la URL de enrutamiento

```
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE1' WITH
 (PRIMARY_ROLE(READ_ONLY_ROUTING_LIST=('WSFCNODE2','WSFCNODE1')));
GO
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE2' WITH (PRIMARY_ROLE
 (READ_ONLY_ROUTING_LIST=('WSFCNODE1','WSFCNODE2')));
GO
```

Paso 4. Cree la lista de enrutamiento

```
SELECT AGSrc.replica_server_name AS PrimaryReplica, AGRepl.replica_server_name AS
 ReadOnlyReplica, AGRepl.read_only_routing_url AS RoutingURL , AGRL.routing_priority
```

```
AS RoutingPriority FROM sys.availability_read_only_routing_lists AGRL INNER JOIN
sys.availability_replicas AGSrc ON AGRL.replica_id = AGSrc.replica_id INNER JOIN
sys.availability_replicas AGRepl ON AGRL.read_only_replica_id = AGRepl.replica_id
INNER JOIN sys.availability_groups AV ON AV.group_id = AGSrc.group_id ORDER BY
PrimaryReplica
```

Paso 5. Utilidad de comandos SQL

```
sqlcmd -S SQLAG1,1433 -E -d test -K ReadOnly
```

Conectar mediante un túnel SSH en pgAdmin

Creado por Jeevan Shetty (AWS) y Bhanu Ganesh Gudivada (AWS)

Entorno: producción	Tecnologías: bases de datos; seguridad, identidad, conformidad	Carga de trabajo: código abierto
Servicios de AWS: Amazon RDS; Amazon Aurora		

Resumen

Por motivos de seguridad, siempre es bueno colocar las bases de datos en una subred privada. Las consultas en la base de datos se pueden ejecutar mediante conexión a través de un host bastión de Amazon Elastic Compute Cloud (Amazon EC2) en una subred pública de la nube de Amazon Web Services (AWS). Esto requiere la instalación de software, como pgAdmin o DBeaver, que suelen utilizar los desarrolladores o administradores de bases de datos, en el host Amazon EC2.

Ejecutar pgAdmin en un servidor Linux y acceder a él a través de un navegador web requiere la instalación de dependencias adicionales y la configuración de permisos.

Como solución alternativa, los desarrolladores o administradores de bases de datos pueden conectarse a una base de datos PostgreSQL mediante pgAdmin para habilitar un túnel SSH desde su sistema local. En este enfoque, pgAdmin utiliza el host Amazon EC2 de la subred pública como host intermediario antes de conectarse a la base de datos. El diagrama de la sección de arquitectura muestra la configuración.

Nota: Asegúrese de que el grupo de seguridad adjunto a la base de datos PostgreSQL permita la conexión en el puerto 5432 desde el host de Amazon EC2.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS existente
- Una nube privada virtual (VPC) con una subred pública y una subred privada

- Instancia EC2 con un grupo de seguridad adjunto
- Base de datos de la edición compatible con Amazon Aurora PostgreSQL con un grupo de seguridad adjunto
- Un par de claves Secure Shell (SSH) para configurar el túnel

Versiones de producto

- pgAdmin versión 6.2+
- Amazon Aurora, edición compatible con PostgreSQL, versión 12.7+

Arquitectura

Pila de tecnología de destino

- Amazon EC2
- Amazon Aurora compatible con PostgreSQL

Arquitectura de destino

El siguiente diagrama muestra el uso de pgAdmin con un túnel SSH para conectarse a través de una puerta de enlace de Internet a la instancia EC2, que se conecta a la base de datos.

Herramientas

Servicios de AWS

- La edición de Amazon Aurora compatible con PostgreSQL es un motor de base de datos relacional compatible con ACID, completamente administrado que le permite configurar, utilizar y escalar implementaciones de PostgreSQL.
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.

Otros servicios

- pgAdmin es una herramienta de gestión de código abierto para PostgreSQL. Proporciona una interfaz gráfica que permite crear, mantener y utilizar objetos de bases de datos.

Epics

Creación de la conexión

Tarea	Descripción	Habilidades requeridas
Cree un servidor.	En pgAdmin, seleccione Crear y, a continuación, Servidor. Para obtener ayuda adicional sobre la configuración de pgAdmin para registrar un servidor, configurar una conexión y conectarse a través de un túnel SSH mediante el cuadro de diálogo del servidor, consulte los enlaces de la sección Recursos relaciona dos.	Administrador de base de datos
Proporcione un nombre para el servidor.	En la pestaña General, introduzca un nombre.	Administrador de base de datos
Ingrese los detalles de base de datos.	En la pestaña Conexión, introduzca los valores siguientes: • Nombre/dirección del host • Puerto • Mantenimiento de bases de datos • Nombre de usuario • Contraseña	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Introduzca los detalles del servidor Amazon EC2.	En la pestaña Túnel SSH, proporcione los detalles de la instancia de Amazon EC2 que se encuentra en la subred pública. • Establezca Usar túnel SSH en Sí para especificar que pgAdmin debe usar un túnel SSH al conectarse al servidor especificado. • En el campo Host del túnel, especifique el nombre o la dirección IP del host SSH (por ejemplo, 10.x.x.x). • En el campo Puerto del túnel, especifique el puerto del host SSH (por ejemplo, 22). • En el campo Nombre de usuario, introuzca el nombre de un usuario con privilegi os de inicio de sesión en el host SSH (por ejemplo, ec2-user). • Especifique el tipo de autenticación como archivo de identidad para que PGAdmin utilice un archivo de clave privada al conectarse. • Incluya la ubicación del archivo Privacy Enhanced Mail (PEM) en el campo	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	del archivo de identidad. El archivo.pem es el par de claves de Amazon EC2.	
Guardar y conectar.	Seleccione Guardar para completar la configuración y conectarse a la base de datos Aurora compatible con PostgreSQL mediante el túnel SSH.	Administrador de base de datos

Recursos relacionados

- Diálogo del servidor
- Conectar al servidor

Convertir consultas JSON de Oracle en SQL de bases de datos PostgreSQL

Documento creado por Pinesh Singal (AWS) y Lokesh Gurram (AWS)

Entorno: PoC o piloto	Origen: bases de datos: relacionales	Destino: Amazon RDS PostgreSQL
Tipo R: renovar arquitectura	Carga de trabajo: Oracle	Tecnologías: bases de datos; migración
Servicios de AWS: Amazon Aurora; Amazon RDS		

Resumen

Este proceso de migración para pasar del entorno local a la nube de Amazon Web Services (AWS) utiliza la herramienta de conversión de esquemas de AWS (AWS SCT) para convertir el código de una base de datos Orqacle en una base de datos PostgreSQL. AWS SCT convierte automáticamente la mayor parte del código. Sin embargo, las consultas de Oracle relacionadas con JSON no se convierten automáticamente.

A partir de la versión 12.2 de Oracle, Oracle Database admite varias funciones de JSON que ayudan a convertir los datos basados en JSON en datos basados en filas. Sin embargo, AWS SCT no convierte automáticamente los datos basados en JSON a un lenguaje compatible con PostgreSQL.

Este patrón de migración se centra principalmente en convertir manualmente las consultas de Oracle relacionadas con JSON con funciones como `JSON_OBJECT`, `JSON_ARRAYAGG`, y `JSON_TABLE` de una base de datos Oracle a una base de datos PostgreSQL.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una instancia de base de datos de Oracle local (en funcionamiento)

- Una instancia de base de datos de Amazon Relational Database Service (Amazon RDS) para la Edición compatible con PostgreSQL o Amazon Aurora

Limitaciones

- Las consultas relacionadas con JSON requieren un formato AND fijo `KEY` y `VALUE`. Si no se utiliza ese formato, se obtiene un resultado incorrecto.
- Si algún cambio en la estructura de JSON añade pares nuevos `KEY` y `VALUE`en la sección de resultados, se debe cambiar el procedimiento o la función correspondiente en la consulta SQL.
- Algunas funciones relacionadas con JSON se admiten en versiones anteriores de Oracle y PostgreSQL, pero con menos capacidades.

Versiones de producto

- Oracle Database, versión 12.2 y posterior
- Amazon RDS para PostgreSQL o Aurora, compatible con PostgreSQL, versión 9.5 y versiones posteriores
- Última versión de AWS SCT (probadas con la versión 1.0.664)

Arquitectura

Pila de tecnología de origen

- Una instancia de base de datos Oracle con la versión 19c

Pila de tecnología de destino

- Una instancia de base de datos compatible con Amazon RDS para PostgreSQL o Aurora PostgreSQL con la versión 13

Arquitectura de destino

1. Utilice AWS SCT con el código de función JSON para convertir el código fuente de Oracle a PostgreSQL.

2. La conversión produce archivos.sql migrados compatibles con PostgreSQL.
3. Convierta manualmente los códigos de función JSON de Oracle no convertidos en códigos de función JSON de PostgreSQL.
4. Ejecute los archivos.sql en la instancia de base de datos compatible con PostgreSQL de Aurora de destino.

Herramientas

Servicios de AWS

- Amazon Aurora es un motor de base de datos relacional que está diseñado para la nube y es compatible con MySQL y PostgreSQL.
- Amazon Relational Database Service (Amazon RDS) para PostgreSQL le ayuda a configurar, utilizar y escalar una base de datos relacional de PostgreSQL en la nube de AWS.
- La Herramienta de conversión de esquemas de AWS (AWS SCT) simplifica las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado, lo que incluye las vistas, los procedimientos almacenados y las funciones, a un formato compatible con la base de datos de destino.

Otros servicios

- Oracle SQL Developer es un entorno de desarrollo integrado que simplifica el desarrollo y la administración de bases de datos de Oracle, tanto en implementaciones tradicionales como en implementaciones basadas en la nube.
- pgAdmin o DBeaver. pgAdmin es una herramienta de gestión de código abierto para PostgreSQL. Proporciona una interfaz gráfica que permite crear, mantener y utilizar objetos de bases de datos. DBeaver es una herramienta de base de datos universal.

Prácticas recomendadas

La consulta de Oracle tiene el tipo `CAST` como valor predeterminado cuando se utiliza la función `JSON_TABLE`. Una buena práctica es utilizarla también `CAST` en PostgreSQL, utilizando caracteres dobles mayores que (>>).

Para obtener más información, consulte Postgres_SQL_read_JSON en la sección Información adicional.

Epics

Genere los datos JSON en las bases de datos Oracle y PostgreSQL

Tarea	Descripción	Habilidades requeridas
Guarde los datos JSON en la base de datos de Oracle.	Cree una tabla en la base de datos de Oracle y almacene los datos JSON en la columna `CLOB`. Utilice el Oracle_Table_Creation_Insert_Script que se encuentra en la sección Información adicional.	Ingeniero de migraciones
Guarde los datos JSON en la base de datos PostgreSQL.	Cree una tabla en la base de datos PostgreSQL y almacene los datos JSON en la columna `TEXT`. Utilice el archivo Postgres_Table_Creation_Insert_Script que se encuentra en la sección Información adicional.	Ingeniero de migraciones

Convierte el JSON al formato ROW

Tarea	Descripción	Habilidades requeridas
Convertir los datos JSON en la base de datos Oracle.	Escriba una consulta SQL de Oracle para leer los datos JSON en formato ROW. Para obtener más detalles y ejemplos de sintaxis, consulte Oracle_SQL_read_JSON en la sección Información adicional.	Ingeniero de migraciones
Convierta los datos JSON en la base de datos PostgreSQL.	Escriba una consulta de PostgreSQL para leer los	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	datos JSON en formato ROW. Para obtener más detalles y ejemplos de sintaxis, consulte Oracle_SQL_read_JSON en la sección Información adicional.	

Convertir manualmente los datos JSON mediante la consulta SQL e informe el resultado en formato JSON

Tarea	Descripción	Habilidades requeridas
Realizar agregaciones y validaciones en la consulta SQL de Oracle.	Para convertir manualmente los datos de JSON, realice una unión, agregación y validación en la consulta SQL de Oracle e informe el resultado en formato JSON. Utilice el código que aparece en Oracle_SQL_JSON_Aggregation_JOIN en la sección Información adicional. 1. JOIN: los datos con formato JSON se pasan como parámetro de entrada a la consulta. Se realiza una unión interna entre estos datos estáticos y los datos JSON de la tabla de base de datos de Oracle `aws_test_table` . 2. Agregación con validación: los datos JSON tienen `KEY VALUE`	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	parámetros con valores como `accountNumber`, `parentAccountNumber`, `businessUnitId` y `positionId`, que se utilizan para las agregaciones `SUM` y `COUNT`. 3. Formato JSON: después de la unión y la agregación, los datos se presentan en formato JSON mediante `JSON_OBJECT` y `JSON_ARRAYAGG`.	

Tarea	Descripción	Habilidades requeridas
Realice agregaciones y validaciones en la consulta SQL de Postgres.	Para convertir manualmente los datos de JSON, realice una unión, agregación y validación en la consulta de PostgreSQL e informe el resultado en formato JSON. Use el código que aparece en Postgres_SQL_JSON_AGGREGATION_JOIN en la sección Información adicional. 1. JOIN: los datos con formato JSON (`tab1`) se pasan como parámetro de entrada a la consulta de la cláusula `WITH`. Se realiza una unión entre estos datos estáticos y los datos JSON, que se encuentran en la tabla `tab`. También se hace una unión con la cláusula `WITH`, que contiene datos de JSON en la tabla `aws_test_pg_table` . 2. Agregación: los datos de JSON tienen parámetros `KEY` y `VALUE` con valores como `accountNumber` , `parentAccountNumber` , `businessUnitId` , y `positionId` , que se utilizan para las agregaciones `SUM` y `COUNT`.	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	3. Formato JSON: después de la unión y la agregación, los datos se presentan en formato JSON mediante `JSON_BUILD_OBJECT` y `JSON_AGG`.	

Convertir el procedimiento de Oracle en una función de PostgreSQL que contenga consultas JSON

Tarea	Descripción	Habilidades requeridas
Convierta las consultas JSON del procedimiento de Oracle en filas.	Para el procedimiento de Oracle de ejemplo, utilice la consulta de Oracle anterior y el código de Oracle_Procedure_with_JSON_Query en la sección Información adicional.	Ingeniero de migraciones
Convierta las funciones de PostgreSQL que tienen consultas JSON en datos basados en filas.	Para las funciones de PostgreSQL de ejemplo, utilice la consulta de PostgreSQL anterior y el código que se encuentra en Postgres_function_with_JSON_Query en la sección Información adicional.	Ingeniero de migraciones

Recursos relacionados

- Funciones JSON de Oracle
- Funciones JSON de PostgreSQL
- Ejemplos de funciones JSON de Oracle

- Ejemplos de funciones JSON de PostgreSQL
- Herramienta de conversión de esquemas de AWS

Información adicional

Para convertir el código JSON de la base de datos Oracle a la base de datos PostgreSQL, utilice los siguientes scripts en orden.

1. Oracle_Table_Creation_Insert_Script

```
create table aws_test_table(id number,created_on date default sysdate,modified_on
 date,json_doc clob);

REM INSERTING into EXPORT_TABLE
SET DEFINE OFF;
Insert into aws_test_table (ID,CREATED_ON,MODIFIED_ON,json_doc)
values (1,to_date('02-AUG-2022 12:30:14','DD-MON-YYYY HH24:MI:SS'),to_date('02-AUG-2022
 12:30:14','DD-MON-YYYY HH24:MI:SS'),TO_CLOB(q'[{
  "metadata" : {
    "upperLastNameFirstName" : "ABC XYZ",
    "upperEmailAddress" : "abc@gmail.com",
    "profileType" : "P"
  },
  "data" : {
    "onlineContactId" : "032323323",
    "displayName" : "Abc, Xyz",
    "firstName" : "Xyz",
    "lastName" : "Abc",
    "emailAddress" : "abc@gmail.com",
    "productRegistrationStatus" : "Not registered",
    "positionId" : "0100",
    "arrayPattern" : " -'",
    "a]')
|| TO_CLOB(q'[ccount" : {
      "companyId" : "SMGE",
      "businessUnitId" : 7,
      "accountNumber" : 42000,
      "parentAccountNumber" : 32000,
      "firstName" : "john",
      "lastName" : "doe",
      "street1" : "retOdertcaShr ",
      "city" : "new york",
```

```
      "postalcode" : "XY ABC",
      "country" : "United States"
    },
    "products" : [
      {
        "appUserGuid" : "i0acc4450000001823fbad478e2eab8a0",
        "id" : "0000000046",
]')
|| TO_CLOB(q'[        "name" : "ProView",
        "domain" : "EREADER",
        "registrationStatus" : false,
        "status" : "11"
      }
    ]
  }
}]'));
Insert into aws_test_table (ID,CREATED_ON,MODIFIED_ON,json_doc) values (2,to_date('02-
AUG-2022 12:30:14','DD-MON-YYYY HH24:MI:SS'),to_date('02-AUG-2022 12:30:14','DD-MON-
YYYY HH24:MI:SS'),TO_CLOB(q'[{
  "metadata" : {
    "upperLastNameFirstName" : "PQR XYZ",
    "upperEmailAddress" : "pqr@gmail.com",
    "profileType" : "P"
  },
  "data" : {
    "onlineContactId" : "54534343",
    "displayName" : "Xyz, pqr",
    "firstName" : "pqr",
    "lastName" : "Xyz",
    "emailAddress" : "pqr@gmail.com",
    "productRegistrationStatus" : "Not registered",
    "positionId" : "0090",
    "arrayPattern" : " -'",
    "account" : {
      "companyId" : "CARS",
      "busin]')
|| TO_CLOB(q'[essUnitId" : 6,
      "accountNumber" : 42001,
      "parentAccountNumber" : 32001,
      "firstName" : "terry",
      "lastName" : "whitlock",
      "street1" : "UO  123",
      "city" : "TOTORON",
      "region" : "NO",
```

```
      "postalcode" : "LKM 111",
      "country" : "Canada"
    },
    "products" : [
      {
        "appUserGuid" : "ia744d7790000016899f8cf3f417d6df6",
        "id" : "0000000014",
        "name" : "ProView eLooseleaf",
      ]')
|| TO_CLOB(q'[  "domain" : "EREADER",
        "registrationStatus" : false,
        "status" : "11"
      }
    ]
  }
}]'));

commit;
```

2. Postgres_Table_Creation_Insert_Script

```
create table aws_test_pg_table(id int,created_on date ,modified_on date,json_doc text);
insert into aws_test_pg_table(id,created_on,modified_on,json_doc)
values(1,now(),now(),'{
  "metadata" : {
    "upperLastNameFirstName" : "ABC XYZ",
    "upperEmailAddress" : "abc@gmail.com",
    "profileType" : "P"
  },
  "data" : {
    "onlineContactId" : "032323323",
    "displayName" : "Abc, Xyz",
    "firstName" : "Xyz",
    "lastName" : "Abc",
    "emailAddress" : "abc@gmail.com",
    "productRegistrationStatus" : "Not registered",
    "positionId" : "0100",
    "arrayPattern" : " -",
    "account" : {
      "companyId" : "SMGE",
      "businessUnitId" : 7,
      "accountNumber" : 42000,
      "parentAccountNumber" : 32000,
```

```
      "firstName" : "john",
      "lastName" : "doe",
      "street1" : "retOdertcaShr ",
      "city" : "new york",
      "postalcode" : "XY ABC",
      "country" : "United States"
    },
    "products" : [
      {
        "appUserGuid" : "i0acc4450000001823fbad478e2eab8a0",
        "id" : "0000000046",
        "name" : "ProView",
        "domain" : "EREADER",
        "registrationStatus" : false,
        "status" : "11"
      }
    ]
  }
}');


insert into aws_test_pg_table(id,created_on,modified_on,json_doc)
values(2,now(),now(),'{
  "metadata" : {
    "upperLastNameFirstName" : "PQR XYZ",
    "upperEmailAddress" : "pqr@gmail.com",
    "profileType" : "P"
  },
  "data" : {
    "onlineContactId" : "54534343",
    "displayName" : "Xyz, pqr",
    "firstName" : "pqr",
    "lastName" : "Xyz",
    "emailAddress" : "a*b**@h**.k**",
    "productRegistrationStatus" : "Not registered",
    "positionId" : "0090",
    "arrayPattern" : " -",
    "account" : {
      "companyId" : "CARS",
      "businessUnitId" : 6,
      "accountNumber" : 42001,
      "parentAccountNumber" : 32001,
      "firstName" : "terry",
      "lastName" : "whitlock",
```

```
      "street1" : "UO  123",
      "city" : "TOTORON",
      "region" : "NO",
      "postalcode" : "LKM 111",
      "country" : "Canada"
    },
    "products" : [
      {
        "appUserGuid" : "ia744d7790000016899f8cf3f417d6df6",
        "id" : "0000000014",
        "name" : "ProView eLooseleaf",
        "domain" : "EREADER",
        "registrationStatus" : false,
        "status" : "11"
      }
    ]
  }
}');
```

3. Oracle_SQL_READ_JSON

Los siguientes bloques de código muestran cómo convertir los datos JSON de Oracle a formato de fila.

Ejemplo de consulta y sintaxis

```
SELECT   JSON_OBJECT(
 'accountCounts' VALUE JSON_ARRAYAGG(
            JSON_OBJECT(
                'businessUnitId' VALUE business_unit_id,
                        'parentAccountNumber' VALUE parent_account_number,
                        'accountNumber' VALUE account_number,
                        'totalOnlineContactsCount' VALUE online_contacts_count,
                        'countByPosition' VALUE
                    JSON_OBJECT(
                        'taxProfessionalCount' VALUE tax_count,
                        'attorneyCount' VALUE attorney_count,
                        'nonAttorneyCount' VALUE non_attorney_count,
                        'clerkCount' VALUE clerk_count
                                ) ) ) ) FROM
    (SELECT   tab_data.business_unit_id,
            tab_data.parent_account_number,
            tab_data.account_number,
```

```
           SUM(1) online_contacts_count,
           SUM(CASE WHEN tab_data.position_id = '0095' THEN  1 ELSE 0 END) tax_count,
           SUM(CASE    WHEN tab_data.position_id = '0100' THEN 1 ELSE 0 END)
attorney_count,
           SUM(CASE    WHEN tab_data.position_id = '0090' THEN 1 ELSE 0 END)
non_attorney_count,
           SUM(CASE    WHEN tab_data.position_id = '0050' THEN 1 ELSE 0 END)
clerk_count
       FROM aws_test_table scco,JSON_TABLE ( json_doc, '$' ERROR ON ERROR
 COLUMNS (
         parent_account_number NUMBER PATH
          '$.data.account.parentAccountNumber',
           account_number NUMBER PATH '$.data.account.accountNumber',
           business_unit_id NUMBER PATH '$.data.account.businessUnitId',
           position_id VARCHAR2 ( 4 ) PATH '$.data.positionId'    )
           ) AS tab_data
           INNER JOIN JSON_TABLE ( '{
       "accounts": [{
         "accountNumber": 42000,
         "parentAccountNumber": 32000,
         "businessUnitId": 7
       }, {
         "accountNumber": 42001,
         "parentAccountNumber": 32001,
         "businessUnitId": 6
       }]
     }', '$.accounts[*]' ERROR ON ERROR
     COLUMNS (
     parent_account_number PATH '$.parentAccountNumber',
     account_number PATH '$.accountNumber',
     business_unit_id PATH '$.businessUnitId')
     ) static_data
     ON ( static_data.parent_account_number = tab_data.parent_account_number
          AND static_data.account_number = tab_data.account_number
          AND static_data.business_unit_id = tab_data.business_unit_id )
       GROUP BY
           tab_data.business_unit_id,
           tab_data.parent_account_number,
           tab_data.account_number );
```

El documento JSON almacena los datos como colecciones. Cada colección puede tener pares KEY y VALUE. Cada VALUE puede tener anidados pares KEY y VALUE. En la siguiente tabla se proporciona información sobre la lectura del VALUE específico del documento JSON.

KEY	HIERARCHY or PATH to be used to get the VALUE	VALUE
`profileType`	`metadata` -> `profileType`	«P»
`positionId`	`data` -> `positionId`	«0100»
`accountNumber`	`data` -> account -> `accountNumber`	42000

En la tabla anterior, KEY `profileType` es una VALUE de las `metadata` KEY. El KEY `positionId` es un VALUE de los `data` KEY. El KEY `accountNumber` es un VALUE de los `account`KEY, y el `account` KEY es un VALUE de los `data`KEY.

Ejemplo de documento JSON

```
{
  "metadata" : {
    "upperLastNameFirstName" : "ABC XYZ",
    "upperEmailAddress" : "abc@gmail.com",
"profileType" : "P"
  },
  "data" : {
    "onlineContactId" : "032323323",
    "displayName" : "Abc, Xyz",
    "firstName" : "Xyz",
    "lastName" : "Abc",
    "emailAddress" : "abc@gmail.com",
    "productRegistrationStatus" : "Not registered",
"positionId" : "0100",
    "arrayPattern" : " -",
    "account" : {
      "companyId" : "SMGE",
      "businessUnitId" : 7,
"accountNumber" : 42000,
      "parentAccountNumber" : 32000,
      "firstName" : "john",
      "lastName" : "doe",
      "street1" : "retOdertcaShr ",
      "city" : "new york",
      "postalcode" : "XY ABC",
```

```
      "country" : "United States"
    },
    "products" : [
      {
        "appUserGuid" : "i0acc4450000001823fbad478e2eab8a0",
        "id" : "0000000046",
        "name" : "ProView",
        "domain" : "EREADER",
        "registrationStatus" : false,
        "status" : "11"
      }
    ]
  }
}
```

Consulta SQL que se utiliza para obtener los campos seleccionados del documento JSON

```
select parent_account_number,account_number,business_unit_id,position_id from
 aws_test_table aws,JSON_TABLE ( json_doc, '$' ERROR ON ERROR
COLUMNS (
parent_account_number NUMBER PATH '$.data.account.parentAccountNumber',
account_number NUMBER PATH '$.data.account.accountNumber',
business_unit_id NUMBER PATH '$.data.account.businessUnitId',
position_id VARCHAR2 ( 4 ) PATH '$.data.positionId'
)) as sc
```

En la consulta anterior, `JSON_TABLE` es una función integrada en Oracle que convierte los datos JSON en formato de fila. La función JSON_TABLE espera parámetros en formato JSON.

Cada elemento `COLUMNS` tiene un valor predefinido `PATH`, y cuando hay un `VALUE` adecuado para un determinado elemento `KEY`, se devuelve en formato de fila.

Resultado de la consulta anterior

PARENT_AC COUNT_NUMBER	ACCOUNT_NUMBER	BUSINESS_UNIT_ID	POSITION_ID
32000	42000	7	0100
32001	42001	6	0090

4. Postgres_SQL_READ_JSON

Ejemplo de consulta y sintaxis

```
select *
from (
select (json_doc::json->'data'->'account'->>'parentAccountNumber')::INTEGER as
 parentAccountNumber,
(json_doc::json->'data'->'account'->>'accountNumber')::INTEGER as accountNumber,
(json_doc::json->'data'->'account'->>'businessUnitId')::INTEGER as businessUnitId,
(json_doc::json->'data'->>'positionId')::VARCHAR as positionId
from aws_test_pg_table) d ;
```

En Oracle, `PATH` se utiliza para identificar el `KEY` y `VALUE` especifico. Sin embargo, PostgreSQL utiliza un modelo `HIERARCHY` para leer `KEY` y `VALUE` desde JSON. Los mismos datos de JSON que se mencionan en `Oracle_SQL_Read_JSON` se utilizan en los siguientes ejemplos.

No se admiten consultas SQL de tipo CAST

(Si fuerza el tipo de texto `CAST`, la consulta fallará y se producirá un error de sintaxis).

```
select *
from (
select (json_doc::json->'data'->'account'->'parentAccountNumber') as
 parentAccountNumber,
(json_doc::json->'data'->'account'->'accountNumber')as accountNumber,
(json_doc::json->'data'->'account'->'businessUnitId') as businessUnitId,
(json_doc::json->'data'->'positionId')as positionId
from aws_test_pg_table) d ;
```

Si se utiliza un operador una vez mayor (>), se devolverá el `VALUE` definido para ese `KEY`. Por ejemplo, `KEY`: `positionId`, y `VALUE`: `"0100"`.

No se permite escribir el tipo `CAST` cuando se utiliza el operador una vez mayor (>).

Se admiten consultas SQL de tipo CAST

```
select *
from (
select (json_doc::json->'data'->'account'->>'parentAccountNumber')::INTEGER as
 parentAccountNumber,
(json_doc::json->'data'->'account'->>'accountNumber')::INTEGER as accountNumber,
```

```
(json_doc::json->'data'->'account'->>'businessUnitId')::INTEGER as businessUnitId,
(json_doc::json->'data'->>'positionId')::varchar as positionId
from aws_test_pg_table) d ;
```

Para usar el tipo `CAST`, debe usar un operador mayor del doble. Si utiliza el operador una vez mayor, la consulta devuelve el `VALUE` definido (por ejemplo `KEY`: `positionId`, y `VALUE`: `"0100"`). Si se utiliza el operador mayor del doble (>>), se devolverá el valor real definido para ese valor `KEY` (por ejemplo, `KEY`: `positionId`, y `VALUE`: `0100` sin comillas dobles).

En el caso anterior, `parentAccountNumber` es el tipo `CAST` a `INT`, `accountNumber` es el tipo `CAST` a `INT`, `businessUnitId` es el tipo `CAST` a `INT`, y `positionId` es el tipo `CAST` a `VARCHAR`.

En las tablas siguientes se muestran los resultados de las consultas que explican el papel del operador único mayor que (>) y del operador doble mayor que (>>).

En la primera tabla, la consulta utiliza el único operador mayor que (>). Cada columna es de tipo JSON y no se puede convertir en otro tipo de datos.

parentAccountNumber	Número de cuenta	businessUnitId	ID de puesto
2003565430	2003564830	7	«0100»
2005284042	2005284042	6	«0090»
2000272719	2000272719	1	“0100”

En la segunda tabla, la consulta utiliza el operador doble mayor que (>>). Cada columna admite el tipo `CAST` en función del valor de la columna. Por ejemplo, en este caso `INTEGER`.

parentAccountNumber	Número de cuenta	businessUnitId	ID de puesto
2003565430	2003564830	7	0100
2005284042	2005284042	6	0090
2000272719	2000272719	1	0100

5. Oracle_SQL_JSON_AGGREGATION_JOIN

Consulta de ejemplo

```
SELECT
    JSON_OBJECT(
        'accountCounts' VALUE JSON_ARRAYAGG(
            JSON_OBJECT(
                'businessUnitId' VALUE business_unit_id,
                        'parentAccountNumber' VALUE parent_account_number,
                        'accountNumber' VALUE account_number,
                        'totalOnlineContactsCount' VALUE online_contacts_count,
                        'countByPosition' VALUE
                    JSON_OBJECT(
                        'taxProfessionalCount' VALUE tax_count,
                        'attorneyCount' VALUE attorney_count,
                        'nonAttorneyCount' VALUE non_attorney_count,
                        'clerkCount' VALUE clerk_count
                               ) ) ) )
FROM
    (SELECT
             tab_data.business_unit_id,
             tab_data.parent_account_number,
             tab_data.account_number,
             SUM(1) online_contacts_count,
             SUM(CASE WHEN tab_data.position_id = '0095' THEN  1 ELSE 0 END) tax_count,
             SUM(CASE    WHEN tab_data.position_id = '0100' THEN 1 ELSE 0 END)
 attorney_count,
             SUM(CASE    WHEN tab_data.position_id = '0090' THEN 1 ELSE 0 END)
 non_attorney_count,
             SUM(CASE    WHEN tab_data.position_id = '0050' THEN 1 ELSE 0 END)
 clerk_count
           FROM aws_test_table scco,JSON_TABLE ( json_doc, '$' ERROR ON ERROR
  COLUMNS (
            parent_account_number NUMBER PATH
             '$.data.account.parentAccountNumber',
             account_number NUMBER PATH '$.data.account.accountNumber',
             business_unit_id NUMBER PATH '$.data.account.businessUnitId',
             position_id VARCHAR2 ( 4 ) PATH '$.data.positionId'    )
             ) AS tab_data
             INNER JOIN JSON_TABLE ( '{
           "accounts": [{
             "accountNumber": 42000,
             "parentAccountNumber": 32000,
```

```
          "businessUnitId": 7
        }, {
          "accountNumber": 42001,
          "parentAccountNumber": 32001,
          "businessUnitId": 6
        }]
      }', '$.accounts[*]' ERROR ON ERROR
      COLUMNS (
      parent_account_number PATH '$.parentAccountNumber',
      account_number PATH '$.accountNumber',
      business_unit_id PATH '$.businessUnitId')
      ) static_data
      ON ( static_data.parent_account_number = tab_data.parent_account_number
           AND static_data.account_number = tab_data.account_number
           AND static_data.business_unit_id = tab_data.business_unit_id )
        GROUP BY
            tab_data.business_unit_id,
            tab_data.parent_account_number,
            tab_data.account_number
    );
```

Para convertir los datos de nivel de fila al formato JSON, Oracle tiene funciones integradas como `JSON_OBJECT`, `JSON_ARRAY`, `JSON_OBJECTAGG` y `JSON_ARRAYAGG`.

- `JSON_OBJECT` acepta dos parámetros: `KEY` y `VALUE`. El parámetro `KEY` debe estar codificado de forma rígida o ser de naturaleza estática. El parámetro `VALUE` se deriva de la salida de la tabla.
- `JSON_ARRAYAGG` acepta `JSON_OBJECT` como parámetro. Esto ayuda a agrupar el conjunto de `JSON_OBJECT` elementos en forma de lista. Por ejemplo, si tiene un elemento `JSON_OBJECT` que tiene varios registros (múltiples pares `KEY` y `VALUE`en el conjunto de datos), `JSON_ARRAYAGG` agrega el conjunto de datos y crea una lista. Según el lenguaje de estructura de datos, `LIST` es un grupo de elementos. En este contexto, `LIST` es un grupo de elementos `JSON_OBJECT`.

En el siguiente ejemplo, se muestra un elemento `JSON_OBJECT`.

```
{
   "taxProfessionalCount": 0,
   "attorneyCount": 0,
   "nonAttorneyCount": 1,
   "clerkCount": 0
}
```

En el siguiente ejemplo, se muestran dos elementos `JSON_OBJECT`, con `LIST` indicado mediante llaves cuadradas (`[ ]`).

```
[
    {
        "taxProfessionalCount": 0,
        "attorneyCount": 0,
        "nonAttorneyCount": 1,
        "clerkCount": 0
      }
,
    {
        "taxProfessionalCount": 2,
        "attorneyCount": 1,
        "nonAttorneyCount": 3,
        "clerkCount":4
      }
]
```

Ejemplo de consulta SQL

```
SELECT
    JSON_OBJECT(
        'accountCounts' VALUE JSON_ARRAYAGG(
            JSON_OBJECT(
                'businessUnitId' VALUE business_unit_id,
                        'parentAccountNumber' VALUE parent_account_number,
                        'accountNumber' VALUE account_number,
                        'totalOnlineContactsCount' VALUE online_contacts_count,
                        'countByPosition' VALUE
                    JSON_OBJECT(
                        'taxProfessionalCount' VALUE tax_count,
                        'attorneyCount' VALUE attorney_count,
                        'nonAttorneyCount' VALUE non_attorney_count,
                        'clerkCount' VALUE clerk_count
                               )
                        )
                                          )
              )
FROM
    (SELECT
            tab_data.business_unit_id,
            tab_data.parent_account_number,
```

```
           tab_data.account_number,
           SUM(1) online_contacts_count,
           SUM(CASE WHEN tab_data.position_id = '0095' THEN  1 ELSE   0 END
           )      tax_count,
           SUM(CASE    WHEN tab_data.position_id = '0100' THEN        1    ELSE
 0 END
           )      attorney_count,

           SUM(CASE    WHEN tab_data.position_id = '0090' THEN        1    ELSE
 0 END
           )      non_attorney_count,

           SUM(CASE    WHEN tab_data.position_id = '0050' THEN        1    ELSE
 0 END
           )      clerk_count

       FROM
           aws_test_table scco,  JSON_TABLE ( json_doc, '$' ERROR ON ERROR
           COLUMNS (
           parent_account_number NUMBER PATH '$.data.account.parentAccountNumber',
           account_number NUMBER PATH '$.data.account.accountNumber',
           business_unit_id NUMBER PATH '$.data.account.businessUnitId',
           position_id VARCHAR2 ( 4 ) PATH '$.data.positionId'    )
           ) AS tab_data
           INNER JOIN JSON_TABLE ( '{
       "accounts": [{
         "accountNumber": 42000,
         "parentAccountNumber": 32000,
         "businessUnitId": 7
       }, {
         "accountNumber": 42001,
         "parentAccountNumber": 32001,
         "businessUnitId": 6
       }]
     }', '$.accounts[*]' ERROR ON ERROR
     COLUMNS (
     parent_account_number PATH '$.parentAccountNumber',
     account_number PATH '$.accountNumber',
     business_unit_id PATH '$.businessUnitId')
     ) static_data ON ( static_data.parent_account_number =
 tab_data.parent_account_number
                         AND static_data.account_number = tab_data.account_number
```

```
                          AND static_data.business_unit_id =
 tab_data.business_unit_id )
        GROUP BY
            tab_data.business_unit_id,
            tab_data.parent_account_number,
            tab_data.account_number
    );
```

Ejemplo de resultado de la consulta SQL anterior

```
{
  "accountCounts": [
    {
      "businessUnitId": 6,
      "parentAccountNumber": 32001,
      "accountNumber": 42001,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 0,
        "nonAttorneyCount": 1,
        "clerkCount": 0
      }
    },
    {
      "businessUnitId": 7,
      "parentAccountNumber": 32000,
      "accountNumber": 42000,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 1,
        "nonAttorneyCount": 0,
        "clerkCount": 0
      }
    }
  ]
}
```

6. Postgres_SQL_JSON_Aggregation_JOIN

Las funciones integradas de PostgresQL `JSON_BUILD_OBJECT` y `JSON_AGG` convierten los datos de nivel de fila a formato JSON. PostgreSQL `JSON_OBJECT` y `JSON_AGG`son equivalentes a Oracle `JSON_BUILD_OBJECT` y `JSON_ARRAYAGG`.

Consulta de ejemplo

```
select
JSON_BUILD_OBJECT ('accountCounts',
    JSON_AGG(
        JSON_BUILD_OBJECT ('businessUnitId',businessUnitId
        ,'parentAccountNumber',parentAccountNumber
        ,'accountNumber',accountNumber
        ,'totalOnlineContactsCount',online_contacts_count,
        'countByPosition',
            JSON_BUILD_OBJECT (
            'taxProfessionalCount',tax_professional_count
            ,'attorneyCount',attorney_count
            ,'nonAttorneyCount',non_attorney_count
            ,'clerkCount',clerk_count
            )
        )
    )
)
from (
with tab as (select * from (
select (json_doc::json->'data'->'account'->>'parentAccountNumber')::INTEGER as
 parentAccountNumber,
(json_doc::json->'data'->'account'->>'accountNumber')::INTEGER as accountNumber,
(json_doc::json->'data'->'account'->>'businessUnitId')::INTEGER as businessUnitId,
(json_doc::json->'data'->>'positionId')::varchar as positionId
from aws_test_pg_table) a ) ,
tab1 as ( select
(json_array_elements(b.jc -> 'accounts') ->> 'accountNumber')::integer accountNumber,
(json_array_elements(b.jc -> 'accounts') ->> 'businessUnitId')::integer
 businessUnitId,
(json_array_elements(b.jc -> 'accounts') ->> 'parentAccountNumber')::integer
 parentAccountNumber
from (
select '{
        "accounts": [{
          "accountNumber": 42001,
          "parentAccountNumber": 32001,
          "businessUnitId": 6
```

```
        }, {
          "accountNumber": 42000,
          "parentAccountNumber": 32000,
          "businessUnitId": 7
        }]
      }'::json as jc) b)
select
tab.businessUnitId::text,
tab.parentAccountNumber::text,
tab.accountNumber::text,
SUM(1) online_contacts_count,
SUM(CASE WHEN tab.positionId::text = '0095' THEN 1 ELSE 0  END)
  tax_professional_count,
SUM(CASE WHEN tab.positionId::text = '0100' THEN 1 ELSE 0  END)      attorney_count,
SUM(CASE  WHEN tab.positionId::text = '0090' THEN      1  ELSE      0 END)
  non_attorney_count,
SUM(CASE  WHEN tab.positionId::text = '0050' THEN      1  ELSE      0 END)
  clerk_count
from tab1,tab
where tab.parentAccountNumber::INTEGER=tab1.parentAccountNumber::INTEGER
and tab.accountNumber::INTEGER=tab1.accountNumber::INTEGER
and tab.businessUnitId::INTEGER=tab1.businessUnitId::INTEGER
GROUP BY      tab.businessUnitId::text,
            tab.parentAccountNumber::text,
            tab.accountNumber::text) a;
```

Ejemplo de salida de la consulta anterior

Las salidas de Oracle y PostgreSQL son exactamente las mismas.

```
{
  "accountCounts": [
    {
      "businessUnitId": 6,
      "parentAccountNumber": 32001,
      "accountNumber": 42001,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 0,
        "nonAttorneyCount": 1,
        "clerkCount": 0
      }
    },
```

```
    {
      "businessUnitId": 7,
      "parentAccountNumber": 32000,
      "accountNumber": 42000,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 1,
        "nonAttorneyCount": 0,
        "clerkCount": 0
      }
    }
  ]
}
```

7. Oracle_Procedure_with_JSON_Query

Este código convierte el procedimiento de Oracle en una función de PostgreSQL que tiene consultas JSON SQL. Muestra cómo la consulta transpone JSON a filas y viceversa.

```
CREATE OR REPLACE PROCEDURE p_json_test(p_in_accounts_json IN varchar2,
 p_out_accunts_json  OUT varchar2)
IS
BEGIN
/*
p_in_accounts_json paramter should have following format:
       {
        "accounts": [{
          "accountNumber": 42000,
          "parentAccountNumber": 32000,
          "businessUnitId": 7
        }, {
          "accountNumber": 42001,
          "parentAccountNumber": 32001,
          "businessUnitId": 6
        }]
      }
*/
SELECT
    JSON_OBJECT(
        'accountCounts' VALUE JSON_ARRAYAGG(
            JSON_OBJECT(
                'businessUnitId' VALUE business_unit_id,
```

```
                        'parentAccountNumber' VALUE parent_account_number,
                        'accountNumber' VALUE account_number,
                        'totalOnlineContactsCount' VALUE online_contacts_count,
                        'countByPosition' VALUE
                    JSON_OBJECT(
                        'taxProfessionalCount' VALUE tax_count,
                        'attorneyCount' VALUE attorney_count,
                        'nonAttorneyCount' VALUE non_attorney_count,
                        'clerkCount' VALUE clerk_count
                               ) ) ) )
into p_out_accunts_json
FROM
    (SELECT
            tab_data.business_unit_id,
            tab_data.parent_account_number,
            tab_data.account_number,
            SUM(1) online_contacts_count,
            SUM(CASE WHEN tab_data.position_id = '0095' THEN  1 ELSE 0 END) tax_count,
            SUM(CASE    WHEN tab_data.position_id = '0100' THEN 1 ELSE 0 END)
 attorney_count,
            SUM(CASE    WHEN tab_data.position_id = '0090' THEN 1 ELSE 0 END)
 non_attorney_count,
            SUM(CASE    WHEN tab_data.position_id = '0050' THEN 1 ELSE 0 END)
 clerk_count
        FROM aws_test_table scco,JSON_TABLE ( json_doc, '$' ERROR ON ERROR
            COLUMNS (
            parent_account_number NUMBER PATH '$.data.account.parentAccountNumber',
            account_number NUMBER PATH '$.data.account.accountNumber',
            business_unit_id NUMBER PATH '$.data.account.businessUnitId',
            position_id VARCHAR2 ( 4 ) PATH '$.data.positionId'    )
            ) AS tab_data
            INNER JOIN JSON_TABLE ( p_in_accounts_json, '$.accounts[*]' ERROR ON ERROR

      COLUMNS (
      parent_account_number PATH '$.parentAccountNumber',
      account_number PATH '$.accountNumber',
      business_unit_id PATH '$.businessUnitId')
      ) static_data
      ON ( static_data.parent_account_number = tab_data.parent_account_number
           AND static_data.account_number = tab_data.account_number
           AND static_data.business_unit_id = tab_data.business_unit_id )
        GROUP BY
            tab_data.business_unit_id,
            tab_data.parent_account_number,
```

```
            tab_data.account_number
    );
EXCEPTION
WHEN OTHERS THEN
   raise_application_error(-20001,'Error while running the JSON query');
END;
/
```

Ejecutando el procedimiento

El siguiente bloque de código explica cómo puede ejecutar el procedimiento de Oracle creado anteriormente con una entrada JSON de ejemplo en el procedimiento. También proporciona el resultado o la salida de este procedimiento.

```
set serveroutput on;
declare
v_out varchar2(30000);
v_in varchar2(30000):= '{
        "accounts": [{
          "accountNumber": 42000,
          "parentAccountNumber": 32000,
          "businessUnitId": 7
        }, {
          "accountNumber": 42001,
          "parentAccountNumber": 32001,
          "businessUnitId": 6
        }]
      }';
begin
  p_json_test(v_in,v_out);
  dbms_output.put_line(v_out);
end;
/
```

Resultado del procedimiento

```
{
  "accountCounts": [
    {
      "businessUnitId": 6,
      "parentAccountNumber": 32001,
      "accountNumber": 42001,
      "totalOnlineContactsCount": 1,
```

```
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 0,
        "nonAttorneyCount": 1,
        "clerkCount": 0
      }
    },
    {
      "businessUnitId": 7,
      "parentAccountNumber": 32000,
      "accountNumber": 42000,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 1,
        "nonAttorneyCount": 0,
        "clerkCount": 0
      }
    }
  ]
}
```

8. Postgres_Function_with_JSON_Query

Función de ejemplo

```
CREATE OR REPLACE  FUNCTION f_pg_json_test(p_in_accounts_json  text)
RETURNS text
LANGUAGE plpgsql
AS
$$
DECLARE
 v_out_accunts_json   text;
BEGIN
SELECT
JSON_BUILD_OBJECT ('accountCounts',
    JSON_AGG(
        JSON_BUILD_OBJECT ('businessUnitId',businessUnitId
        ,'parentAccountNumber',parentAccountNumber
        ,'accountNumber',accountNumber
        ,'totalOnlineContactsCount',online_contacts_count,
        'countByPosition',
            JSON_BUILD_OBJECT (
            'taxProfessionalCount',tax_professional_count
```

```
            ,'attorneyCount',attorney_count
            ,'nonAttorneyCount',non_attorney_count
            ,'clerkCount',clerk_count
            ))))
INTO v_out_accunts_json
FROM (
WITH tab AS (SELECT * FROM (
SELECT (json_doc::json->'data'->'account'->>'parentAccountNumber')::INTEGER AS
 parentAccountNumber,
(json_doc::json->'data'->'account'->>'accountNumber')::INTEGER AS accountNumber,
(json_doc::json->'data'->'account'->>'businessUnitId')::INTEGER AS businessUnitId,
(json_doc::json->'data'->>'positionId')::varchar AS positionId
FROM aws_test_pg_table) a ) ,
tab1 AS ( SELECT
(json_array_elements(b.jc -> 'accounts') ->> 'accountNumber')::integer accountNumber,
(json_array_elements(b.jc -> 'accounts') ->> 'businessUnitId')::integer businessUnitId,
(json_array_elements(b.jc -> 'accounts') ->> 'parentAccountNumber')::integer
 parentAccountNumber
FROM (
SELECT p_in_accounts_json::json AS jc) b)
SELECT
tab.businessUnitId::text,
tab.parentAccountNumber::text,
tab.accountNumber::text,
SUM(1) online_contacts_count,
SUM(CASE WHEN tab.positionId::text = '0095' THEN 1 ELSE 0  END)
  tax_professional_count,
SUM(CASE WHEN tab.positionId::text = '0100' THEN 1 ELSE 0  END)      attorney_count,
SUM(CASE  WHEN tab.positionId::text = '0090' THEN      1  ELSE      0 END)
  non_attorney_count,
SUM(CASE  WHEN tab.positionId::text = '0050' THEN      1  ELSE      0 END)
  clerk_count
FROM tab1,tab
WHERE tab.parentAccountNumber::INTEGER=tab1.parentAccountNumber::INTEGER
AND tab.accountNumber::INTEGER=tab1.accountNumber::INTEGER
AND tab.businessUnitId::INTEGER=tab1.businessUnitId::INTEGER
GROUP BY      tab.businessUnitId::text,
            tab.parentAccountNumber::text,
            tab.accountNumber::text) a;
RETURN v_out_accunts_json;
END;
$$;
```

Ejecución de la función

```
select    f_pg_json_test('{
        "accounts": [{
          "accountNumber": 42001,
          "parentAccountNumber": 32001,
          "businessUnitId": 6
        }, {
          "accountNumber": 42000,
          "parentAccountNumber": 32000,
          "businessUnitId": 7
        }]
      }')   ;
```

Salida de función

La siguiente salida de es similar a la salida del procedimiento de Oracle. La diferencia es que esta salida está en formato de texto.

```
{
  "accountCounts": [
    {
      "businessUnitId": "6",
      "parentAccountNumber": "32001",
      "accountNumber": "42001",
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 0,
        "nonAttorneyCount": 1,
        "clerkCount": 0
      }
    },
    {
      "businessUnitId": "7",
      "parentAccountNumber": "32000",
      "accountNumber": "42000",
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 1,
        "nonAttorneyCount": 0,
        "clerkCount": 0
```

```
        }
      }
    ]
}
```

Copiar tablas de Amazon DynamoDB entre cuentas mediante una implementación personalizada

Documento creado por Ramkumar Ramanujam (AWS)

Entorno: producción	Origen: Amazon DynamoDB	Destino: Amazon DynamoDB
Tipo R: N/D	Carga de trabajo: todas las demás cargas de trabajo	Tecnologías: bases de datos
Servicios de AWS: Amazon DynamoDB		

Resumen

Cuando se trabaja con Amazon DynamoDB en Amazon Web Services (AWS), un caso de uso habitual consiste en copiar o sincronizar tablas de DynamoDB en entornos de desarrollo, de prueba o de ensayo con datos de la tabla que se encuentra en el entorno de producción. Como práctica estándar, cada entorno utiliza una cuenta AWS diferente.

DynamoDB ahora admite copias de seguridad entre cuentas mediante AWS Backup. Para obtener información sobre los costos de almacenamiento asociados al uso de AWS Backup, consulte los precios de AWS Backup. Cuando se utiliza AWS Backup para copiar entre cuentas, las cuentas de origen y de destino deben formar parte de una organización de AWS Organizations. Existen otras soluciones para realizar copias de seguridad y restauraciones entre cuentas mediante servicios de AWS, como AWS Data Pipeline o AWS Glue. Sin embargo, el uso de esas soluciones aumenta el tamaño de las aplicaciones, ya que es necesario implementar y mantener más servicios de AWS.

También puede utilizar Amazon DynamoDB Streams para capturar los cambios en la tabla de la cuenta de origen. A continuación, puede iniciar una función de AWS Lambda y realizar los cambios correspondientes en la tabla de destino de la cuenta de destino. Sin embargo, esa solución se aplica a los casos de uso en los que las tablas de origen y de destino deben mantenerse siempre sincronizadas. Es posible que no se aplique a los entornos de desarrollo, pruebas y uso transitorio en los que los datos se actualizan con frecuencia.

Este patrón proporciona los pasos para implementar una solución personalizada para copiar una tabla de Amazon DynamoDB de una cuenta a otra. Este patrón se puede implementar mediante

lenguajes de programación comunes, como C#, Java y Python. Recomendamos utilizar un lenguaje que sea compatible con un AWS SDK.

Requisitos previos y limitaciones

Requisitos previos

- Dos cuentas de AWS activas
- Tablas de DynamoDB en ambas cuentas
- Configuración de políticas y roles de AWS Identity and Access Management (IAM)
- Conocimiento de cómo acceder a las tablas de Amazon DynamoDB mediante cualquier lenguaje de programación común, como C#, Java o Python

Limitaciones

Este patrón se aplica a las tablas de DynamoDB de alrededor de 2 GB o menos. Con una lógica adicional para gestionar las interrupciones de conexión o sesión, las limitaciones y los errores y reintentos, también se puede utilizar para tablas más grandes.

La operación de escaneo de DynamoDB, que lee los elementos de la tabla de origen, solo puede recuperar hasta 1 MB de datos en una sola llamada. En el caso de tablas más grandes, de más de 2 GB, esta limitación puede aumentar el tiempo total necesario para realizar una copia completa de la tabla.

Arquitectura

Automatizar y escalar

Este patrón se aplica a las tablas de DynamoDB de tamaño más pequeño, de unos 2 GB.

Para aplicar este patrón a tablas más grandes, aborde los problemas siguientes:

- Durante la operación de copia de la tabla, se mantienen dos sesiones activas, utilizando diferentes tokens de seguridad. Si la operación de copia de la tabla tarda más que los tiempos de caducidad del token, debe implementar una lógica para actualizar los tokens de seguridad.
- Si no se aprovisionan suficientes unidades de capacidad de lectura (RCU) y unidades de capacidad de escritura (WCU), las lecturas o escrituras en la tabla de origen o destino podrían tener limitaciones. Asegúrese de atrapar y gestionar estas excepciones.

- Controle cualquier otro error o excepción y establezca un mecanismo de reintento para volver a intentarlo o continuar desde el punto en el que se produjo el error en la operación de copia.

Herramientas

Herramientas

- Amazon DynamoDB: Amazon DynamoDB es un servicio de base de datos NoSQL totalmente administrado que ofrece un rendimiento rápido y predecible, así como una perfecta escalabilidad.
- Las herramientas adicionales necesarias variarán según el lenguaje de programación que se elija para la implementación. Por ejemplo, si usa C#, necesitará Microsoft Visual Studio y los siguientes NuGet paquetes:
  - `AWSSDK`
  - `AWSSDK.DynamoDBv2`

Código

El siguiente fragmento de código de Python elimina y vuelve a crear una tabla de DynamoDB mediante la biblioteca Boto3.

No utilice el `AWS_ACCESS_KEY_ID` ni el `AWS_SECRET_ACCESS_KEY` de un nombre de usuario de IAM porque se trata de credenciales a largo plazo, que deben evitarse para el acceso programático a los servicios de AWS. Para obtener más información sobre cómo usar credenciales de seguridad temporales, consulte la sección Prácticas recomendables.

Las credenciales `AWS_ACCESS_KEY_ID`, `AWS_SECRET_ACCESS_KEY` y `TEMPORARY_SESSION_TOKEN` utilizadas en el siguiente fragmento de código son credenciales temporales obtenidas de AWS Security Token Service (AWS STS).

```
import boto3
import sys
import json

#args = input-parameters = GLOBAL_SEC_INDEXES_JSON_COLLECTION,
 ATTRIBUTES_JSON_COLLECTION, TARGET_DYNAMODB_NAME, TARGET_REGION, ...

#Input param: GLOBAL_SEC_INDEXES_JSON_COLLECTION
```

```
#[{"IndexName":"Test-index","KeySchema":[{"AttributeName":"AppId","KeyType":"HASH"},
{"AttributeName":"AppType","KeyType":"RANGE"}],"Projection":
{"ProjectionType":"INCLUDE","NonKeyAttributes":["PK","SK","OwnerName","AppVersion"]}}]

#Input param: ATTRIBUTES_JSON_COLLECTION
#[{"AttributeName":"PK","AttributeType":"S"},
{"AttributeName":"SK","AttributeType":"S"},
{"AttributeName":"AppId","AttributeType":"S"},
{"AttributeName":"AppType","AttributeType":"N"}]

region = args['TARGET_REGION']
target_ddb_name = args['TARGET_DYNAMODB_NAME']

global_secondary_indexes = json.loads(args['GLOBAL_SEC_INDEXES_JSON_COLLECTION'])
attribute_definitions = json.loads(args['ATTRIBUTES_JSON_COLLECTION'])

# Drop and create target DynamoDB table
dynamodb_client = boto3.Session(
        aws_access_key_id=args['AWS_ACCESS_KEY_ID'],
        aws_secret_access_key=args['AWS_SECRET_ACCESS_KEY'],
        aws_session_token=args['TEMPORARY_SESSION_TOKEN'],
    ).client('dynamodb')

# Delete table
print('Deleting table: ' + target_ddb_name + ' ...')

try:
    dynamodb_client.delete_table(TableName=target_ddb_name)

    #Wait for table deletion to complete
    waiter = dynamodb_client.get_waiter('table_not_exists')
    waiter.wait(TableName=target_ddb_name)
    print('Table deleted.')
except dynamodb_client.exceptions.ResourceNotFoundException:
    print('Table already deleted / does not exist.')
    pass

print('Creating table: ' + target_ddb_name + ' ...')

table = dynamodb_client.create_table(
    TableName=target_ddb_name,
    KeySchema=[
        {
            'AttributeName': 'PK',
```

```
            'KeyType': 'HASH'  # Partition key
        },
        {
            'AttributeName': 'SK',
            'KeyType': 'RANGE'  # Sort key
        }
    ],
    AttributeDefinitions=attribute_definitions,
    GlobalSecondaryIndexes=global_secondary_indexes,
    BillingMode='PAY_PER_REQUEST'
)

waiter = dynamodb_client.get_waiter('table_exists')
waiter.wait(TableName=target_ddb_name)

print('Table created.')
```

Prácticas recomendadas

Credenciales temporales

Como práctica recomendada de seguridad, al acceder a los servicios de AWS mediante programación, evite utilizar la dirección `AWS_ACCESS_KEY_ID` y `AWS_SECRET_ACCESS_KEY` de un usuario de IAM, ya que se trata de credenciales a largo plazo. Intente utilizar siempre credenciales temporales para acceder a los servicios de AWS mediante programación.

Así, por ejemplo, un desarrollador codifica de forma rígida la dirección `AWS_ACCESS_KEY_ID` y `AWS_SECRET_ACCESS_KEY` de un usuario de IAM en la aplicación durante el desarrollo, pero no elimina los valores codificados antes de incorporar los cambios en el repositorio de código. Estas credenciales expuestas pueden ser utilizadas por usuarios de forma involuntaria o malintencionada, lo que puede tener graves consecuencias (especialmente si las credenciales expuestas tienen privilegios de administrador). Estas credenciales expuestas se deben desactivar o eliminar inmediatamente mediante la consola de IAM o interfaz de la línea de comandos de AWS (AWS CLI).

Para obtener credenciales temporales para el acceso mediante programación a los servicios de AWS, utilice AWS STS. Las credenciales temporales son válidas solo durante el tiempo especificado (de 15 minutos a 36 horas). La duración máxima permitida de las credenciales temporales varía en función de factores como la configuración de los roles y el encadenamiento de funciones. Para obtener más información acerca de AWS STS, consulte la documentación.

Epics

Configurar tablas de DynamoDB

Tarea	Descripción	Habilidades requeridas
Cree tablas de DynamoDB.	Cree tablas de DynamoDB, con índices, en las cuentas de AWS de origen y de destino. Configure el aprovisionamiento de capacidad como modo bajo demanda, lo que permite a DynamoDB escalar las capacidades de lectura/escritura de forma dinámica en función de la carga de trabajo. Como alternativa, puede utilizar la capacidad aprovisionada con 4000 RCU y 4000 WCU.	Desarrollador de aplicaciones, administrador de bases de datos e ingeniero de migraciones
Rellene la tabla de origen.	Rellene la tabla de DynamoDB de la cuenta de origen con datos de prueba. Disponer de al menos 50 MB o más de datos de prueba ayuda a ver el pico y el promedio de las RCU consumidas durante la copia de la tabla. A continuación, puede cambiar el aprovisionamiento de capacidad según sea necesario.	Desarrollador de aplicaciones, administrador de bases de datos e ingeniero de migraciones

Configurar las credenciales para acceder a las tablas de DynamoDB

Tarea	Descripción	Habilidades requeridas
Cree roles de IAM para acceder a las tablas de DynamoDB de origen y destino.	Cree un rol de IAM en la cuenta de origen con permisos de acceso (lectura) a la tabla de DynamoDB de la cuenta de origen. Agregue la cuenta de origen como entidad de confianza para este rol. Cree un rol de IAM en la cuenta de destino con permisos de acceso (creación , lectura, actualización, eliminación) a la tabla de DynamoDB de la cuenta de destino. Agregue la cuenta de destino como entidad de confianza para este rol.	Desarrollador de aplicaciones, AWS DevOps

Copiar datos de tablas de una cuenta a otra

Tarea	Descripción	Habilidades requeridas
Obtenga credenciales temporales para los roles de IAM.	Obtenga credenciales temporales para el rol de IAM creado en la cuenta de origen. Obtenga credenciales temporales para el rol de	Desarrollador de aplicación, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	IAM creado en la cuenta de destino. Una forma de obtener las credenciales temporales para el rol de IAM es usar AWS STS desde la AWS CLI. `aws sts assume-role --role-arn arn:aws:iam::<account-id>:role/<role-name> --role-session-name <session-name> --profile <profile-name>` Utilice el perfil de AWS adecuado (correspondiente a la cuenta de origen o de destino). Para obtener más información sobre cómo obtener credencia les temporales consulte lo siguiente: • AWS Security Token Service API Reference (Referencia de API del servicio de token de seguridad de AWS) • Getting IAM role credentials for CLI access (Obtener las credenciales del rol de IAM para el acceso a la CLI)	

Tarea	Descripción	Habilidades requeridas
Inicialice los clientes de DynamoDB para el acceso a DynamoDB de origen y destino.	Inicialice los clientes de DynamoDB, que proporcio na AWS SDK, para las tablas de DynamoDB de origen y destino. • Para el cliente DynamoDB de origen, utilice las credenciales temporales obtenidas de la cuenta de origen. • Para el cliente DynamoDB de destino, utilice las credenciales temporales obtenidas de la cuenta de destino. Para obtener más información sobre cómo realizar solicitud es mediante credenciales temporales de IAM, consulte la Documentación de AWS.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Eliminar y recrear la tabla de destino.	Elimine y vuelva a crear la tabla de DynamoDB de destino (junto con los índices) en la cuenta de destino mediante el cliente DynamoDB de la cuenta de destino. La eliminación de todos los registros de una tabla de DynamoDB es una operación costosa porque consume las WCU aprovisionadas. Al eliminar y volver a crear la tabla, se evitan esos costos adicionales. Puede añadir índices a una tabla después de crearla, pero esto requiere de 2 a 5 minutos más. Resulta más eficiente crear índices durante la creación de la tabla, pasando la colección de índices a la llamada `createTable` .	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Realice la copia de la tabla.	Repita los pasos siguientes hasta que se copien todos los datos: • Realice un análisis de la tabla de la cuenta de origen mediante el cliente DynamoDB de origen. Cada escaneo de DynamoDB recupera solo 1 MB de datos de la tabla, por lo que debe repetir esta operación hasta que se lean todos los elementos o registros. • Para cada conjunto de elementos escaneados, escriba los elementos en la tabla de la cuenta de destino, con el cliente de DynamoDB de destino, mediante la llamada `BatchWriteItem` del SDK de AWS para DynamoDB. De este modo, se reduce el número de solicitudes `PutItem` que se envían a DynamoDB. • `BatchWriteItem` tiene un límite de 25 operaciones de escritura o incorporación, es decir, de hasta 16 MB. Debe añadir una lógica para acumular hasta 25 objetos escaneados antes de	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	llamar a `BatchWriteItem`. `BatchWriteItem` devuelve una lista de los elementos que no se han podido copiar correctamente. Con esta lista, agregue una lógica de reintento para realizar otra llamada de `BatchWriteItem` únicamente con los elementos que no se hayan realizado correctamente. Para obtener más información, consulte la implementación de referencia en C# (para eliminar, crear y rellenar tablas) en la sección de adjuntos. También se adjunta un ejemplo de archivo de notación de JavaScript objetos (JSON) de configuración de tablas.	

Recursos relacionados

- Documentación de Amazon DynamoDB
- Creating an IAM user in your AWS account (Crear un usuario de IAM en la cuenta de AWS)
- SDK de AWS
- Using temporary credentials with AWS resources (Usar credenciales temporales con recursos de AWS)

Información adicional

Este patrón se implementó con C# para copiar una tabla de DynamoDB con 200 000 elementos (el tamaño medio de los elementos es de 5 KB y el tamaño de la tabla de 250 MB). La tabla de DynamoDB de destino se configuró con una capacidad aprovisionada de 4000 RCU y 4000 WCU.

La operación completa de copia de la tabla (de la cuenta de origen a la cuenta de destino), incluida la eliminación y la recreación de la tabla, duró 5 minutos. Unidades de capacidad total: 30 000 RCU y aproximadamente 400 000 WCU.

Para obtener más información sobre los modos de capacidad de DynamoDB, consulte Read/Write capacity mode (Modo de capacidad de lectura/escritura) en la documentación de AWS.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Copiar tablas de Amazon DynamoDB entre cuentas mediante AWS Backup

Documento creado por Ramkumar Ramanujam (AWS)

Entorno: PoC o piloto	Tecnologías: migración; bases de datos	Servicios de AWS: Amazon DynamoDB; AWS Backup

Resumen

Cuando se trabaja con Amazon DynamoDB en Amazon Web Services (AWS), un caso de uso habitual consiste en copiar o sincronizar tablas de DynamoDB en entornos de desarrollo, de prueba o de ensayo con datos de la tabla que se encuentra en el entorno de producción. Como práctica estándar, cada entorno utiliza una cuenta AWS diferente.

AWS Backup admite realizar copias de seguridad y restaurar datos entre regiones y cuentas para DynamoDB, Amazon Simple Storage Service (Amazon S3) y otros servicios de AWS. Este patrón muestra los pasos para utilizar el proceso de copia de seguridad y restauración entre cuentas de AWS Backup para copiar tablas de DynamoDB entre cuentas de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Dos cuentas AWS activas que pertenezcan a la misma organización de AWS Organizations
- Tablas de DynamoDB en ambas cuentas.
- Permisos de AWS Identity and Access Management (IAM) para crear y utilizar almacenes de AWS Backup

Limitaciones

- Las cuentas AWS de origen y destino deben formar parte de la misma organización de AWS Organizations.

Arquitectura

Pila de tecnología de destino

- AWS Backup
- Amazon DynamoDB

Arquitectura de destino

1. Cree la copia de seguridad de la tabla de DynamoDB en el almacén de copias de seguridad de AWS Backup de la cuenta de origen.
2. Copie la copia de seguridad en el almacén de copias de seguridad de la cuenta de destino.
3. Restaure la DynamoDb tabla en la cuenta de destino mediante la copia de seguridad del almacén de copias de seguridad de la cuenta de destino.

Automatizar y escalar

Puede utilizar AWS Backup para programar copias de seguridad que se ejecuten en intervalos específicos.

Herramientas

- AWS Backup: AWS Backup es un servicio totalmente administrado para centralizar y automatizar la protección de datos en todos los servicios de AWS, tanto en la nube como en las instalaciones. Con este servicio, puede configurar políticas de copia de seguridad y supervisar la actividad de los recursos de AWS en un solo lugar. Le permite automatizar y consolidar las tareas de copia de seguridad que se service-by-service realizaban anteriormente y elimina la necesidad de crear scripts personalizados y procesos manuales.
- Amazon DynamoDB: Amazon DynamoDB es un servicio de base de datos NoSQL totalmente administrado que ofrece un rendimiento rápido y predecible, así como una perfecta escalabilidad.

Epics

Activar las funciones de AWS Backup en las cuentas de origen y destino

Tarea	Descripción	Habilidades requeridas
Active las características avanzadas de copia de seguridad de DynamoDB y entre cuentas.	En las cuentas AWS de origen y de destino, realice lo siguiente: 1. En la consola de administración de AWS, abra la consola de AWS Backup. 2. Seleccione Settings (Configuración). 3. En Advanced features for Amazon DynamoDB backups (Características avanzadas para copias de seguridad de Amazon DynamoDB), confirme que la opción Advanced features esté activada o seleccione Enable (Activar). 4. En Cross-account management (Administración multicuenta), seleccione Enable (Activar) para Cross-account backup (Copia de seguridad multicuenta).	AWS DevOps, ingeniero de migración

Crear almacenes de copia de seguridad en las cuentas de origen y destino

Tarea	Descripción	Habilidades requeridas
Creación de almacenes de copias de seguridad.	En las cuentas AWS de origen y de destino, realice lo siguiente: 1. En la consola de AWS Backup, seleccione Backup Vaults (Almacenes de copias de seguridad). 2. Seleccione Create Backup vault (Crear almacén de copias de seguridad). 3. Copie el nombre de recurso de Amazon (ARN) del almacén de copias de seguridad y guárdelo. Se necesitarán los ARN de los dos almacenes de copias de seguridad (el de origen y el de destino), al copiar la copia de seguridad de la tabla de DynamoDB entre la cuenta de origen y la de destino.	AWS DevOps, ingeniero de migración

Realizar copias de seguridad y restaurar mediante almacenes de copias de seguridad

Tarea	Descripción	Habilidades requeridas
En la cuenta de origen, cree una copia de seguridad de la tabla de DynamoDB.	Para crear una copia de seguridad de la tabla de DynamoDB en la cuenta de origen, realice lo siguiente:	AWS DevOps, DBA, ingeniero de migración

Tarea	Descripción	Habilidades requeridas
	1. En la página Dashboard (panel) de AWS Backup, seleccione Create on-demand backup (Crear copia de seguridad bajo demanda). 2. En la sección Settings (Configuración), para Resource type (Tipo de recurso), seleccione DynamoDB y, a continuación, seleccione el nombre de la tabla. 3. En la lista desplegable Backup Vault (Almacén de copias de seguridad), seleccione el almacén que creó en la cuenta de origen. 4. Seleccione el Retention period (Periodo de conservación) que desee. 5. Seleccione Create on-demand backup (Crear copia de seguridad bajo demanda). Se creará un nuevo trabajo de copia de seguridad. Para supervisar el estado del trabajo de copia de seguridad, acceda a la página Jobs (Trabajos) de AWS Backup y seleccione la pestaña Backup	

Tarea	Descripción	Habilidades requeridas
	Jobs (Trabajos de copia de seguridad). En esta pestaña se muestran todos los trabajos de copia de seguridad activos, en curso y finalizados.	

Tarea	Descripción	Habilidades requeridas
Copie la copia de seguridad de la cuenta de origen a la cuenta de destino.	Una vez finalizado el trabajo de copia de seguridad, copie la copia de seguridad de la tabla de DynamoDB del almacén de copias de seguridad de la cuenta de origen al almacén de copias de seguridad de la cuenta de destino. Para copiar el almacén de copias de seguridad, realice lo siguiente en la cuenta de origen: 1. En la consola de AWS Backup, seleccione Backup Vaults (Almacenes de copias de seguridad). 2. En Backups (Copias de seguridad), seleccione la copia de seguridad de la tabla de DynamoDB. 3. Seleccione Actions (Acciones), Copy (Copiar). 4. Especifique la región de AWS de la cuenta de destino. 5. Para el External vault ARN (Nombre de recurso de Amazon de almacén externo), escriba el ARN del almacén de copias de	AWS DevOps, ingeniero de migración, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	seguridad que creó en la cuenta de destino. 6. Para copiar las copias de seguridad de la cuenta de origen a la cuenta de destino, sitúese en el almacén de copias de seguridad de la cuenta de destino y habilite el acceso de una cuenta diferente.	
Restaurar la copia de seguridad en la cuenta de destino.	En la cuenta AWS de destino, haga lo siguiente: 1. En la consola de AWS Backup, seleccione Backup Vaults (Almacenes de copias de seguridad). 2. En Backups (Copias de seguridad), seleccione la copia de seguridad que copió de la cuenta de origen. 3. Seleccione Actions (Acciones), Restore (Restaurar). 4. Especifique el nombre de la tabla de DynamoDB de destino que desea restaurar .	AWS DevOps, DBA, ingeniero de migración

Recursos relacionados

- Uso de AWS Backup con DynamoDB

- Crear copias de las copias de seguridad entre cuentas AWS
- Precios de AWS Backup

Crear informes detallados de costos y uso para Amazon RDS y Amazon Aurora

Creado por Lakshmanan Lakshmanan (AWS) y Sudarshan Narasimhan

Entorno: producción	Tecnologías: Bases de datos; gestión de costos; análisis	Servicios de AWS: Amazon Athena; Amazon Aurora; Amazon RDS; Administración de facturación y costos de AWS

Resumen

Este patrón muestra cómo realizar un seguimiento de los costos de uso de los clústeres de Amazon Relational Database Service (Amazon RDS) o Amazon Aurora mediante la configuración de etiquetas de asignación de costos definidas por el usuario. Puede usar estas etiquetas para crear informes detallados de costos y uso en el explorador de costos de AWS para clústeres en varias dimensiones. Por ejemplo, puede realizar un seguimiento de los costos de uso a nivel de equipo, proyecto o centro de costos y, a continuación, analizar los datos en Amazon Athena.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una o más instancias de Amazon RDS o Amazon Aurora

Limitaciones

Para conocer las restricciones de etiquetado, consulte la Guía del usuario de facturación de AWS.

Arquitectura

Pila de tecnología de destino

- Amazon RDS o Amazon Aurora

- AWSInforme de uso y costos
- AWS Cost Explorer
- Amazon Athena

Flujo de trabajo y arquitectura

El flujo de trabajo de etiquetado y análisis consta de los siguientes pasos:

1. Un ingeniero de datos, un administrador de bases de datos o un administrador de AWS crea etiquetas de asignación de costos definidas por el usuario para los clústeres de Amazon RDS o Aurora.
2. Un administrador de AWS activa las etiquetas.
3. Las etiquetas envían los metadatos al explorador de costos de AWS.
4. Un ingeniero de datos, un administrador de bases de datos o un administrador de AWS crea un informe mensual de asignación de costos.
5. Un ingeniero de datos, un administrador de bases de datos o un administrador de AWS analiza el informe mensual de asignación de costos mediante Amazon Athena.

En el siguiente diagrama, se muestra cómo aplicar etiquetas para realizar un seguimiento de los costos de uso de las instancias de Amazon RDS o Aurora.

El siguiente diagrama de arquitectura muestra cómo el informe de asignación de costos se integra con Amazon Athena para su análisis.

El informe de asignación de costos mensual se almacena en un bucket de Amazon S3 que especifique. Al configurar Athena con la CloudFormation plantilla de AWS, tal y como se describe en la sección Epics, la plantilla incluye varios recursos adicionales, como un rastreador de AWS Glue, una base de datos de AWS Glue, un evento del Amazon Simple Notification System (Amazon SNS), funciones de AWS Lambda y roles de AWS Identity and Access Management (IAM) para las funciones de Lambda. A medida que llegan nuevos archivos de datos de costos al bucket de S3, las notificaciones de eventos se utilizan para reenviar estos archivos a una función de Lambda para

su procesamiento. La función de Lambda inicia un trabajo de rastreador de AWS Glue para crear o actualizar la tabla en el catálogo de datos de AWS Glue. Esta tabla se usa a continuación para consultar datos en Athena.

Herramientas

- Amazon Athena es un servicio de consultas interactivo que facilita el análisis de datos en Amazon S3 con SQL estándar.
- Amazon Aurora es un motor de base de datos relacional completamente administrado diseñado para la nube y compatible con MySQL y PostgreSQL.
- Amazon Relational Database Service (Amazon RDS) le ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS.
- AWS CloudFormation es un servicio de infraestructura como código (IaC) que le permite modelar, aprovisionar y administrar fácilmente recursos de AWS y de terceros.
- El Explorador de costos de AWS permite ver y analizar los costos y el uso.

Epics

Crear y activar etiquetas para su clúster de Amazon RDS o Aurora

Tarea	Descripción	Habilidades requeridas
Cree etiquetas de asignación de costos definidas por el usuario para su clúster de Amazon RDS o Aurora.	Para añadir etiquetas a un clúster de Amazon RDS o Aurora nuevo o existente, siga las instrucciones de Añadir, publicar y eliminar etiquetas de la Guía del usuario de Amazon Aurora. Nota: Para obtener información sobre cómo configurar un clúster de Amazon Aurora, consulte las instrucciones para MySQL y PostgreSQL en la	Administrador de AWS, ingeniero de datos, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	Guía del usuario de Amazon Aurora.	
Active las etiquetas de asignación de costos definidas por el usuario.	Siga las instrucciones de Activación de etiquetas de asignación de costos definidas por el usuario en la Guía del usuario de facturación de AWS.	Administrador de AWS

Crear informes de uso y costo

Tarea	Descripción	Habilidades requeridas
Cree y configure informes de costos y uso para sus clústeres.	1. Inicie sesión en la consola de administración de AWS y abra la consola de facturación de AWS. 2. En el panel de navegación, elija Reportes de uso y costo. 3. Elija Crear informe. 4. Proporcione un nombre para el informe, mantenga la configuración predeterminada para las demás opciones y, a continuación, seleccione Siguiente. 5. Seleccione Configurar y proporcione los detalles de un bucket de S3 existente. También puede elegir crear un bucket de S3 nuevo	Propietario de la aplicación, administrador de AWS, administrador de bases de datos, AWS general, ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	desde esta pantalla. Elija Siguiente. 6. Verifique la política predeterminada que se aplicará a su bucket, seleccione la casilla de confirmación y, a continuación, seleccione Guardar. 7. En Prefijo de ruta de informe, especifique el prefijo que desee anexar al nombre del informe. 8. En Granularidad temporal, seleccione Cada hora, Cada día o Cada mes, en función de la frecuencia con la que desee que se recopilen los datos para el informe. 9. Para el Informe de control de versiones, seleccione si desea que las nuevas versiones del informe se creen por separado o que se sobrescriba el informe existente con cada versión. 10. Para Habilitar la integración de datos de informes para, seleccione Amazon Athena. Verifique que el tipo de compresión esté establecido en Parquet. 11. Elija Siguiente.	

Tarea	Descripción	Habilidades requeridas
	12. Revise la configuración del informe y, a continuación, seleccione Revisar y completar. Los datos estarán disponibles en 24 horas.	

Analizar los datos de los informes de costos y uso

Tarea	Descripción	Habilidades requeridas
Analice los datos del informe de costos y uso.	1. Configure y utilice Athena para analizar los datos del informe. Para obtener instrucciones, consulte Consultar informes de costos y uso de con Amazon Athena en la Guía del usuario de informes de costos y uso de AWS. Le recomendamos que utilice la CloudFormation plantilla de AWS proporcionada por Athena. 2. Ejecute consultas de Athena. Por ejemplo, puede utilizar la siguiente consulta SQL para comprobar el estado de la actualización de datos.	Propietario de la aplicación, administrador de AWS, administrador de bases de datos, AWS general, ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	`select status from cost_and_usage_data_status` Para obtener más información, consulte Ejecutar consultas de Amazon Athena en la Guía del usuario de los informes de costos y uso de AWS. Nota: cuando ejecute su consulta de SQL, asegúrese de que la base de datos correcta esté seleccionada en la lista desplegable.	

Recursos relacionados

Referencias

- Configuración de Athena con CloudFormation plantillas de AWS (recomendado)
- Configuración manual de Athena
- Ejecutar consultas de Amazon Athena
- Cargar datos de informes en otros recursos

Tutoriales y videos

- Analice los informes de costos y uso con Amazon Athena (vídeo) YouTube

Emule cargas de trabajo de Oracle RAC mediante puntos de conexión personalizados en Aurora PostgreSQL

Creado por HariKrishna Boorgadda (AWS)

Entorno: PoC o piloto	Origen: bases de datos: relacionales	Destino: Aurora PostgreSQL
Tipo R: redefinir la plataforma	Carga de trabajo: Oracle	Tecnologías: bases de datos; migración
Servicios de AWS: Amazon Aurora; Amazon CloudWatch		

Resumen

Este patrón describe cómo emular servicios en una carga de trabajo de Oracle Real Application Clusters (Oracle RAC) mediante Amazon Aurora compatible con PostgreSQL usando puntos de conexión personalizados que distribuyen las cargas de trabajo entre las instancias de un único clúster. Este patrón muestra cómo crear puntos de conexión personalizados para bases de datos de Amazon Aurora. Los puntos de conexión personalizados le permiten distribuir y equilibrar la carga de trabajo en diferentes conjuntos de instancias de base de datos de su clúster de Aurora.

En un entorno Oracle RAC, los servicios pueden abarcar una o más instancias, y facilitar el equilibrio de la carga de trabajo en función del rendimiento de las transacciones. Las características del servicio incluyen la recuperación end-to-end desatendida, los cambios continuos según la carga de trabajo y la total transparencia de la ubicación. Puede usar este patrón para emular algunas de estas características. Por ejemplo, puede emular la capacidad de enrutar las conexiones para las aplicaciones de informes.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un controlador JDBC de PostgreSQL

- Una base de datos Aurora compatible con PostgreSQL
- Una base de datos Oracle RAC migrada a una base de datos Aurora compatible con PostgreSQL

Limitaciones

- Para conocer las limitaciones de los puntos de conexión personalizados, consulte Especificar las propiedades de los puntos de conexión personalizados en la documentación de Amazon RDS.

Arquitectura

Pila de tecnología de origen

- Una base de datos Oracle RAC de tres nodos

Pila de tecnología de destino

- Una base de datos Aurora compatible con PostgreSQL con dos réplicas de lectura

Arquitectura de origen

En el siguiente diagrama se muestra la arquitectura de una base de datos Oracle RAC de tres nodos.

Arquitectura de destino

En el siguiente diagrama se muestra la arquitectura de una base de datos Aurora compatible con PostgreSQL con dos réplicas de lectura. Las tres aplicaciones o servicios diferentes usan puntos de conexión personalizados, que atienden a distintos usuarios de aplicaciones y redirigen el tráfico y la carga entre las réplicas principales y las de lectura.

Herramientas

- Amazon Aurora PostgreSQL-Compatible es un motor de base de datos relacional completamente administrado que le permite configurar, administrar y escalar implementaciones de PostgreSQL.
- Amazon le CloudWatch ayuda a monitorizar las métricas de sus recursos de AWS y las aplicaciones que ejecuta en AWS en tiempo real.

- Amazon Relational Database Service (Amazon RDS) para PostgreSQL le ayuda a configurar, utilizar y escalar una base de datos relacional de PostgreSQL en la nube de AWS.
- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que permite interactuar con los servicios de AWS mediante comandos en el intérprete de comandos de línea de comandos.

Epics

Cree el clúster de Aurora compatible con PostgreSQL

Tarea	Descripción	Habilidades requeridas
Cree un clúster.	Para crear el clúster, consulte Crear un clúster de base de datos y conectarse a una base de datos en un clúster de base de datos de Aurora PostgreSQL en la documentación de Amazon RDS.	Administrador de AWS
Cree un grupo de parámetros personalizados para la carga de trabajo.	Para crear un grupo de parámetros, consulte Crear un grupo de parámetros de clúster de base de datos en la documentación de Amazon RDS.	Administrador de AWS
Cree alarmas y notificaciones de eventos.	Puedes usar las notificaciones de eventos y las CloudWatch alarmas de Amazon para avisarte cuando el clúster cambie de estado y para capturar métricas cuando se alcance un umbral predefinido. Para crear una CloudWatch alarma, consulte Crear una	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	CloudWatch alarma basada en un umbral estático en la CloudWatch documentación. Para crear una notificación de evento, consulte Crear una regla de CloudWatch eventos que se active en un evento en la CloudWatch documentación.	

Agregue réplicas al clúster de base de datos Aurora compatible con PostgreSQL

Tarea	Descripción	Habilidades requeridas
Añada las réplicas de lectura al clúster.	1. Crear una réplica de lectura. 2. Agregue la réplica de lectura a la misma zona de disponibilidad en la que se encuentra su clúster de base de datos. Nota: puede usar una zona de disponibilidad diferente si así lo requieren sus requisitos de nodo de conmutación por error.	Administrador de AWS
Anote el punto de conexión de la réplica de lectura.	Documente el punto de conexión de la réplica de lectura. Lo usará más adelante, en la creación de los puntos de conexión personalizados.	Administrador de AWS

Creación de puntos de conexión personalizados

Tarea	Descripción	Habilidades requeridas
Introduzca un nombre para el punto de conexión personalizado.	Cree un nombre único de punto de conexión, relacionado con su carga de trabajo o aplicación, para cada punto de conexión que necesite.	Administrador de AWS
Agregue los miembros del punto de conexión.	Agregue sus puntos de conexión de réplica de lectura a un grupo personalizado. Para obtener más información, consulte Editar un punto de conexión personalizado en la documentación de Amazon RDS.	Administrador de AWS
(Opcional) Agregue futuras instancias al clúster.	Si desea añadir más réplicas o puntos de conexión al grupo personalizado, consulte Añadir réplicas de Aurora a un clúster de base de datos en la documentación de Amazon RDS.	Administrador de AWS
Creación del punto de conexión	Para crear el punto de conexión, consulte Crear un punto de conexión personalizado en la documentación de Amazon RDS.	Administrador de AWS

Pruebe las conexiones de la aplicación usando puntos de conexión personalizados

Tarea	Descripción	Habilidades requeridas
Comparta los detalles del punto de conexión personalizado con la aplicación que corresponda a su carga de trabajo.	Agregue los detalles de su punto de conexión personalizado a los detalles de conexión a la base de datos en la aplicación de informes que desea probar.	Administrador de AWS
Conecte la carga de trabajo mediante el punto de conexión personalizado.	Valide los detalles del punto de conexión personalizado en la aplicación de informes.	Administrador de AWS
Compruebe los detalles de la conexión en la base de datos.	1. Pruebe el nombre de usuario y el recuento de conexiones de su aplicación. 2. Compruebe el equilibrio de carga entre sus cargas de trabajo para asegurarse de que las conexiones estén distribuidas en diferentes puntos de conexión personalizados (principal y réplicas de lectura).	Administrador de AWS

Recursos relacionados

- Tipos de puntos de conexión de Aurora
- Reglas de afiliación para puntos de conexión personalizados
- E: Ejemplo de nd-to-end AWS CLI para puntos de enlace personalizados
- Amazon Aurora como alternativa a Oracle RAC
- Desafíos en la migración de Oracle a PostgreSQL y cómo superarlos

Habilite conexiones cifradas para instancias de base de datos de PostgreSQL en Amazon RDS

Creado por Rohit Kapoor (AWS)

Entorno: PoC o piloto	Tecnologías: bases de datos; redes; seguridad, identidad, cumplimiento	Carga de trabajo: código abierto
Servicios de AWS: Amazon RDS; Amazon Aurora		

Resumen

Amazon Relational Database Service (Amazon RDS) admite el cifrado SSL en instancias de base de datos PostgreSQL. Con SSL, puede cifrar una conexión de PostgreSQL entre sus aplicaciones y sus instancias de base de datos de Amazon RDS para PostgreSQL. De forma predeterminada, Amazon RDS para PostgreSQL emplea SSL/TLS y espera que todos los clientes se conecten mediante cifrado SSL/TLS. Amazon RDS para PostgreSQL admite las versiones 1.1 y 1.2 de TLS.

En este patrón se describe cómo puede habilitar conexiones cifradas para una instancia de base de datos de Amazon RDS para PostgreSQL. Puede usar el mismo proceso para habilitar conexiones cifradas en Amazon Aurora compatible con PostgreSQL.

Requisitos previos y limitaciones

- Una cuenta de AWS activa
- Una instancia de base de datos de Amazon RDS para PostgreSQL
- Un paquete SSL

Arquitectura

Herramientas

- pgAdmin es una plataforma de administración y desarrollo de código abierto para PostgreSQL. Puede usar pgAdmin en Linux, Unix, macOS y Windows para administrar los objetos de su base de datos en PostgreSQL 10 y versiones posteriores.
- Los editores de PostgreSQL proporcionan una interfaz más fácil de usar que le ayuda a crear, desarrollar y ejecutar consultas, así como a editar el código según sus necesidades.

Prácticas recomendadas

- Supervise las conexiones de bases de datos no seguras.
- Audite los derechos de acceso a la base de datos.
- Asegúrese de que las copias de seguridad y las instantáneas estén cifradas en reposo.
- Supervise el acceso a bases de datos.
- Evite los grupos de acceso sin restricciones.
- Mejora tus notificaciones con Amazon GuardDuty.
- Supervise el cumplimiento de las políticas con regularidad.

Epics

Descargue un certificado de confianza e impórtelo a su almacén de confianza

Tarea	Descripción	Habilidades requeridas
Cargue un certificado de confianza en su ordenador.	Para agregar certificados al almacén de entidades emisoras de certificados raíz de confianza de su equipo, siga estos pasos. (Estas instrucciones usan Windows Server como ejemplo). 1. En Windows Server, seleccione Iniciar, Ejecutar	DevOps ingeniero, ingeniero de migración, DBA

Tarea	Descripción	Habilidades requeridas
	y, a continuación, escriba mmc. 2. En la consola, elija Archivo, Agregar/Quitar complemento. 3. En Complementos disponibles, elija Certificados y, a continuación, elija Agregar. 4. En Este complemento siempre administrará los certificados de, elija Cuenta de equipo y pulse Siguiente. 5. Seleccione Equipo local y, a continuación, Finalizar. 6. Si no tiene más complementos que añadir a la consola, pulse Aceptar. 7. En el árbol de la consola, haga doble clic en Certificados. 8. Haga clic con el botón derecho en Entidades emisoras de certificados raíz. 9. Seleccione Todas las tareas, Importar para importar los certificados descargados. 10. Siga los pasos del asistente de importación de certificados.	

Fuerza las conexiones SSL.

Tarea	Descripción	Habilidades requeridas
Cree un grupo de parámetros y establezca el parámetro rds.force_ssl.	Si la instancia de base de datos PostgreSQL tiene un grupo de parámetros personalizado, edite dicho grupo y cambie `rds.force_ssl` a 1. Si la instancia de base de datos usa el grupo de parámetros predeterminado sin `rds.force_ssl` habilitado, cree un nuevo grupo de parámetros. Puede modificar el nuevo grupo de parámetros usando la API de Amazon RDS o bien manualmente siguiendo estos pasos. Para crear un nuevo grupo de parámetros: 1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon RDS para la región de AWS que aloja la instancia de base de datos. 2. En el panel de navegación, seleccione Parameter groups (Grupos de parámetros).	DevOps ingeniero, ingeniero de migración, DBA

Tarea	Descripción	Habilidades requeridas
	3. Elija Crear grupo de parámetros y defina los siguientes valores: • En Familia de grupo de parámetros, elija postgres14. • En Nombre de grupo, escriba pgsql-<database_instance>-ssl. • En Descripción, introduzca una descripción en formato libre para el grupo de parámetros que va a añadir. • Seleccione Crear. 4. Elija el grupo de parámetros que ha creado. 5. En Parameter group actions (Acciones de grupos de parámetros), seleccione Edit (Editar). 6. Busque rds.force_ssl y cambie su configuración a 1. Nota: Realice pruebas en el lado del cliente antes de cambiar este parámetro. 7. Elija Guardar cambios. Para asociar el grupo de parámetros a su instancia de base de datos PostgreSQL:	

Tarea	Descripción	Habilidades requeridas
	1. En la consola de Amazon RDS, en el panel de navegación, elija Bases de datos y, a continuación, seleccione la instancia de base de datos PostgreSQL. 2. Elija Modificar. 3. En Configuración adicional, seleccione el nuevo grupo de parámetros y, a continuación, elija Continuar. 4. En Programar modificaciones, elija Aplicar inmediatamente. 5. Elija Modify DB instance (Modificar la instancia de la base de datos). Para obtener más información, consulte la documentación de Amazon RDS.	
Fuerza las conexiones SSL.	Conéctese a la instancia de base de datos de Amazon RDS para PostgreSQL. Los intentos de conexión que no usan SSL se rechazan con un mensaje de error. Para obtener más información, consulte la documentación de Amazon RDS.	DevOps ingeniero, ingeniero de migración, DBA

Instale la extensión SSL

Tarea	Descripción	Habilidades requeridas
Instale la extensión SSL.	1. Inicie una conexión psql o pgAdmin como Administrador de base de datos. 2. Llame a la función ssl_is_used () para determinar si se está usando SSL. `select ssl_is_used();` La función devuelve `t` si la conexión usa SSL; de lo contrario, devuelve `f`. 3. Instale la extensión SSL. `create extension sslinfo;` `show ssl;` `select ssl_cipher();` Para obtener más información, consulte la documentación de Amazon RDS.	DevOps ingeniero, ingeniero de migración, DBA

Configure su cliente PostgreSQL para SSL

Tarea	Descripción	Habilidades requeridas
Configure un cliente para SSL.	Al usar SSL, puede iniciar el servidor PostgreSQL con soporte para conexiones cifradas que empleen protocolos TLS. El servidor	DevOps ingeniero, ingeniero de migración, DBA

Tarea	Descripción	Habilidades requeridas
	escucha tanto las conexiones estándar como las SSL en el mismo puerto TCP, y negocia con cualquier cliente que se conecte si debe utilizar SSL. Por defecto, esto es una una opción de cliente. Si usa el cliente psql: 1. Asegúrese de que el certificado Amazon RDS se ha cargado en su ordenador local. 2. Inicie una conexión de cliente SSL añadiendo lo siguiente: `psql postgres -h SOMEHOST.amazonaws.com -p 8192 -U someuser sslmode=verify-full sslrootcert=rds-ssl-ca-cert.pem` `select ssl_cipher();` Para otros clientes de PostgreSQL: • Modifique el parámetro de clave pública de la aplicación correspondiente. Esto puede estar disponible como una opción, como parte de su cadena de	

Tarea	Descripción	Habilidades requeridas
	conexión, o como una propiedad en la página de conexión en las herramien tas de la interfaz gráfica de usuario. Consulte las siguientes páginas para estos clientes: • Documentación de pgAdmin • Documentación de JDBC	

Solución de problemas

Problema	Solución
No se puede descargar el certificado SSL.	Compruebe la conexión al sitio web y vuelva a intentar descargar el certificado en su ordenador local.

Recursos relacionados

- Documentación de Amazon RDS para PostgreSQL
- Uso de SSL con una instancia de base de datos PostgreSQL (documentación de Amazon RDS)
- Conexiones TCP/IP seguras con SSL (documentación de PostgreSQL)
- Uso de SSL (documentación de JDBC)

Cifrar una instancia de base de datos de Amazon RDS para PostgreSQL existente

Creado por Piyush Goyal (AWS), Shobana Raghu (AWS) y Yaser Raja (AWS)

Entorno: Producción	Tecnologías: bases de datos, seguridad, identidad, cumplimiento	Servicios de AWS: Amazon RDS; AWS KMS; AWS DMS

Resumen

Este patrón explica cómo cifrar una instancia de base de datos de Amazon Relational Database Service (Amazon RDS) para PostgreSQL en la nube de Amazon Web Services (AWS) con un tiempo de inactividad mínimo. Este proceso también funciona para instancias de base de datos de Amazon RDS para MySQL.

Puede habilitar el cifrado para una instancia de base de datos de Amazon RDS cuando la cree, pero no después de haberla creado. Sin embargo, puede añadir cifrado a una instancia de base de datos sin cifrar creando una instantánea de la instancia de base de datos y, a continuación, creando una copia cifrada de esa instantánea. A continuación, puede restaurar una instancia de base de datos a partir de la instantánea encriptada para obtener una copia encriptada de su instancia de base de datos original. Si su proyecto permite un tiempo de inactividad (al menos en el caso de las transacciones de escritura) para esta actividad, esto es todo lo que tiene que hacer. Cuando esté disponible la nueva copia cifrada de la instancia de base de datos, podrá dirigir sus aplicaciones a la nueva base de datos. Sin embargo, si su proyecto no permite un tiempo de inactividad significativo para esta actividad, necesitará un enfoque alternativo que le ayude a minimizar dicho tiempo de inactividad. Este patrón emplea AWS Database Migration Service (AWS DMS) para migrar y replicar continuamente los datos, de modo que la transición a la nueva base de datos cifrada se podrá realizar con un tiempo de inactividad mínimo.

En las instancias de base de datos cifradas de Amazon RDS se utiliza el algoritmo de cifrado AES-256 estándar del sector para cifrar los datos en el servidor que aloja la instancia de base de datos de Amazon RDS. Una vez cifrados los datos, Amazon RDS se encarga de la autenticación de acceso y del descifrado de los datos de forma transparente, con un impacto mínimo en el desempeño. No es necesario modificar las aplicaciones cliente de base de datos para utilizar el cifrado.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una instancia de base de datos de Amazon RDS para PostgreSQL sin encriptar
- Experiencia trabajando con tareas de AWS DMS (creación, modificación o detención) (consulte Trabajar con tareas de AWS DMS en la documentación de AWS DMS)
- Familiaridad con AWS Key Management Service (AWS KMS) para el cifrado de bases de datos (consulte la documentación de AWS KMS)

Limitaciones

- Únicamente se puede activar el cifrado para una instancia de base de datos de Amazon RDS al crearla, no después de que se ha creado.
- Los datos de las tablas no registradas no se podrán restaurar mediante instantáneas. Para obtener más información, consulte Prácticas recomendadas para trabajar con PostgreSQL.
- No se puede tener una réplica de lectura cifrada de una instancia de base de datos sin cifrar ni una réplica de lectura sin cifrar de una instancia de base de datos cifrada.
- No se puede restaurar una copia de seguridad ni una instantánea sin cifrar en una instancia de base de datos cifrada.
- AWS DMS no transfiere automáticamente las secuencias, por lo que necesitará pasos adicionales para gestionarlas.

Para obtener más información, consulte Limitaciones de las instancias de base de datos cifradas de Amazon RDS en la documentación de Amazon RDS.

Arquitectura

Arquitectura de origen

- Instancia de base de datos de RDS sin cifrar

Arquitectura de destino

- Instancia de base de datos de RDS cifrada

- La instancia de base de datos de RDS de destino se crea restaurando la copia de instantánea de base de datos de la instancia de base de datos de RDS de origen.
- Al restaurar la instantánea, se emplea una clave de AWS KMS para el cifrado.
- Para migrar los datos, se emplea una tarea de replicación de AWS DMS.

Herramientas

Herramientas usadas para habilitar el cifrado:

- Clave de AWS KMS prara encriptar: Cuando crea una instancia de base de datos cifrada, puede elegir una clave administrada por el cliente o la clave de AWS KMS para Amazon RDS para cifrar la instancia de base de datos. Si no especifica el identificador de clave para una clave administrada por el cliente, Amazon RDS utiliza la clave administrada de AWS para la nueva instancia de base de datos. Amazon RDS crea una clave administrada de AWS para Amazon RDS para su cuenta de AWS. Su cuenta de AWS tiene una clave administrada de AWS diferente para Amazon RDS para cada región de AWS. Para obtener más información sobre el uso de claves de KMS para el cifrado de Amazon RDS, consulte Cifrar recursos de Amazon RDS.

Herramientas usadas para la replicación continua:

- AWS DMS: puede usar AWS Database Migration Service (AWS DMS) para replicar los cambios desde la base de datos de origen a la base de datos de destino. Es importante mantener sincronizadas las bases de datos de origen y destino para poder reducir al mínimo el tiempo de inactividad. Para obtener información sobre la configuración de AWS DMS y la creación de tareas, consulte la documentación de AWS DMS.

Epics

Cree una instantánea de la instancia de base de datos de origen y cífrela

Tarea	Descripción	Habilidades requeridas
Compruebe los detalles de la instancia de base de datos PostgreSQL de origen.	En la consola de Amazon RDS, seleccione la instancia de base de datos PostgreSQL de origen. En la pestaña Configuración, asegúrese de que el cifrado no esté habilitado en esta instancia. Para ver una ilustración de la pantalla, consulte la sección de Información adicional.	Administrador de base de datos
Crear la instantánea de base de datos.	Cree una instantánea de la base de datos de la instancia que desea encriptar. La cantidad de tiempo que tarda en crearse una instantánea depende del tamaño de su base de datos. Para obtener instrucciones, consulte Crear una instantánea de base de datos en la documentación de Amazon RDS.	Administrador de base de datos
Cifre la instantánea.	En el panel de navegación de la consola de Amazon RDS, elija Instantáneas y, a continuación, seleccione la instantánea de base de datos que ha creado. En Actions (Acciones), elija Copy Snapshot (Copiar instantán	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	ea). Indique la región de AWS de destino y el nombre de la copia de la instantánea de base de datos en los campos correspondientes. Seleccione la casilla de verificación Habilitar el cifrado. En Master Key, especifique el identificador de la clave de KMS que se debe usar para cifrar la copia de la instantánea de base de datos. Elija Copy Snapshot. Para más información, consulte Copiar una instantánea en la documentación de Amazon RDS.	

Prepare la instancia de base de datos de destino

Tarea	Descripción	Habilidades requeridas
Restaurare la instantánea de la base de datos.	En la consola de Amazon RDS, seleccione Instantáneas. Elija la instantánea cifrada que ha creado. En Actions (Acciones), seleccione Restore Snapshot (Restaurar instantánea). Para Identificador de Instancia de la base de datos, proporcione un nombre único para la nueva instancia de la base de datos. Revise los detalles de la instancia y, a continuac	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	ión, seleccione Restaurar instancia de base de datos. Se creará una nueva instancia de base de datos cifrada a partir de la instantánea. Para más información, consulte Restauración a partir de una instantánea de la base de datos en la documentación de Amazon RDS.	
Migre los datos mediante AWS DMS.	En la consola de AWS DMS, cree una tarea de AWS DMS. En Tipo de migración, elija Migrar datos existentes y replicar los cambios en curso. En Configuración de tareas, en el Modo de preparación de la tabla de destino, seleccione Truncar. Para más información, consulte Crear una tarea en la documentación de AWS DMS.	Administrador de base de datos
Habilitar la validación de datos.	En Configuración de tareas, seleccione Habilitar validación. Esto le permite comparar los datos de origen con los de destino para verificar que los datos se han migrado correctamente.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Deshabilite las restricciones en la instancia de base de datos de destino.	Desactive todos los desencadenantes y restricciones de clave externa en la instancia de base de datos de destino y, a continuación, inicie la tarea de AWS DMS. Para obtener más información sobre cómo deshabilitar los desencadenantes y restricciones de clave externa, consulte la documentación de AWS DMS.	Administrador de base de datos
Compruebe los datos.	Una vez completada la carga, compruebe los datos de la instancia de base de datos de destino para asegurarse de que coinciden con los datos de origen. Para obtener más información consulte la AWS DMS data validation (Validación de datos de AWS DMS) en la documentación de AWS DMS.	Administrador de base de datos

Transición a la instancia de base de datos de destino

Tarea	Descripción	Habilidades requeridas
Detenga las operaciones de escritura en la instancia de base de datos de origen.	Detenga las operaciones de escritura en la instancia de base de datos de origen para que pueda comenzar el tiempo de inactividad de la	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	aplicación. Compruebe que AWS DMS haya completado la replicación de los datos en el proceso. Habilite los desencadenantes y claves externas en la instancia de base de datos de destino.	
Actualice las secuencias de la base de datos	Si la base de datos de origen contiene números de secuencia, compruebe y actualice las secuencias en la base de datos de destino.	Administrador de base de datos
Configure el punto de conexión de la aplicación.	Configure las conexiones de la aplicación para usar los nuevos puntos de conexión de la instancia de base de datos de Amazon RDS. La instancia de base de datos ya está cifrada.	Administrador de base de datos, propietario de la aplicación

Recursos relacionados

- Creación de una tarea de AWS DMS
- Supervisión de las tareas de replicación mediante Amazon CloudWatch
- Monitorización de tareas de AWS DMS
- Actualización de la clave de cifrado de Amazon RDS

Información adicional

Comprobar el cifrado de la instancia de base de datos PostgreSQL de origen:

Notas adicionales para este patrón:

- Habilite la replicación en PostgreSQL estableciendo el parámetro `rds.logical_replication` en 1.

Nota importante: las ranuras de replicación retienen los archivos de registro de escritura anticipada (WAL) hasta que los archivos se consumen externamente, por ejemplo, mediante `pg_recvlogical`, mediante trabajos de extracción, transformación y carga (ETL) o mediante AWS DMS. Al establecer el valor del parámetro `rds.logical_replication` en 1, AWS DMS establece los parámetros `wal_level`, `max_wal_senders`, `max_replication_slots` y `max_connections`. Si hay ranuras de replicación lógica pero no se consumen los archivos WAL retenidos por la ranura de replicación, es posible que aumente el uso del disco del registro de transacciones y disminuya el espacio de almacenamiento libre. Para obtener más información y los pasos para resolver este problema, consulte el artículo ¿Cómo puedo identificar la causa del error «No queda espacio en el dispositivo» o «» DiskFull en Amazon RDS for PostgreSQL? en el centro de conocimiento de AWS Support.

- Los cambios de esquema que realice en la instancia de base de datos de origen tras crear la instantánea de base de datos no quedarán reflejados en la instancia de base de datos de destino.
- Después de crear una instancia de base de datos encriptada, no puede cambiar la clave KMS utilizada por esa instancia de base de datos. Asegúrese de determinar los requisitos de su clave de KMS antes de crear la instancia de base de datos cifrada.
- Debe deshabilitar los desencadenantes y claves externas en la instancia de base de datos de destino antes de ejecutar la tarea de AWS DMS. Podrá volver a habilitarlos cuando se complete la tarea.

Imponga el etiquetado automático de las bases de datos de Amazon RDS en el lanzamiento

Entorno: producción	Tecnologías: bases de datos; nativo en la nube; seguridad, identidad, conformidad	Servicios de AWS: Amazon RDS; Amazon SNS; AWS CloudTrail; Amazon CloudWatch

Resumen

Amazon Relational Database Service (Amazon RDS) es un servicio web que facilita la configuración, el funcionamiento y la escala de una base de datos relacional en la nube de Amazon Web Services (AWS). Proporciona una capacidad rentable y de tamaño ajustable para una base de datos relacional estándar y se ocupa de las tareas de administración de bases de datos comunes.

Las etiquetas le permiten clasificar los recursos de AWS de diversas maneras. El etiquetado de bases de datos relacionales es útil cuando tiene muchos recursos en la cuenta y desea identificar rápidamente un recurso específico en función de las etiquetas. Puede utilizar etiquetas de Amazon RDS para añadir metadatos personalizados a las instancias de base de datos de RDS. Una etiqueta es una marca que consta de una clave y un valor definidos por el usuario. Le recomendamos que cree un conjunto de etiquetas coherente para satisfacer los requisitos de su organización.

Este patrón proporciona una CloudFormation plantilla de AWS que le ayuda a supervisar y etiquetar las instancias de base de datos de RDS. La plantilla crea un evento de Amazon CloudWatch Events que vigila el evento CloudTrail CreatedBInstance de AWS. (CloudTrail captura las llamadas a la API de Amazon RDS como eventos). Cuando detecta este evento, llama a una función de AWS Lambda que aplica automáticamente las claves de etiquetas y los valores que usted defina. La plantilla también envía una notificación de que la instancia ha sido etiquetada mediante Amazon Simple Notification Service (Amazon SNS).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.

- Un bucket de Amazon Simple Storage Service (Amazon S3) para cargar el código de Lambda.
- Una dirección de correo electrónico activa en la que recibir las notificaciones de etiquetado.

Limitaciones

- La solución admite los eventos CloudTrail CreatedBInstance. No crea notificaciones para ningún otro evento.

Arquitectura

Arquitectura de flujo de trabajo

Automatizar y escalar

- Puede utilizar la CloudFormation plantilla de AWS varias veces para distintas regiones y cuentas de AWS. Debe ejecutar la plantilla solo una vez en cada región o cuenta.

Herramientas

Servicios de AWS

- AWS CloudTrail: AWS CloudTrail es un servicio de AWS que le ayuda con la gobernanza, el cumplimiento y la auditoría operativa y de riesgos de su cuenta de AWS. Las acciones realizadas por un usuario, un rol o un servicio de AWS se registran como eventos en CloudTrail.
- Amazon CloudWatch Events: Amazon CloudWatch Events ofrece una transmisión casi en tiempo real de los eventos del sistema que describen los cambios en los recursos de AWS. CloudWatch Events se da cuenta de los cambios operativos a medida que se producen y toma las medidas correctivas necesarias, mediante el envío de mensajes en respuesta al entorno, la activación de funciones, la introducción de cambios y la recopilación de información sobre el estado.
- AWS Lambda: AWS Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo. Solo pagará por el tiempo de computación que consuma, no se aplican cargos cuando el código no se está ejecutando.

- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos altamente escalable que se puede utilizar para una amplia gama de soluciones de almacenamiento, incluidos sitios web, aplicaciones móviles, copias de seguridad y lagos de datos.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) es un servicio web que permite a las aplicaciones, los usuarios finales y los dispositivos enviar y recibir al instante notificaciones desde la nube.

Codigo

Este patrón incluye un adjunto con dos archivos:

- `index.zip` es un archivo comprimido que incluye el código de Lambda de este patrón.
- `rds.yaml`es una CloudFormation plantilla que despliega el código Lambda.

Consulte la sección Epics para obtener información sobre cómo usar estos archivos.

Epics

Implementar el código de Lambda

Tarea	Descripción	Habilidades requeridas
Cargue el código en un bucket de S3.	Cree un bucket de S3 nuevo o utilice un bucket de S3 ya existente para cargar el archivo adjunto `index.zip` (código de Lambda). Este bucket debe estar en la misma región de AWS que los recursos (instancias de base de datos de RDS) que desea supervisar.	Arquitecto de la nube
Implemente la plantilla CloudFormation .	Abra la consola de Cloudform ation en la misma región de AWS que el bucket de S3 e implemente el archivo	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	`rds.yaml` que se incluye en el archivo adjunto. En la siguiente Epic, proporcione los valores de los parámetros.	

Complete los parámetros de la CloudFormation plantilla

Tarea	Descripción	Habilidades requeridas
Proporcione el nombre del bucket de S3.	Escriba el nombre del bucket de S3 que ha creado o seleccionado en la primera Epic. Este bucket de S3 contiene el archivo.zip del código Lambda y debe estar en la misma región de AWS que CloudFormation la plantilla y las instancias de base de datos de RDS que desea supervisar.	Arquitecto de la nube
Proporcione la clave de S3.	Proporcione la ubicación del archivo .zip del código de Lambda en su bucket de S3, sin barras diagonales iniciales (por ejemplo, `index.zip` o `controls/index.zip`).	Arquitecto de la nube
Proporcione una dirección de correo electrónico.	Proporcione una dirección de correo electrónico activa en la que desee recibir notificac iones de infracciones.	Arquitecto de la nube
Especifique un nivel de registro.	Especifique el nivel de registro y el detalle. `Info` designa	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	mensajes informativos detallados sobre el progreso de la aplicación y solo debe usarse para la depuración. `Error` designa los eventos de error que aún podrían permitir que la aplicación siguiera ejecutándose. `Warning` designa situaciones potencial mente dañinas.	
Introduzca las claves y los valores de las etiquetas de sus instancias de base de datos de RDS.	Escriba las claves de etiqueta y los valores que desea aplicar automáticamente a la instancia de RDS. Para más información, consulte Etiquetar recursos de base de datos de Amazon en la documentación de AWS.	Arquitecto de la nube

Confirmar la suscripción

Tarea	Descripción	Habilidades requeridas
Confirme la suscripción de correo electrónico.	Cuando la CloudFormation plantilla se implementa correctamente, envía un mensaje de correo electrónico de suscripción a la dirección de correo electrónico que proporcionó. Debe confirmar esta suscripción de correo electrónico para recibir	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	notificaciones de cuando se han etiquetado sus instancias.	

Recursos relacionados

- Creación de un bucket (documentación de Amazon S3)
- Etiquetado de los recursos de Amazon RDS (documentación de Amazon Aurora)
- Carga de objetos (documentación de Amazon S3)
- Creación de una regla de CloudWatch eventos que se active en una llamada a la API de AWS mediante AWS CloudTrail (CloudWatch documentación de Amazon)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Estime el costo de una tabla de DynamoDB para la capacidad bajo demanda

Entorno: producción	Tecnologías: bases de datos; nativas en la nube; sin servidor; administración de costos	Servicios de AWS: Amazon DynamoDB

Resumen

Amazon DynamoDB es una base de datos transaccional NoSQL que proporciona una latencia de milisegundos de un solo dígito incluso a escala de petabytes. Esta oferta sin servidor de Amazon Web Services (AWS) se está haciendo popular debido a su rendimiento y escalabilidad consistentes. No es necesario aprovisionar la infraestructura subyacente. Su única tabla puede crecer hasta petabytes.

Con el modo de capacidad bajo demanda, usted paga por solicitud por las lecturas y escrituras de datos que la aplicación realiza en las tablas. Los cargos de AWS se basan en las unidades de solicitud de lectura (RRU) y las unidades de solicitud de escritura (WRU) acumuladas en un mes. DynamoDB supervisa el tamaño de la tabla de forma continua durante todo el mes para determinar los cargos de almacenamiento. Soporta copias de seguridad continuas con point-in-time-recovery (PITR). DynamoDB supervisa el tamaño de la tabla habilitada para PITR de forma continua durante todo el mes para determinar los cargos de la copia.

Para estimar el costo de DynamoDB para un proyecto, es importante calcular cuánto RRU, WRU y almacenamiento se consumirán en las diferentes etapas del ciclo de vida del producto. Para obtener una estimación aproximada de los costos, puede utilizar la Calculadora de precios de AWS, pero debe proporcionar un número aproximado de RRU, WRU y requisitos de almacenamiento para la tabla. Puede resultar difícil estimarlos al principio del proyecto. La Calculadora de precios de AWS no tiene en cuenta la tasa de crecimiento de los datos ni el tamaño de los elementos, ni el número de lecturas y escrituras de la tabla base y de los Índices secundarios globales (GSI) por separado. Para utilizar la calculadora de precios de AWS, debe estimar todos esos aspectos a fin de suponer cifras aproximadas de la WRU, la RRU y el tamaño del almacenamiento a fin de obtener una estimación de los costos.

Este patrón proporciona un mecanismo y una plantilla de Microsoft Excel reutilizable para estimar los factores de costo básicos de DynamoDB, como los costos de escritura, lectura, almacenamiento, copia de seguridad y recuperación, para el modo de capacidad bajo demanda. Es más detallada que la calculadora de precios de AWS y considera los requisitos de la tabla base y de los GSI de forma independiente. También tiene en cuenta la tasa de crecimiento mensual de los datos por artículo y prevé los costos para tres años.

Requisitos previos y limitaciones

Requisitos previos

- Conocimientos básicos de DynamoDB y diseño de modelos de datos de DynamoDB
- Conocimientos básicos sobre los precios de DynamoDB, WRU, RRU, almacenamiento y copia de seguridad y recuperación (para obtener más información, consulte Precios de la capacidad bajo demanda)
- Conocimiento de los datos, el modelo de datos y el tamaño de los elementos en DynamoDB
- Conocimiento de los GSI de DynamoDB

Limitaciones

- La plantilla proporciona un cálculo aproximado, pero no es adecuada para todas las configuraciones. Para obtener una estimación más precisa, debe medir el tamaño individual de cada elemento de la tabla base y de los GSI.
- Para obtener una estimación más precisa, debe tener en cuenta el número esperado de escrituras (insertar, actualizar y eliminar) y lecturas de cada elemento en un mes promedio.
- Este patrón permite estimar únicamente los costos de escritura, lectura, almacenamiento y copia de seguridad y recuperación para los próximos años, sobre la base de hipótesis de crecimiento fijo de los datos.

Herramientas

Servicios de AWS

- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.

Otras herramientas

- La Calculadora de precios de AWS es una herramienta de planificación basada en la web destinada a crear presupuestos para los casos de uso de AWS.

Prácticas recomendadas

Para ayudar a mantener los costos bajos, tenga en cuenta las siguientes prácticas recomendadas de diseño de DynamoDB.

- Diseño de claves de partición: utilice una clave de partición de alta cardinalidad para distribuir la carga de manera uniforme.
- Patrón de diseño de listas de adyacencia: utilice este patrón de diseño para la gestión one-to-many y many-to-many las relaciones.
- Índice disperso: utilice un índice disperso para sus GSI. Cuando crea un GSI, especifica una clave de partición y, de forma opcional, una clave de clasificación. Solo los elementos de la tabla base que contienen la clave de partición de GSI correspondiente aparecen en el índice disperso. Esto ayuda a mantener los GSI más pequeños.
- Sobrecarga de índices: utilice el mismo GSI para indexar varios tipos de elementos.
- Partición de escritura de GSI: particione de manera inteligente para distribuir los datos entre las particiones y realice consultas más rápidas y eficientes.
- Elementos grandes: solo almacene los metadatos dentro de la tabla, guarde el blob en Amazon S3 y guarde la referencia en DynamoDB. Divida los elementos grandes en varios elementos e indexe de manera eficiente mediante claves de clasificación.

A fin de conocer más prácticas recomendadas de diseño, consulte la Guía para desarrolladores de Amazon DynamoDB.

Epics

Extraiga la información de los artículos de su modelo de datos de DynamoDB

Tarea	Descripción	Habilidades requeridas
Obtener el tamaño del artículo.	1. Compruebe cuántos tipos diferentes de objetos vas a almacenar en su tabla. 2. Para calcular el tamaño de cada elemento en kilobytes, añada el tamaño de clave y valor de cada atributo. 3. Calcule el tamaño del elemento para una tabla base y para cada GSI.	Ingeniero de datos
Calcule el costo de escritura.	Para estimar el costo de escritura en el modo de capacidad bajo demanda, primero hay que medir cuántas WRUs se consumirá n en un mes. Para ello, debe tener en cuenta los siguientes factores: • Número de operaciones de creación, actualización y eliminación para cada elemento en un mes. • Número de GSI disponibles. Considere cada índice de forma independiente. • Tamaño medio de un elemento del índice	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	• Número de tiempos de sincronización en un índice • ¿Cuántas cosas nuevas (por ejemplo, componentes o productos) se añadirán a la tabla cada mes? La cantidad de elementos que se añaden puede variar cada mes, pero puede suponer una tasa de crecimiento media en función de sus modelos de negocio. Para obtener más información, consulte la sección Additiona l information (Información adicional).	

Tarea	Descripción	Habilidades requeridas
Calcule el costo de lectura.	Para estimar el costo de escritura en el modo de capacidad bajo demanda, primero hay que medir cuántas RRU se consumirá n en un mes. Para ello, debe tener en cuenta los siguientes factores: • Número de GSI disponibles. Considere cada índice de forma independiente. • Tamaño medio de un elemento del índice • Número medio de lecturas por producto al mes. • Número total de elementos disponibles (componentes o productos) en la tabla de DynamoDB.	Desarrollador de aplicaciones, ingeniero de datos

Tarea	Descripción	Habilidades requeridas
Calcule el tamaño y el costo del almacenamiento.	En primer lugar, calcule el requisito de almacenamiento mensual promedio en función del tamaño del artículo de la tabla. A continuación, calcule el costo de almacenamiento multiplicando el tamaño de almacenamiento por el precio por GB de almacenamiento de su región de AWS. Si ya ha introducido datos para estimar el costo de escritura, no es necesario que los vuelva a introduci r para calcular el tamaño de almacenamiento. De lo contrario, para estimar el tamaño de almacenamiento, debe tener en cuenta los siguientes factores: • Número de elementos de datos en un módulo (producto) según el diseño de la tabla. • Tamaño medio de los elementos en kilobytes. • Número de GSI disponibles. Considere cada índice de forma independiente. • Tamaño medio de un elemento del índice	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	• ¿Cuántas cosas nuevos productos se añadirán a la tabla cada mes? La cantidad de productos que se añaden puede variar cada mes, pero puede suponer una tasa de crecimiento media en función de sus modelos de negocio. En este ejemplo, se utiliza una media de 10 millones de productos nuevos cada mes.	

Introduzca la información del artículo y el objeto en la plantilla de Excel

Tarea	Descripción	Habilidades requeridas
Descargue la plantilla de Excel de la sección de adjuntos y ajústela para que se adapte a su tabla de casos de uso.	1. Descargue la plantilla de Excel. 2. Ajuste el módulo empresarial y los GSI en función del diseño de la tabla.	Ingeniero de datos
Introduzca la información en la plantilla de Excel.	1. Actualice la información del artículo en la hoja. Actualice los datos solo en las celdas naranjas. 2. Ajuste los números de los objetos: ¿cuánto se puede añadir a la tabla cada mes? 3. Actualice los precios de la WRU y la RRU por millón para su región de AWS.	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	4. Actualice los precios de almacenamiento y copias de seguridad por GB al mes para su región de AWS. 5. Actualice el precio de recuperación por GB para su región de AWS. En la plantilla, hay tres elementos o entidades: información, metadatos y relación. Hay dos GSI. Para su caso de uso, si necesita más elementos, cree filas nuevas. Si necesita más GSI, copie un bloque de GSI existente y péguelo para crear tantos bloques de GSI como lo vaya necesitando. A continuación, ajuste los cálculos de las columnas SUM y TOTAL.	

Recursos relacionados

Referencias

- Precios de Amazon DynamoDB para capacidad bajo demanda
- Calculadora de precios de AWS para DynamoDB
- Prácticas recomendadas para el diseño y la arquitectura con DynamoDB
- Introducción a DynamoDB

Guías y patrones

- Modelado de datos con Amazon DynamoDB
- Costos de almacenamiento estimados para una tabla de Amazon DynamoDB

Información adicional

Ejemplo de cálculo de costos de escritura

El diseño del modelo de datos de DynamoDB muestra tres elementos por producto y un tamaño medio de artículo de 4 KB. Al añadir un producto nuevo a la tabla base de DynamoDB, consume el número de elementos * (tamaño del elemento/unidad de escritura de 1 KB) = 3 * (4/1) = 12 WRU. En este ejemplo, si se escribe 1 KB, el producto consume 1 WRU.

Lea el ejemplo de cálculo de costos

Para obtener la estimación de la RRU, considere el promedio de cuántas veces se leerá cada elemento en un mes. Por ejemplo, el elemento de información se leerá, en promedio, 10 veces en un mes, el elemento de metadatos se leerá dos veces y el elemento de relación se leerá cinco veces. En la plantilla de ejemplo, la RRU total de todos los componentes = número de componentes nuevos creados al mes * RRU por componente al mes = 10 millones * 17 RRU = 170 millones de RRU cada mes.

Cada mes, se añadirán elementos nuevos (componentes o productos) y el número total de productos aumentará con el tiempo. Por lo tanto, los requisitos de RRU también aumentarán con el tiempo.

- Durante el primer mes, el consumo de RRU será de 170 millones.
- Durante el segundo mes, el consumo de RRU será 2 * 170 millones, es decir, 340 millones.
- Durante el primer mes, el consumo de RRU será de 3 * 170 millones, es decir, 510 millones.

El siguiente gráfico muestra una previsión mensual del consumo y los costos de la RRU.

Tenga en cuenta que los precios en el gráfico son solo ilustrativos. Para crear previsiones precisas para su caso de uso, consulte la página de precios de AWS y utilice esos precios en la hoja de Excel.

Ejemplos de cálculos de costos de almacenamiento, copia de seguridad y recuperación

El almacenamiento, la copia de seguridad y la restauración de DynamoDB están conectados entre sí. La copia de seguridad está conectada directamente con el almacenamiento y la recuperación está

directamente relacionada con el tamaño de la copia de seguridad. A medida que aumente el tamaño de la tabla, los costos correspondientes de almacenamiento, copia de seguridad y restauración aumentarán proporcionalmente.

Tamaño y costo del almacenamiento

El costo del almacenamiento aumentará con el tiempo en función de la tasa de crecimiento de los datos. Por ejemplo, supongamos que el tamaño medio de un componente o producto en la tabla base y en las GSI es de 11 KB y que cada mes se añadirán 10 millones de productos nuevos a la tabla de base de datos. En ese caso, el tamaño de la tabla de DynamoDB aumentará (11 KB * 10 millones) /1024/1024 = 105 GB al mes. El primer mes, el tamaño de almacenamiento de la tabla será de 105 GB, el segundo será de 105 + 105 = 210 GB, y así sucesivamente.

- Durante el primer mes, el costo del almacenamiento será de 105 GB * el precio de almacenamiento por GB para su región de AWS.
- Durante el segundo mes, el costo del almacenamiento será de 210 GB * el precio de almacenamiento por GB para su región.
- Durante el tercer mes, el costo del almacenamiento será de 315 GB * el precio de almacenamiento por GB para su región.

Para conocer el tamaño y el costo del almacenamiento para los próximos tres años, consulte la sección Tamaño del almacenamiento y previsión.

de la copia de seguridad

El costo de las copias de seguridad aumentará con el tiempo en función de la tasa de crecimiento de los datos. Al activar la copia de seguridad continua con point-in-time-recovery (PITR), los cargos por copia de seguridad continua se basan en una media de GB de almacenamiento al mes. En un mes natural, el tamaño medio de las copias de seguridad sería el mismo que el tamaño de almacenamiento de la tabla, aunque el tamaño real podría ser un poco diferente. Como se añadirán productos nuevos cada mes, el tamaño total de almacenamiento y el tamaño de las copias de seguridad aumentarán con el tiempo. Por ejemplo, durante el primer mes, el tamaño medio de las copias de seguridad de 105 GB podría aumentar a 210 GB durante el segundo mes.

- Durante el primer mes, el costo de la copia de seguridad será de 105 GB al mes * el precio de la copia de seguridad continua por GB para su región de AWS.
- Durante el segundo mes, el costo de la copia de seguridad será de 210 GB al mes * el precio de la copia de seguridad continua por GB para su región.

- Durante el tercer mes, el costo de la copia de seguridad será de 315 GB al mes * el precio de la copia de seguridad continua por GB para su región.
- … y así sucesivamente.

El costo de la copia de seguridad se incluye en el gráfico de la sección Previsión del tamaño y el costo del almacenamiento.

Costo de recuperación

Cuando realiza copias de seguridad continuas con la PITR habilitada, los cargos por la operación de recuperación se basan en el tamaño de la restauración. Cada vez que restaure, pagará en función de los gigabytes de datos restaurados. Si el tamaño de la tabla es grande y realiza la restauración varias veces en un mes, será costosa.

Para estimar el costo de la restauración, en este ejemplo se supone que se realiza una recuperación del PITR una vez al mes al final del mes. En el ejemplo, se utiliza el tamaño medio mensual de la copia de seguridad como tamaño de los datos de restauración de ese mes. Durante el primer mes, el tamaño medio de la copia de seguridad es de 105 GB, y para la recuperación al final del mes, el tamaño de los datos de restauración sería de 105 GB. Para el segundo mes, serían 210 GB, y así sucesivamente.

El costo de recuperación aumentará con el tiempo en función de la tasa de crecimiento de los datos.

- Durante el primer mes, el costo de recuperación será de 105 GB * el precio de recuperación por GB para su región de AWS.
- Durante el segundo mes, el costo de recuperación será de 210 GB * el precio de restauración por GB para su región.
- Durante el tercer mes, el costo de recuperación será de 315 GB * el precio de restauración por GB para su región.

Para obtener más información, consulte la pestaña Almacenamiento, copia de seguridad y recuperación de la plantilla de Excel y el gráfico de la siguiente sección.

Previsión del tamaño y los costos del almacenamiento

En la plantilla, el tamaño de almacenamiento facturable real se calcula restando 25 GB al mes de la capa gratuita de la clase de tabla estándar. En la hoja, obtendrá un gráfico de pronóstico dividido en valores mensuales.

El siguiente gráfico de ejemplo prevé el tamaño de almacenamiento mensual en GB, el costo de almacenamiento facturable, el costo de las copias de seguridad bajo demanda y el costo de recuperación para los próximos 36 meses naturales. Todos los costos están en USD. A partir del gráfico, queda claro que los costos de almacenamiento, copia de seguridad y recuperación aumentan proporcionalmente al aumento del tamaño del almacenamiento.

Tenga en cuenta que los precios en el gráfico son solo ilustrativos. Para crear previsiones precisas para su caso de uso, consulte la página de precios de AWS y utilice esos precios en la hoja de Excel.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Costos de almacenamiento estimados para una tabla de Amazon DynamoDB

Documento creado por Moinul Al-Mamun

Entorno: PoC o piloto	Tecnologías: bases de datos; macrodatos; gestión de costos; almacenamiento y copias de seguridad	Servicios de AWS: Amazon DynamoDB

Resumen

Amazon DynamoDB es una base de datos transaccional NoSQL que proporciona una latencia de milisegundos de un solo dígito incluso a escala de petabytes. Esta oferta sin servidor de Amazon Web Services (AWS) se está haciendo popular debido a su rendimiento y escalabilidad consistentes. No es necesario que aprovisione almacenamiento. Su única tabla puede crecer hasta petabytes.

DynamoDB supervisa el tamaño de la tabla de forma continua durante todo el mes para determinar los cargos de almacenamiento. A continuación, AWS le cobrará por el tamaño medio de almacenamiento en gigabytes. Cuanto más crezca su tabla con el tiempo, más crecerán sus costos de almacenamiento. Para calcular el coste de almacenamiento, puede utilizar la Calculadora de precios de AWS, pero debe proporcionar el tamaño aproximado de la tabla, incluidos los índices secundarios globales (GSI), que es muy difícil de estimar al principio del proyecto. Además, la calculadora de precios de AWS no tiene en cuenta la tasa de crecimiento de los datos.

Este patrón proporciona un mecanismo y una plantilla de Microsoft Excel reutilizable para calcular el tamaño y el coste del almacenamiento de DynamoDB. Considera los requisitos de almacenamiento para la tabla base y los GSI de forma independiente. Calcula el tamaño del almacenamiento teniendo en cuenta el tamaño de los elementos individuales y la tasa de crecimiento de los datos a lo largo del tiempo.

Para obtener una estimación, inserte dos datos en la plantilla:

- El tamaño del elemento individual en kilobytes para la tabla base y los GSI
- Cuántos objetos o productos nuevos se podrían añadir a la tabla, en promedio, en un mes (por ejemplo, 10 millones)

La plantilla generará un gráfico de previsión de costos y almacenamiento para los próximos tres años, como se muestra en el siguiente ejemplo.

Requisitos previos y limitaciones

Requisitos previos

- Conocimientos básicos de DynamoDB y del almacenamiento y los precios de DynamoDB
- Conocimiento de los datos, el modelo de datos y el tamaño de los elementos en DynamoDB
- Conocimiento de los índices secundarios globales (GSI) de DynamoDB

Limitaciones

- La plantilla proporciona un cálculo aproximado, pero no es adecuada para todas las configuraciones. Para obtener una estimación más precisa, debe medir el tamaño individual de cada elemento de la tabla base y de los GSI.
- Este patrón permite estimar únicamente el tamaño y los costos de almacenamiento para los próximos años, sobre la base de hipótesis de crecimiento fijo de los datos.

Herramientas

Servicios de AWS

- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.

Otras herramientas

- La Calculadora de precios de AWS es una herramienta de planificación basada en la web destinada a crear presupuestos para los casos de uso de AWS.

Epics

Extraiga la información de los artículos de su modelo de datos de DynamoDB

Tarea	Descripción	Habilidades requeridas
Obtener el tamaño del artículo.	1. Compruebe cuántos tipos diferentes de objetos vas a almacenar en su tabla. 2. Para calcular el tamaño de cada elemento en kilobytes, añada el tamaño de clave y valor de cada atributo. 3. Calcule el tamaño del elemento para una tabla base y para cada GSI.	Ingeniero de datos
Obtenga el número de objetos que se han agregado en un mes.	Calcule cuántos component es u objetos se añadirán a la tabla de DynamoDB, de media, en un mes.	Ingeniero de datos

Introduzca la información del artículo y el objeto en la plantilla de Excel

Tarea	Descripción	Habilidades requeridas
Descargue la plantilla de Excel de la sección de adjuntos y ajústela para que se adapte a su tabla de casos de uso.	1. Descargue la plantilla de Excel. 2. Ajuste el módulo empresari al y los GSI en función del diseño de la tabla.	Ingeniero de datos
Introduzca la información en la plantilla de Excel.	1. Actualice la información del artículo en la hoja.	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	2. Ajuste los números de los objetos: ¿cuánto se puede añadir a la tabla cada mes? 3. Actualice los precios de almacenamiento y copias de seguridad por GB al mes para su región de AWS.	

Recursos relacionados

- Precio de Amazon DynamoDB bajo demanda
- Calculadora de precios de AWS para DynamoDB

Información adicional

Tenga en cuenta que la plantilla adjunta solo prevé el tamaño y el coste del almacenamiento para la clase de tabla de almacenamiento estándar. En función de la previsión de los costos de almacenamiento y teniendo en cuenta el tamaño individual del artículo y la tasa de crecimiento del producto o del objeto, puede estimar lo siguiente:

- Costo de exportación de datos
- Precio de copias de seguridad y recuperación
- Requisitos de almacenamiento de datos.

Costo del almacenamiento de datos de Amazon DynamoDB

DynamoDB supervisa el tamaño de la tabla de forma continua durante todo el mes para determinar los cargos de almacenamiento. DynamoDB mide el tamaño de los datos facturables al agregar el tamaño de byte sin procesar de los datos y una capacidad de almacenamiento por elemento que depende de las características que haya habilitado. Para obtener más información, consulte la Guía para desarrolladores de DynamoDB.

El precio del almacenamiento de datos depende de la clase de tabla. Los primeros 25 GB almacenados cada mes son gratuitos si utiliza la clase de tabla estándar de DynamoDB. Para

obtener más información sobre los costos de almacenamiento de la clase de tabla estándar y la clase de tabla de acceso poco frecuente estándar en diferentes regiones de AWS, consulte Precios de la capacidad bajo demanda.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Calcule el tamaño del motor de Amazon RDS para una base de datos de Oracle mediante informes de AWR

Creado por Abhishek Verma (AWS) y Eduardo Valentim (AWS)

Entorno: producción	Origen: base de datos de Oracle	Destino: Amazon RDS o Amazon Aurora.
Tipo R: renovar arquitectura	Carga de trabajo: Oracle	Tecnologías: bases de datos; migración
Servicios de AWS: Amazon RDS; Amazon Aurora		

Resumen

Al migrar una base de datos de Oracle a Amazon Relational Database Service (Amazon RDS) o Amazon Aurora, el cálculo de la CPU, la memoria y las E/S del disco de la base de datos de destino es un requisito clave. Puede estimar la capacidad requerida de la base de datos de destino analizando los informes del repositorio automático de cargas de trabajo (AWR) de Oracle. Este patrón explica cómo utilizar los informes de AWR para estimar estos valores.

La base de datos de Oracle de origen puede estar en las instalaciones o alojada en una instancia de Amazon Elastic Compute Cloud (Amazon EC2) o puede ser una instancia de la base de datos de Amazon RDS para Oracle. La base de datos de destino puede ser cualquier base de datos de Amazon RDS o Aurora.

Nota: Las estimaciones de capacidad serán más precisas si el motor de base de datos de destino es Oracle. En el caso de otras bases de datos de Amazon RDS, el tamaño del motor puede variar debido a las diferencias en la arquitectura de la base de datos.

Le recomendamos que realice la prueba de rendimiento antes de migrar la base de datos de Oracle.

Requisitos previos y limitaciones

Requisitos previos

- Una licencia de Oracle Database Enterprise Edition y una licencia de Oracle Diagnostics Pack para descargar los informes de AWR.

Versiones de producto

- Todas las ediciones de bases de datos de Oracle para las versiones 11g (versiones 11.2.0.3.v1 y posteriores) y hasta 12.2, 18c y 19c.
- Este patrón no cubre Oracle Engineered Systems ni Oracle Cloud Infrastructure (OCI).

Arquitectura

Pila de tecnología de origen

Uno de los siguientes:

- Una base de datos de Oracle en las instalaciones
- Una base de datos de Oracle en una instancia EC2
- Una instancia de base de datos de Amazon RDS para Oracle

Pila de tecnología de destino

- Cualquier base de datos de Amazon RDS a Amazon Aurora.

Arquitectura de destino

Para obtener información sobre el proceso de migración completo, consulte el patrón Migración de una base de datos de Oracle a Aurora PostgreSQL mediante AWS DMS y AWS SCT.

Automatizar y escalar

Si tiene que migrar varias bases de datos de Oracle y desea utilizar métricas de rendimiento adicionales, puede automatizar el proceso siguiendo los pasos descritos en la entrada del blog Dimensionar correctamente las instancias de Amazon RDS a escala en función de las métricas de rendimiento de Oracle.

Herramientas

- El Repositorio automático de cargas de trabajo (AWR) de Oracle es un repositorio integrado en las bases de datos de Oracle. Recopila y almacena periódicamente los datos de actividad y carga de trabajo del sistema, que luego son analizados por el Monitor de diagnóstico automático de bases de datos (ADDM). AWR toma instantáneas de los datos de rendimiento del sistema periódicamente (de forma predeterminada, cada 60 minutos) y almacena la información (de forma predeterminada, hasta 8 días). Puede utilizar las vistas y los informes de AWR para analizar estos datos.

Prácticas recomendadas

- Para calcular las necesidades de recursos de la base de datos de destino, puede utilizar un único informe de AWR, varios informes de AWR o vistas de AWR dinámicas. Le recomendamos que utilice varios informes de AWR durante el período de máxima carga para estimar los recursos necesarios para gestionar esos picos de carga. Además, las vistas dinámicas proporcionan más puntos de datos que lo ayudan a calcular las necesidades de recursos con mayor precisión.
- Debe estimar las IOPS solo para la base de datos que planea migrar, no para otras bases de datos y procesos que utilizan el disco.
- Para calcular la cantidad de E/S que utiliza la base de datos, no utilice la información de la sección Perfil de carga del informe AWR. En su lugar, utilice la sección de perfiles de E/S, si está disponible, o vaya a la sección de estadísticas de actividad de la instancia y observe los valores totales de las operaciones físicas de lectura y escritura.
- Cuando estime el uso de la CPU, le recomendamos que utilice el método de métricas de la base de datos en lugar de las estadísticas del sistema operativo (SO), ya que se basa en la CPU que utilizan únicamente las bases de datos. (Las estadísticas del sistema operativo también incluyen el uso de la CPU por parte de otros procesos). También debería consultar las recomendaciones relacionadas con la CPU en el informe de ADDM para mejorar el rendimiento tras la migración.
- Tenga en cuenta los límites de rendimiento de E/S (rendimiento de Amazon Elastic Block Store (Amazon EBS) y rendimiento de red para el tamaño de instancia específico a la hora de determinar el tipo de instancia correcto.
- Realice la prueba de rendimiento antes de la migración para validar el tamaño del motor.

Epics

Crear un informe de AWR

Tarea	Descripción	Habilidades requeridas
Habilite el informe AWR.	Para activar el informe, siga las instrucciones de la documentación de Oracle.	Administrador de base de datos
Compruebe el periodo de retención.	Para comprobar el periodo de retención del informe AWR, utilice la siguiente consulta. `SQL> SELECT snap_interval,retention FROM dba_hist_wr_control;`	Administrador de base de datos
Genere la instantánea.	Si el intervalo de instantáneas de AWR no es lo suficientemente detallado como para captar el pico de carga de trabajo, puede generar el informe de AWR manualmente. Para generar la instantánea de AWR manual, utilice la siguiente consulta. `SQL> EXEC dbms_workload_repository.create_snapshot;`	Administrador de base de datos
Compruebe las instantáneas recientes.	Para comprobar las instantáneas de AWR recientes, utilice la siguiente consulta. `SQL> SELECT snap_id, to_char(begin_inte`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`rval_time,'dd/MON/yy hh24:mi') Begin_Interval, to_char(end_interval_time,'dd/MON/yy hh24:mi') End_Interval FROM dba_hist_snapshot ORDER BY 1;`	

Estime los requisitos de E/S del disco

Tarea	Descripción	Habilidades requeridas
Elija un método.	Las IOPS son la medida estándar de las operaciones de entrada y salida por segundo en un dispositivo de almacenamiento e incluyen las operaciones de lectura y escritura. Si va a migrar una base de datos en las instalaciones a AWS, debe determinar los picos de E/S de disco que utiliza la base de datos. Puede utilizar los siguientes métodos para estimar la E/S del disco de la base de datos de destino: • Sección de perfil de carga del informe AWR • Sección de estadísticas de actividad de instancias del informe AWR (utilice	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	esta sección para Oracle Database 12c o versiones posteriores) • Sección de perfiles de E/S del informe AWR (utilice esta sección para las versiones de Oracle Database anteriores a la 12c) • Vistas AWR Estos cuatro métodos se describen en los siguientes pasos.	

Tarea	Descripción	Habilidades requeridas
Opción 1: utilice el perfil de carga.	La siguiente tabla muestra un ejemplo de la sección Perfil de carga del informe AWR. Importante: para obtener información más precisa, le recomendamos que utilice la opción 2 (perfiles de E/S) o la opción 3 (estadísticas de actividad de la instancia) en lugar del perfil de carga. Por segu / Tran ón / Por ejecu / Por llamac Tiem s de base de datos / 26,6 / 0.2 / 0,00 / 0,02 CPU de base de datos / 18,0 / 0.1 / 0,00 / 0.01 CPU de fond / 0.2 / 0.0 / 0,00 / 0,00 Tam de / 2.45 ,9 / 17.0	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Redo (byte Lectu 3.37 23.4 lógic ,5 (bloq : Cam 21.6 150, en bloqu Lectu 13.5 94,4 física bloqu Escri 3.46 24,1 física (bloq : Leer 3.58 24,9 las solici es de E/ S: Solic 574, 4.0 es de escri IO: Leer 106. 0.7 E/	

Tarea	Descripción		Habilidades requeridas
	S (MB)		
	Escri E/ S (MB)	27,1	0.2
	Filas de esca de mens a insta ea:	0.0	0.0
	Mens a insta ea de lectu lógic de sesió		
	User calls	1.24	8.7
	Análi (SQL	4.62	32,2
	Análi duro (SQL	8.9	0.1

Tarea	Descripción	Habilidades requeridas
	Área de traba de SQL (MB) 824,9 5.7 Inicio de sesió 1.7 0.0 Ejecu (SQL 136.6 950,4 Reve : 22.9 0.2 Tran ones 143.8 En función de esta información, puede calcular las IOPS y el rendimiento de la siguiente manera: IOPS = solicitudes de lectura de E/S: + solicitudes de escritura de E/S = 3586,8 + 574,7 = 4134,5 Rendimiento = lectura física (bloques) + escritura física (bloques) = 13 575,1 + 3467,3 = 17 042,4	

Tarea	Descripción	Habilidades requeridas
	Como el tamaño del bloque en Oracle es de 8 KB, puede calcular el rendimiento total de la siguiente manera: El rendimiento total en MB es 17 042,4 * 8 * 1024 / 1024 / 1024 = 133,2 MB Advertencia: no utilice el perfil de carga para estimar el tamaño de la instancia. No es tan preciso como las estadísticas de actividad de las instancias o los perfiles de E/S.	

Tarea	Descripción	Habilidades requeridas
Opción 2: utilizar estadísticas de actividad de instancia.	Si utiliza una versión de la base de datos de Oracle anterior a la 12c, puede utilizar la sección de estadísticas de actividad de las instancias del informe AWR para estimar las IOPS y el rendimiento. En la tabla siguiente se muestra un ejemplo de esta sección. Estadística / Total / Por segun / por Trans lectura física total de solicitudes de E/S / 2.547..217 / 3.610, / 25,11 bytes totales de lectura física / 80.776.124.928 / 114,48 26,26 / 796.149 8 escritura física, total de solicitudes / 534.19 08 / 757,1 / 5.27	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	de E/S bytes totales de escritu física 25.517 8.849. 36.165 1,84 251.508 8 En función de esta informaci ón, puede calcular el total de IOPS y el rendimiento de la siguiente manera: TIOPS totales = 3610,28 + 757,11 = 4367 Mbps totales = 114 482 426,26 + 36 165 631,84 = 150 648 058,1 / 1024 / 1024 = 143 Mbps	

Tarea	Descripción	Habilidades requeridas
Opción 3: utilizar perfiles de E/S.	En la base de datos de Oracle 12c, el informe AWR incluye una sección de perfiles de E/S que presenta toda la información en una sola tabla y proporciona datos más precisos sobre el rendimiento de la base de datos. En la tabla siguiente se muestra un ejemplo de esta sección. Lectur + escritu por segun Lectur por segun Escritur s por segundo Solicit es por segun: 4.367, 3.610, 757,1 Solicit es de bases de datos: 4.161, 3.586, 574,7 Solicit es optimi as: 0.0 0.0 0.0	Administrador de base de datos

Tarea	Descripción			Habilidades requeridas
	Rehac solicitu es:	179,3	2.8	176,6
	Total (MB):	143.7	109,2	34,5
	Base de datos (MB):	133,1	106.1	27,1
	Total optimi: o (MB):	0.0	0.0	0.0
	Rehac (MB):	7.6	2.7	4.9
	Base de datos (bloqu :	17.042	13.575	3.467,3
	A través de Buffer Cache (bloqu :	5.898,	5.360,	537,6

Tarea	Descripción	Habilidades requeridas
	Directo 11.143 8.214, 2.929,7 (bloqu : En esta tabla se proporcio nan los siguientes valores de rendimiento e IOPS totales: Rendimiento = 143 MBPS (desde la quinta fila, denominada Total, segunda columna) IOPS = 4367,4 (desde la primera fila, denominada Solicitudes totales, segunda columna)	

Tarea	Descripción	Habilidades requeridas
Opción 4: utilizar vistas AWR.	Puede ver la misma información de IOPS y rendimiento mediante las vistas de AWR. Para obtener esta información, utilice la siguiente consulta: `break on report compute sum of Value on report select METRIC_NAME,avg(AVERAGE) as "Value" from dba_hist_sysmetric_summary where METRIC_NAME in ('Physical Read Total IO Requests Per Sec','Physical Write Total IO Requests Per Sec') group by metric_name;`	Administrador de base de datos

Calcule los requisitos de CPU

Tarea	Descripción	Habilidades requeridas
Elija un método.	Puede estimar la CPU necesaria para la base de datos de destino de tres maneras: • Mediante el uso de los núcleos disponibles reales del procesador • Mediante el uso de los núcleos utilizados según	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	las estadísticas del sistema operativo • Mediante el uso de los núcleos utilizados según las estadísticas Si está analizando los núcleos utilizados, le recomendamos que utilice el método de métricas de la base de datos en lugar de las estadísticas del sistema operativo, ya que se basa en la CPU que utilizan únicamente las bases de datos que planea migrar. (Las estadísticas del sistema operativo también incluyen el uso de la CPU por parte de otros procesos). También debería consultar las recomendaciones relacionadas con la CPU en el informe de ADDM para mejorar el rendimiento tras la migración. También puede estimar los requisitos en función de la generación de CPU. Si utiliza distintas generaciones de CPU, puede estimar la CPU necesaria para la base de datos de destino siguiendo las instrucciones del documento técnico Desmitificar el número	

Tarea	Descripción	Habilidades requeridas
	de vCPU para un rendimiento óptimo de la carga de trabajo.	

Tarea	Descripción	Habilidades requeridas
Opción 1: calcule los requisitos en función de los núcleos disponibles.	En informes AWR: • Las CPU se refieren a las CPU lógicas y virtuales. • Los núcleos son el número de procesadores de un chipset de CPU físico. • Un socket es un dispositivo físico que conecta un chip a una placa. Los procesadores multinúcleo tienen sockets con varios núcleos de CPU. Puede estimar los núcleos disponibles de dos maneras: • Mediante comandos utilizando el sistema operativo • Mediante el informe AWR Para estimar los núcleos disponibles mediante comandos del sistema operativo Utilice el siguiente comando para contar los núcleos del procesador. `$ cat /proc/cpuinfo | grep "cpu cores"|uniq` `cpu cores : 4`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`cat /proc/cpuinfo	egrep "core id|physical id"	tr -d "\n"	sed s/physical/\\nphysical/g	grep -v ^$	sort	uniq	wc -l`  Utilice el siguiente comando para contar los sockets del procesador.  `grep "physical id" /proc/cpuinfo	sort -u` `physical id : 0` `physical id : 1` Nota: No recomendamos utilizar comandos del sistema operativo, como nmon y sar, para extraer el uso de la CPU. Esto se debe a que esos cálculos incluyen el uso de la CPU por parte de otros procesos y es posible que no reflejen la CPU real que utiliza la base de datos. Para estimar los núcleos disponibles mediante el informe AWR También puede deducir el uso de la CPU de la primera sección del informe de AWR. A continuación se muestra un extracto del informe.	

Tarea	Descripción	Habilidades requeridas
	N DB Inst Inst Hor Rele Re d Id num de (Ver sió b inici d d X <DE XX) 1 05- 12.1 NO Sep 0 23:(Hos Plat CPU Núc Soc Mem Nar a (GB) <ho Linu 80 80 2 441,7 e> x86 64- bit En este ejemplo, el recuento de CPU es 80, lo que indica que se trata de CPU lógicas (virtuales). También puede ver que esta configuración tiene dos sockets, un procesado r físico en cada socket (para un total de dos procesado res físicos) y 40 núcleos para cada socket o procesador físico.	

<table>
<tr><th>Tarea</th><th>Descripción</th><th>Habilidades requeridas</th></tr>
<tr><td>Opción 2: Calcule el uso de la CPU mediante las estadísticas del sistema operativo.</td><td>Puede comprobar las estadísticas de uso de la CPU del sistema operativo directamente en el sistema operativo (mediante sar u otra utilidad del sistema operativo host) o revisando los valores de IDLE/(IDLE+BUSY) de la sección de estadísticas del sistema operativo del informe AWR. Puede ver los segundos de CPU consumidos directamente desde v$osstat. Los informes AWR y Statspack también muestran estos datos en la sección de estadísticas del sistema operativo.

Si hay varias bases de datos en el mismo cuadro, todas tienen los mismos valores de v$osstat para BUSY_TIME.

<table><tr><th>Estadística</th><th>Valor</th><th>Valor final</th></tr><tr><td>FREE_MEMORY_BYT</td><td>6.810.67.248</td><td>12.280.799.232</td></tr><tr><td>INACTIV MEMOR TES</td><td>175.627.33.632</td><td>160.380,653,568</td></tr><tr><td>SWAP_F _BYTES</td><td>17.145.64.336</td><td>17.145.872.384</td></tr></table></td><td>Administrador de base de datos</td></tr>
</table>

Tarea	Descripción		Habilidades requeridas
	BUSY_T	1.305.56 .937	
	IDLE_TI	4.312.71 .839	
	IOWAIT_ ME	53.417.1 4	
	NICE_TI	29.815	
	SYS_TIM	148.567. 70	
	USER_T	1.146.91 .783	
	LOAD	25	29
	VM_IN_E ES	593.920	
	VM_OUT TES	327.680	
	PHYSIC/ MEMOR TES	474.362. 17.152	
	NUM_CF	80	
	NUM_CF ORES	80	
	NUM_CF OCKETS	2	

Tarea	Descripción	Habilidades requeridas
	GLOBAL_RECEIVE_SIZE_MAX 4.194.304 GLOBAL_SEND_SIZE_MAX 2.097.152 TCP_RECEIVE_SIZE_DEFAULT 87.380 TCP_RECEIVE_SIZE_MAX 6.291.456 TCP_RECEIVE_SIZE_MIN 4.096 TCP_SEND_SIZE_DEFAULT 16.384 TCP_SEND_SIZE_MAX 4.194.304 TCP_SEND_SIZE_MIN 4.096 Si no hay otros consumidores importantes de CPU en el sistema, utilice la siguiente fórmula para calcular el porcentaje de uso de la CPU:	

Tarea	Descripción	Habilidades requeridas
	Utilización = tiempo de actividad / tiempo total Tiempo de actividad = requisitos = v$osstat.BUSY_TIME C = Tiempo total (actividad + inactivo) C = capacidad = v$ostat.BUSY_TIME + v$ostat.IDLE_TIME Utilización = BUSY_TIME / (BUSY_TIME + IDLE_TIME) = -1 305 569 937 / (1 305 569 937 + 4 312 718 839) = 23 % utilizado	

Tarea	Descripción	Habilidades requeridas
Opción 3: calcule el uso de la CPU mediante métricas de bases de datos.	Si hay varias bases de datos en ejecución en el sistema, puede utilizar las métricas de la base de datos que aparecen al principio del informe. Snap Id / Snap Time / Sess (Ses) / Curso sesión Inicia Snap 1846 28-Sep- 09:0(1226 35,8 Final Snap 1854 06-Oct-2 13:0(1876 41,1 Tran ido: 11 759,((minu Tiem de base de datos 312 625,4 (minu Para obtener las métricas de uso de la CPU, utilice esta fórmula: Uso de la CPU de la base de datos (% de la potencia de	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	la CPU disponible) = tiempo de CPU / NUM_CPUS / tiempo transcurrido donde el uso de la CPU se describe mediante el tiempo de CPU y representa el tiempo dedicado a la CPU, no el tiempo de espera a la CPU. Este cálculo da como resultado: = 312 625,40 / 11 759,64/80 = Se está utilizando el 33 % de la CPU Número de núcleos (33 %) * 80 = 26,4 núcleos Núcleos totales = 26,4 * (120 %) = 31,68 núcleos Puede usar el mayor de estos dos valores para calcular la utilización de la CPU de la instancia de base de datos Amazon RDS o Aurora. Nota: En IBM AIX, la utilizaci ón calculada no coincide con los valores del sistema operativo o de la base de datos. Estos valores coinciden en otros sistemas operativos.	

Calcule los requisitos de memoria

Tarea	Descripción	Habilidades requeridas
Calcule los requisitos de memoria mediante estadísticas de memoria.	Puede usar el informe AWR para calcular la memoria de la base de datos de origen y compararla con la base de datos de destino. También debe comprobar el rendimiento de la base de datos existente y reducir los requisitos de memoria para ahorrar costos o aumentar los requisitos para mejorar el rendimiento. Esto requiere un análisis detallado del tiempo de respuesta del AWR y del acuerdo de nivel de servicio (SLA) de la aplicación. Utilice la suma del uso del área global del sistema (SGA) y del área global del programa (PGA) de Oracle como uso de memoria estimado para Oracle. Añada un 20 por ciento adicional para que el sistema operativo determine un requisito de tamaño de memoria objetivo. En el caso de Oracle RAC, utilice la suma de la utilización de memoria estimada en todos los nodos RAC y reduzca la memoria total, ya que se almacena en bloques comunes.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	1. Compruebe las métricas en la tabla de porcentajes de eficiencia de las instancias. La tabla utiliza los siguiente s términos: • El Porcentaje de aciertos en el búfer es el porcentaj e de veces que se ha encontrado un bloque concreto en la memoria caché del búfer en lugar de realizar una E/S física. Para mejorar el rendimien to, procure alcanzar el 100 por ciento. • El Porcentaje de espera de búfer debe estar cerca del 100 por ciento. • El porcentaje de aciertos de bloqueo debe estar cerca del 100 por ciento. • El porcentaje de CPU que no se analiza es el porcentaje de tiempo de CPU que se dedica a actividades no relaciona das con el análisis. Este valor debe estar cerca del 100 por ciento. Porcentaje de eficiencia de las instancias (objetivo: 100 %)	

Tarea	Descripción				Habilidades requeridas
	% de esper de búfer:	99,99	NoWa % de rehac	100,00	
	% de aciert del búfer:	99,84	% de clasifi ción en memc	100,00	
	% de aciert de bibliot as:	748,7	% de anális suave	99,81	
	% de ejecu para analiz	96,61	% de aciert de cierre	100,00	
	Analiz CPU para analiz % transc ido:	72.73	% de CPU no analiz e:	99,21	

Tarea	Descripción	Habilidades requeridas
	% de aciert de caché flash: 0,00 En este ejemplo, todas las métricas son correctas, por lo que puede utilizar el SGA y el PGA para la base de datos existente como requisito de planificación de la capacidad. 2. Compruebe la sección de estadísticas de la memoria y calcule el SGA/PGA. Inicio Final Memoria del host (MB): 452.387 452.387,3 Uso de SGA (MB): 220 544,0 220 544,0 Uso de PGA (MB): 36.874,9 45.270,0	

Tarea	Descripción	Habilidades requeridas
	Memoria total de la instancia en uso = SGA + PGA = 220 GB + 45 GB = 265 GB Añada un 20 por ciento de búfer: Memoria total de la instancia = 1,2 * 265 GB = 318 GB Dado que SGA y PGA representan el 70 por ciento de la memoria del host, el requisito total de memoria es: Memoria total del host = 318/0,7 = 464 GB Nota: Al migrar a Amazon RDS para Oracle, el PGA y el SGA se calculan previamente en función de una fórmula predefinida. Asegúrese de que los valores precalculados se acerquen a sus estimaciones.	

Determine el tipo de instancia de base de datos de la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Determine el tipo de instancia de base de datos en función de las estimaciones de E/S, CPU y memoria del disco.	Según las estimaciones de los pasos anteriores, la capacidad de la base de datos Amazon RDS o Aurora de destino debería ser:	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	• 68 núcleos de CPU • 143 MBPS de rendimiento • 4367 IOPS para E/S de disco • 464 GB de memoria En la base de datos Amazon RDS o Aurora de destino, puede asignar estos valores al tipo de instancia db.r5.16x large, que tiene una capacidad de 32 núcleos, 512 GB de RAM y 13 600 Mbps de rendimiento. Para obtener más información, consulte la publicación del blog de AWS en el Tamaño adecuado de instancias de Amazon RDS a escala en función de las métricas de rendimiento de Oracle.	

Recursos relacionados

- Clase de instancia de base de datos Aurora (documentación de Amazon Aurora)
- Almacenamiento de instancias de base de datos de Amazon RDS (documentación de Amazon RDS)
- Herramienta AWS Miner (GitHub repositorio)

Exporte tablas de Amazon RDS para SQL Server a un bucket S3 mediante AWS DMS

Creado por Subhani Shaik (AWS)

Entorno: PoC o piloto	Origen: RDS	Destino: S3
Tipo R: N/D	Carga de trabajo: Microsoft	Tecnologías: bases de datos; nativo en la nube
Servicios de AWS: AWS DMS; Amazon RDS; Amazon S3; AWS Secrets Manager; AWS Identity and Access Management		

Resumen

Amazon Relational Database Service (Amazon RDS) para SQL Server no admite la carga de datos en otros servidores vinculados a un motor de base de datos en la nube de Amazon Web Services (AWS). En su lugar, puede utilizar AWS Database Migration Service (AWS DMS) para exportar tablas de Amazon RDS para SQL Server a un bucket de Amazon Simple Storage Service (Amazon S3), donde los datos estarán disponibles para otros motores de bases de datos.

AWS DMS le ayuda a migrar bases de datos a AWS de manera sencilla y segura. La base de datos de origen permanece totalmente operativa durante la migración, minimizando así el tiempo de inactividad de las aplicaciones que dependen de ella. AWS DMS puede migrar sus datos desde y hasta las bases de datos comerciales y de código abierto más utilizadas.

Este patrón utiliza AWS Secrets Manager al configurar los puntos de conexión de AWS DMS. Secrets Manager le ayuda a proteger los secretos necesarios para acceder a sus aplicaciones, servicios y recursos de TI. Puede utilizar el servicio para rotar, administrar y recuperar credenciales de bases de datos, claves de API y otros secretos durante todo su ciclo de vida. Los usuarios y las aplicaciones recuperan los secretos con una llamada a Secrets Manager, lo que reduce la necesidad de codificar información confidencial. Secrets Manager ofrece una rotación de secretos con una integración incorporada para Amazon RDS, Amazon Redshift y Amazon DocumentDB. Además,

el servicio se puede extender a otros tipos de secretos, incluidas las claves de API y los tokens de OAuth. Con Secrets Manager, puede controlar el acceso a los datos secretos mediante permisos detallados y auditar la rotación de secretos de forma centralizada para los recursos de la nube de AWS, los servicios de terceros y en las instalaciones.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un bucket de S3
- Una nube privada virtual (VPC)
- Una subred de base de datos
- Amazon RDS para SQL Server
- Un rol de AWS Identity and Access Management (IAM) con acceso (lista, obtención y colocación de objetos) al bucket S3 en nombre de la instancia de Amazon RDS.
- Secrets Manager para almacenar las credenciales de la instancia de RDS.

Arquitectura

Pila de tecnología

- Amazon RDS para SQL Server
- AWS DMS
- Amazon S3
- AWS Secrets Manager

Arquitectura de destino

En el siguiente diagrama, se muestra la arquitectura para importar datos de la instancia de Amazon RDS al bucket S3 con la ayuda de AWS DMS.

1. La tarea de migración de AWS DMS que se conecta a la instancia de Amazon RDS de origen a través del punto de conexión de origen

2. Copiar datos de la instancia de Amazon RDS de origen
3. La tarea de migración de AWS DMS que se conecta al bucket S3 de destino a través del punto de conexión de destino
4. Exportación de datos copiados al bucket S3 en formato CSV (valores separados por comas)

Herramientas

Servicios de AWS

- AWS Database Migration Service (AWS DMS) le permite migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- Amazon Relational Database Service (Amazon RDS) le ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Secrets Manager le permite reemplazar las credenciales codificadas en el código, incluidas las contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación.

Otros servicios

- Microsoft SQL Server Management Studio (SSMS) es una herramienta para administrar SQL Server, que incluye el acceso, la configuración y la administración de los componentes de SQL Server.

Epics

Configuración de la instancia de Amazon RDS para SQL Server

Tarea	Descripción	Habilidades requeridas
Cree la instancia de Amazon RDS para SQL Server.	1. Abra la consola de administración de AWS,	DBA, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
	elija RDS y utilice la opción de creación estándar para crear una instancia de Amazon RDS con la edición requerida, como SQL Server Express Edition, SQL Server Standard Edition o SQL Server Enterprise Edition. Para la versión, elija 2016 o posterior. 2. En Plantillas, seleccione Desarrollo/Pruebas.	
Configure las credenciales para la instancia.	1. Escriba el nombre de la instancia. 2. Proporcione un nombre de usuario y una contraseña para la instancia de Amazon RDS.	DBA, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
Configure la clase de instancia , el almacenamiento, el escalado automático y la disponibilidad.	1. Seleccione la clase de instancia de base de datos de la lista: clases Estándar, Optimizada para memoria y Ampliable. Elija el tipo de instancia de base de datos que asigne la capacidad computacional, de red y de memoria necesaria para las cargas de trabajo planificadas para esta instancia de base de datos. Para obtener más información, consulte la documentación de AWS. 2. Seleccione el tipo de almacenamiento de la lista: SSD de Uso general SSD de IOPS aprovisionadas o Magnético. Asigne el tamaño de almacenamiento predeterminado según sea necesario. 3. Seleccione Habilitar el escalado automático del almacenamiento para aumentar el almacenamiento de Amazon RDS en función de su planificación de capacidad. 4. AWS DMS admite una implementación Multi-AZ con una instancia de replicación. En caso de que	DBA, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
	se produzca una interrupción en la zona de disponibilidad, el hardware interno o la red, AWS DMS creará una instancia en espera y proporcionará alta disponibilidad (HA) mediante una conmutación por error automática a las réplicas en espera. En función del tamaño de la importación, seleccione la opción adecuada.	
Especifique la VPC, el grupo de subredes, el acceso público y el grupo de seguridad.	Seleccione la VPC, los grupos de subredes de base de datos y el grupo de seguridad de VPC según sea necesario para crear la instancia de Amazon RDS. Siga las prácticas recomendadas, por ejemplo: • No habilite el acceso público a la instancia de base de datos de RDS. • No utilice el CIDR 0.0.0.0/0 en los grupos de seguridad. • Utilice únicamente la dirección IP y los detalles del puerto necesarios para acceder a la instancia de RDS.	DBA, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
Configure la supervisión, el respaldo y el mantenimiento.	1. Especifique las opciones de copia de seguridad que desea. De forma predeterminada, las copias de seguridad están habilitadas con un periodo de retención de 7 días. 2. Elija la configuración adecuada de la ventana de actualización automática de la versión secundaria y de mantenimiento para aplicar las modificaciones o el mantenimiento pendientes a la base de datos por parte de Amazon RDS. 3. Seleccione Crear base de datos.	DBA, ingeniero DevOps

Configure la base de datos y los datos de ejemplo

Tarea	Descripción	Habilidades requeridas
Cree una tabla y cargue los datos del ejemplo.	En la nueva base de datos, cree una tabla. Utilice el código de ejemplo de la sección Información adicional para cargar los datos en la tabla.	DBA, ingeniero DevOps

Configuración de credenciales

Tarea	Descripción	Habilidades requeridas
Cree el secreto.	1. Abra la consola, seleccione Secrets Manager, y Almacenar un nuevo secreto. 2. Introduzca un nombre de usuario y una contraseña para la base de datos de Amazon RDS para SQL Server. Este secreto se utilizará para el punto de conexión de origen de AWS DMS.	DBA, ingeniero DevOps

Configure el acceso entre la base de datos y el bucket S3

Tarea	Descripción	Habilidades requeridas
Para crear un rol de IAM para acceder a Amazon RDS.	1. En la consola, elija IAM y cree un rol de IAM que dé a un bucket S3 acceso de lectura/escritura a Amazon RDS. 2. En Característica, seleccione Integración con S3.	DBA, ingeniero DevOps

Crear el bucket de S3

Tarea	Descripción	Habilidades requeridas
Crear el bucket S3.	Para guardar los datos de Amazon RDS para SQL Server, en la consola, elija S3 y, a continuación, elija Crear bucket. Asegúrese de que el bucket de S3 no sea de acceso público.	DBA, ingeniero DevOps

Configure el acceso entre AWS DMS y el bucket S3

Tarea	Descripción	Habilidades requeridas
Para crear un rol de IAM para que AWS DMS pueda acceder a Amazon S3.	Cree un rol de IAM que permita a AWS DMS enumerar, obtener y colocar objetos del bucket S3.	DBA, ingeniero DevOps

Configuración de AWS DMS

Tarea	Descripción	Habilidades requeridas
Cree el punto de conexión de origen de AWS DMS.	1. En la consola, elija Database Migration Service y elija Puntos de conexión. Cree el Punto de conexión de origen y active la casilla de verificación Seleccionar instancia de base de datos de RDS.	DBA, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
	2. Para el motor Origen, seleccione Microsoft SQL Server. 3. En Acceso a la base de datos de puntos de conexión, elija AWS Secrets Manager e introduzca el secreto y el rol de IAM que creó anteriormente, así como el nombre de la base de datos. 4. Pruebe el punto de conexión de origen.	
Crear un punto de conexión de destino de AWS DMS.	Cree el Punto de conexión de destino y seleccione Amazon S3 como Motor de destino. Proporcione el nombre del bucket S3 y el nombre de la carpeta del rol de IAM que creó anteriormente.	DBA, ingeniero DevOps
Crear una instancia de replicación de AWS DMS.	En la misma VPC, subred y grupo de seguridad, cree la instancia de replicación de AWS DMS. Para obtener más información acerca de las opciones de la clase de instancia, consulte la documentación de AWS.	DBA, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
Cree la tarea de migración de AWS DMS.	Para exportar los datos de Amazon RDS para SQL Server al bucket S3, cree una tarea de migración de base de datos. En tipo de migración, seleccione migrar datos existentes. Seleccione los puntos de conexión y la instancia de replicación de AWS DMS que creó.	DBA, ingeniero DevOps

Exporte los datos al bucket S3

Tarea	Descripción	Habilidades requeridas
Ejecute la tarea de migración de bases de datos de.	Para exportar los datos de la tabla de SQL Server, inicie la tarea de migración de la base de datos. La tarea exportará los datos de Amazon RDS para SQL Server al bucket S3 en formato CSV.	DBA, ingeniero DevOps

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Eliminación de recursos.	Para evitar incurrir en costos adicionales, utilice la consola para eliminar los recursos en el siguiente orden: 1. Tarea de migración 2. Instancia de replicación	DBA, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
	3. puntos de conexión 4. Bucket de S3 5. Instancia de base de datos	

Recursos relacionados

- AWS DMS
- Amazon S3
- Amazon RDS para SQL Server
- Integración de Amazon S3

Información adicional

Para crear la base de datos y la tabla y cargar los datos de ejemplo, utilice el siguiente código.

```
--Step1: Database creation in RDS SQL Server
CREATE DATABASE [Test_DB]
 ON  PRIMARY
( NAME = N'Test_DB', FILENAME = N'D:\rdsdbdata\DATA\Test_DB.mdf' , SIZE = 5120KB ,
 FILEGROWTH = 10%)
 LOG ON
( NAME = N'Test_DB_log', FILENAME = N'D:\rdsdbdata\DATA\Test_DB_log.ldf' , SIZE =
 1024KB , FILEGROWTH = 10%)
GO

--Step2: Create Table
USE Test_DB
GO
Create Table Test_Table(ID int, Company Varchar(30), Location Varchar(20))

--Step3: Load sample data.
USE Test_DB
GO
Insert into Test_Table values(1,'AnyCompany','India')
Insert into Test_Table values(2,'AnyCompany','USA')
Insert into Test_Table values(3,'AnyCompany','UK')
Insert into Test_Table values(4,'AnyCompany','Hyderabad')
```

```
Insert into Test_Table values(5,'AnyCompany','Banglore')
```

Gestionar bloques anónimos en instrucciones SQL dinámicas en Aurora PostgreSQL

Creado por anuradha chintha (AWS)

Entorno: PoC o piloto	Origen: Base de datos relacional	Destino: PostgreSQL
Tipo R: renovar arquitectura	Carga de trabajo: Oracle; código abierto	Tecnologías: Migración; bases de datos
Servicios de AWS: Amazon Aurora; Amazon RDS		

Resumen

Este patrón le muestra cómo evitar el error que se produce al gestionar bloques anónimos en instrucciones SQL dinámicas. Recibirá un mensaje de error cuando use la herramienta de conversión de esquemas de AWS para convertir una base de datos Oracle en una base de datos Aurora compatible con PostgreSQL. Para evitar el error, debe conocer el valor de una variable de enlace 0UT, pero no podrá conocer el valor de una variable de enlace 0UT hasta que ejecute la instrucción SQL. Este error se debe a que la herramienta de conversión de esquemas de AWS (AWS SCT) no entiende la lógica de la instrucción SQL dinámica. AWS SCT no puede convertir la instrucción SQL dinámica en código PL/SQL (es decir, funciones, procedimientos y paquetes).

Requisitos previos y limitaciones

Requisitos previos

- Cuenta de AWS activa
- Instancia de base de datos (DB) de Aurora PostgreSQL
- Amazon Relational Database Service (Amazon RDS) para la instancia de base de datos de Oracle
- Terminal interactiva de PostgreSQL (psql)
- SQL *Plus

- Esquema de `AWS_ORACLE_EXT` (parte del paquete de extensión AWS SCT) en la base de datos de destino
- Versión más reciente de la herramienta de conversión de esquemas de AWS (AWS SCT) y los controladores necesarios

Arquitectura

Pila de tecnología de origen

- Oracle Database 10g en las instalaciones y versiones posteriores

Pila de tecnología de destino

- PostgreSQL de Amazon Aurora
- Amazon RDS para PostgreSQL
- Herramienta de conversión de esquemas de AWS (AWS SCT)

Arquitectura de migración

El siguiente diagrama muestra cómo usar las variables de enlace 0UT de AWS SCT y Oracle para escanear el código de la aplicación en busca de instrucciones SQL integradas y convertir el código a un formato compatible que pueda usar una base de datos de Aurora.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Genere un informe de AWS SCT para la base de datos de origen usando Aurora PostgreSQL como base de datos de destino.
2. Identifique el bloque anónimo en el bloque de código SQL dinámico (por el que AWS SCT generó el error).
3. Convierta el bloque de código manualmente e impleméntelo en una base de datos de destino.

Herramientas

Servicios de AWS

- La edición Amazon Aurora compatible con PostgreSQL es un motor de base de datos relacional compatible con ACID, completamente administrado, que le permite configurar, administrar y escalar implementaciones de PostgreSQL.
- Amazon Relational Database Service (Amazon RDS) para Oracle ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS.
- La Herramienta de conversión de esquemas de AWS (AWS SCT) le ayuda a hacer previsibles las migraciones de bases de datos heterogéneas convirtiendo automáticamente el esquema de la base de datos de origen y la mayoría de los objetos de código de la base de datos a un formato compatible con la base de datos de destino.

Otras herramientas

- pgAdmin le permite conectarse e interactuar con su servidor de base de datos.
- Oracle SQL Developer es un entorno de desarrollo integrado que puede usar para desarrollar y gestionar bases de datos en Oracle Database. Puede usar SQL *Plus u Oracle SQL Developer para este patrón.

Epics

Configurar la base de datos de orgien de Oracle

Tarea	Descripción	Habilidades requeridas
Cree una instancia de Oracle en Amazon RDS o Amazon EC2.	Para crear una instancia de base de datos de Oracle en Amazon RDS, consulte Crear una instancia de base de datos de Oracle y conectarse a una base de datos en una instancia de base de datos en Oracle en la documentación de Amazon RDS. Para crear una instancia de base de datos de Oracle en Amazon Elastic Compute	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Cloud (Amazon EC2), consulte Amazon EC2 para Oracle en la documentación de Recomendaciones de AWS.	
Cree un esquema de base de datos y objetos para la migración.	Puede usar Amazon Cloud Directory para crear un esquema de base de datos. Para más información, consulte Crear un esquema en la documentación de Cloud Directory.	Administrador de base de datos
Configure los grupos de seguridad entrantes y salientes.	Para crear y configurar grupos de seguridad, consulte Controlar el acceso con grupos de seguridad en la documentación de Amazon RDS.	Administrador de base de datos
Confirme que la base de datos se está ejecutando.	Para comprobar el estado de su base de datos, consulte Visualizar los eventos de Amazon RDS en la documentación de Amazon RDS.	Administrador de base de datos

Configure la base de datos Aurora PostgreSQL de destino

Tarea	Descripción	Habilidades requeridas
Cree una instancia de Aurora PostgreSQL en Amazon RDS.	Para crear una instancia de Aurora PostgreSQL, consulte Crear un clúster de base de	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	datos y conectarse a una base de datos en un clúster de base de datos de Aurora PostgreSQL en la documentación de Amazon RDS.	
Configure un grupo de seguridad entrante y saliente.	Para crear y configurar grupos de seguridad, consulte Proporcionar acceso al clúster de base de datos en la VPC creando un grupo de seguridad en la documentación de Aurora.	Administrador de base de datos
Confirme que la base de datos Aurora PostgreSQL se está ejecutando.	Para comprobar el estado de su base de datos, consulte Visualizar los eventos de Amazon RDS en la documentación de Aurora.	Administrador de base de datos

Configure AWS SCT

Tarea	Descripción	Habilidades requeridas
Conectar AWS SCT a la base de datos de origen.	Para conectar AWS SCT a su base de datos de origen, consulte Conectar a PostgreSQL como fuente en la documentación de AWS SCT.	Administrador de base de datos
Conectar AWS SCT a la base de datos de destino.	Para conectar AWS SCT a su base de datos de destino, consulte ¿Qué es la la Herramienta de conversión de esquemas de AWS	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	(AWS SCT)? en la Guía del usuario de la la Herramienta de conversión de esquemas de AWS (AWS SCT).	
Convierta el esquema de la base de datos en AWS SCT y guarde el código convertid o automáticamente como archivo SQL.	Para guardar los archivos convertidos de AWS SCT, consulte Guardar y aplicar el esquema convertido en AWS SCT la Guía del usuario de la la Herramienta de conversión de esquemas de AWS (AWS SCT).	Administrador de base de datos

Migre el código

Tarea	Descripción	Habilidades requeridas
Obtenga el archivo SQL para la conversión manual.	En el archivo convertido de AWS SCT, extraiga el archivo SQL que requiere la conversió n manual.	Administrador de base de datos
Actualice el script.	Actualice manualmente el archivo SQL.	Administrador de base de datos

Recursos relacionados

- Amazon RDS
- Características de Amazon Aurora

Información adicional

En el siguiente ejemplo de código se muestra cómo configurar la base de datos de origen de Oracle:

```
CREATE or replace PROCEDURE calc_stats_new1 (
  a NUMBER,
  b NUMBER,
  result out NUMBER)
IS
BEGIN
result:=a+b;
END;
/
```

```
set serveroutput on ;

DECLARE
  a NUMBER := 4;
  b NUMBER := 7;
  plsql_block VARCHAR2(100);
  output number;
BEGIN
  plsql_block := 'BEGIN calc_stats_new1(:a, :b,:output); END;';
  EXECUTE IMMEDIATE plsql_block USING a, b,out output;
  DBMS_OUTPUT.PUT_LINE('output:'||output);

END;
```

En el siguiente ejemplo de código se muestra cómo configurar la base de datos de Aurora PostgreSQL de destino:

```
 w integer,
 x integer)
RETURNS integer
AS
$BODY$
DECLARE
begin
return w + x ;
end;
$BODY$
LANGUAGE  plpgsql;


CREATE OR REPLACE FUNCTION test_pg.init()
RETURNS void
```

```
AS
$BODY$
BEGIN
if aws_oracle_ext.is_package_initialized
      ('test_pg' ) then
      return;
    end if;
    perform aws_oracle_ext.set_package_initialized
      ('test_pg' );

PERFORM aws_oracle_ext.set_package_variable('test_pg', 'v_output', NULL::INTEGER);
PERFORM aws_oracle_ext.set_package_variable('test_pg', 'v_status', NULL::text);
END;
$BODY$
LANGUAGE  plpgsql;


DO $$
declare
v_sql text;
v_output_loc int;
a integer :=1;
b integer :=2;
BEGIN
perform  test_pg.init();
--raise notice 'v_sql %',v_sql;
execute 'do $a$ declare v_output_l int; begin select * from test_pg.calc_stats_new1('||
a||','||b||') into v_output_l;
PERFORM aws_oracle_ext.set_package_variable(''test_pg'', ''v_output'', v_output_l) ;
 end; $a$'  ;
v_output_loc := aws_oracle_ext.get_package_variable('test_pg', 'v_output');
raise notice 'v_output_loc %',v_output_loc;
END ;
$$
```

Gestionar las sobrecargadas funciones de Oracle en Aurora PostgreSQL

Creado por Sumana Yanamandra (AWS)

Entorno: PoC o piloto	Origen: base de datos de Oracle	Destino: Aurora (compatible con PostgreSQL)
Tipo R: redefinir la plataforma	Carga de trabajo: Oracle	Tecnologías: bases de datos; migración
Servicios de AWS: Amazon Aurora		

Resumen

El código que migre de una base de datos Oracle local a una edición compatible con PostgreSQL de Amazon Aurora puede incluir funciones sobrecargadas. Estas funciones tienen la misma definición, es decir, el mismo nombre de función y el mismo número y tipo de datos de los parámetros de entrada (`IN`), pero el tipo de datos o el número de parámetros de salida (`OUT`) pueden diferir.

Estas discordancias de parámetros pueden causar problemas en PostgreSQL, ya que es difícil determinar qué función ejecutar. Este patrón ilustra cómo gestionar las funciones sobrecargadas al migrar el código de la base de datos a una versión compatible con Aurora PostgreSQL.

Requisitos previos y limitaciones

Requisitos previos

- Una instancia de base de datos Oracle como base de datos de origen
- Una instancia de base de datos Aurora compatible con PostgreSQL como base de datos de destino (consulte las instrucciones en la documentación de Aurora)

Versiones de producto

- Oracle Database 9i o posterior

- Oracle SQL Developer versión 18.4.0.376
- Cliente pgAdmin 4
- Versión 11 o posterior compatible con Aurora PostgreSQL (consulte Identificación de versiones de Amazon Aurora PostgreSQL en la documentación de Aurora)

Herramientas

Servicios de AWS

- Amazon Aurora compatible con PostgreSQL es un motor de base de datos relacional completamente administrado que le permite configurar, administrar y escalar implementaciones de PostgreSQL.

Otras herramientas

- Oracle SQL Developer es un entorno de desarrollo integrado y gratuito para trabajar con SQL en bases de datos de Oracle, tanto en implementaciones tradicionales como en la nube.
- pgAdmin es una herramienta de gestión de código abierto para PostgreSQL. Proporciona una interfaz gráfica que permite crear, mantener y utilizar objetos de bases de datos.

Epics

Crear una función sencilla

Tarea	Descripción	Habilidades requeridas
Cree una función en PostgreSQL que tenga un parámetro de entrada y un parámetro de salida.	El siguiente ejemplo ilustra una función denominada `test_overloading` en Aurora PostgreSQL Compatible. Esta función tiene dos parámetros: un parámetro de texto de entrada y un parámetro de texto de salida.	Ingeniero de datos compatible con Aurora PostgreSQL

Tarea	Descripción	Habilidades requeridas
	`CREATE OR REPLACE FUNCTION public.test_overloading( str1 text, OUT str2 text) LANGUAGE 'plpgsql' COST 100 VOLATILE AS $BODY$ DECLARE BEGIN str2 := 'Success'; RETURN ; EXCEPTION WHEN others THEN RETURN ; END; $BODY$;`	
Ejecute la función en PostgreSQL.	Ejecute la función que creó en el paso anterior. `select public.test_overloading('Test');` El resultado debería ser el siguiente. `Success`	Ingeniero de datos compatible con Aurora PostgreSQL

Sobrecarga la función

Tarea	Descripción	Habilidades requeridas
Use el mismo nombre de función para crear una función sobrecargada en PostgreSQL.	Cree una función sobrecargada en Aurora compatible con PostgreSQL que utilice el mismo nombre de función que la función anterior. El siguiente ejemplo también tiene un nombre `test_overloading` , pero tiene tres parámetros: un parámetro de texto de entrada, un parámetro de texto de salida y un parámetro entero de salida. `CREATE OR REPLACE FUNCTION public.test_overloading( str1 text, OUT str2 text, OUT num1 integer) LANGUAGE 'plpgsql' COST 100 VOLATILE AS $BODY$ DECLARE str3 text; BEGIN str2 := 'Success'; num1 := 100; RETURN ; EXCEPTION WHEN others THEN`	Ingeniero de datos compatible con Aurora PostgreSQL

Tarea	Descripción	Habilidades requeridas
	`RETURN ;` `END;` `$BODY$;`	
Ejecute la función en PostgreSQL.	Al ejecutar esta función, se produce un error con el siguiente mensaje de error. `ERROR: cannot change return type of existing function` `HINT: Use DROP FUNCTION test_overloading(text) first.` Esto sucede porque Aurora, compatible con PostgreSQL, no admite la sobrecarga de funciones directamente. No puede identificar qué función ejecutar, porque el número de parámetros de salida es diferente en la segunda versión de la función, aunque los parámetros de entrada son los mismos.	Ingeniero de datos compatible con Aurora PostgreSQL

Aplique la solución alternativa

Tarea	Descripción	Habilidades requeridas
Añada INOUT al primer parámetro de salida.	Como solución alternativa, modifique el código de la función representando el	Ingeniero de datos compatible con Aurora PostgreSQL

Tarea	Descripción	Habilidades requeridas
	primer parámetro de salida como. INOUT `CREATE OR REPLACE FUNCTION public.test_overloading( str1 text, INOUT str2 text, OUT num1 integer) LANGUAGE 'plpgsql' COST 100 VOLATILE AS $BODY$ DECLARE str3 text; BEGIN str2 := 'Success'; num1 := 100; RETURN ; EXCEPTION WHEN others THEN RETURN ; END; $BODY$;`	

Tarea	Descripción	Habilidades requeridas
Ejecute la función revisada.	Ejecute la función que actualizó mediante la siguiente consulta. Se pasa un valor nulo como segundo argumento de esta función, ya que se ha declarado este parámetro `INOUT` para evitar el error. `select public.test_overloading('Test', null);` La función ahora se ha creado correctamente. `Success, 100`	Ingeniero de datos compatible con Aurora PostgreSQL
Valide los resultados.	Compruebe que el código con la función sobrecargada se haya convertido correctamente.	Ingeniero de datos compatible con Aurora PostgreSQL

Recursos relacionados

- Uso de Amazon Aurora PostgreSQL (documentación de Aurora)
- Sobrecarga de funciones en Oracle (documentación de Oracle)
- Sobrecarga de funciones en PostgreSQL (documentación de PostgreSQL)

Ayudar a reforzar el etiquetado en DynamoDB

Creado por Mansi Suratwala (AWS)

Entorno: producción	Tecnologías: bases de datos; nativo en la nube; seguridad, identidad, conformidad	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon CloudWatch; Amazon DynamoDB; AWS Lambda; Amazon SNS		

Resumen

Este patrón configura notificaciones automáticas cuando falta o se elimina una etiqueta predefinida de Amazon DynamoDB de un recurso de DynamoDB en la nube de Amazon Web Services (AWS).

DynamoDB es un servicio de bases de datos NoSQL totalmente administrado que proporciona un rendimiento rápido y predecible así como escalabilidad. DynamoDB le permite liberarse de la carga administrativa que supone operar y escalar una base de datos distribuida. Cuando utiliza DynamoDB, no tiene que preocuparse del aprovisionamiento, la instalación ni la configuración del hardware, ni tampoco de las tareas de replicación, aplicación de parches de software o escalado de clústeres.

El patrón utiliza una CloudFormation plantilla de AWS, que crea un evento de Amazon CloudWatch Events y una función de AWS Lambda. El evento busca cualquier información de etiquetado de DynamoDB nueva o existente mediante AWS. CloudTrail Si falta o se elimina una etiqueta predefinida, CloudWatch activa una función Lambda, que le envía una notificación del Amazon Simple Notification Service (Amazon SNS) informándole de la infracción.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un bucket de Amazon Simple Storage Service (Amazon S3) para el archivo .zip de Lambda que contiene el script de Python para ejecutar la función de Lambda

Limitaciones

- La solución solo funciona cuando se producen los `UntagResource` CloudTrail eventos `TagResource` or. No crea notificaciones para ningún otro evento.

Arquitectura

Pila de tecnología de destino

- Amazon DynamoDB
- AWS CloudTrail
- Amazon CloudWatch
- AWS Lambda
- Amazon S3
- Amazon SNS

Arquitectura de destino

Automatizar y escalar

Puede utilizar la CloudFormation plantilla de AWS varias veces para distintas regiones y cuentas de AWS. Debe ejecutar la plantilla solo una vez en cada región o cuenta.

Herramientas

Herramientas

- Amazon DynamoDB: DynamoDB es un servicio de base de datos NoSQL totalmente administrado que ofrece un rendimiento rápido y predecible, así como escalabilidad.
- AWS CloudTrail: CloudTrail es un servicio de AWS que le ayuda con la gobernanza, el cumplimiento y la auditoría operativa y de riesgos de su cuenta de AWS. Las acciones realizadas por un usuario, un rol o un servicio de AWS se registran como eventos en CloudTrail.
- Amazon CloudWatch Events: Amazon CloudWatch Events ofrece un flujo casi en tiempo real de eventos del sistema que describen los cambios en los recursos de AWS.

- AWS Lambda: Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos altamente escalable que se puede utilizar para una amplia gama de soluciones de almacenamiento, incluidos sitios web, aplicaciones móviles, copias de seguridad y lagos de datos.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) es un servicio web que permite a las aplicaciones, los usuarios finales y los dispositivos enviar y recibir al instante notificaciones desde la nube.

Codigo

- El archivo .zip del proyecto está disponible como adjunto.

Epics

Cómo definir el bucket de S3

Tarea	Descripción	Habilidades requeridas
Defina el bucket de S3.	En la consola de Amazon S3, seleccione o cree un bucket de S3 con un nombre único que no contenga barras diagonales iniciales . Este bucket de S3 alojará el archivo .zip de código de Lambda. El bucket de S3 debe estar en la misma región de AWS que el recurso de DynamoDB que se está monitoreando.	Arquitecto de la nube

Cómo cargar el código de Lambda en el bucket de S3

Tarea	Descripción	Habilidades requeridas
Cargue el código de Lambda en el bucket de S3.	Cargue el archivo .zip de código de Lambda que se proporciona en la sección Adjuntos en el bucket de S3. El bucket de S3 debe estar en la misma región de que el recurso de DynamoDB que se está supervisando.	Arquitecto de la nube

Implemente la CloudFormation plantilla de AWS

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation plantilla de AWS.	En la CloudFormation consola de AWS, implemente la CloudFormation plantilla de AWS que se proporciona en la sección de adjuntos. En la Epic siguiente, proporcione valores para los parámetros.	Arquitecto de la nube

Complete los parámetros de la CloudFormation plantilla de AWS

Tarea	Descripción	Habilidades requeridas
Ponga nombre al bucket de S3.	Escriba el nombre de bucket de S3 que ha creado o elegido en la primera Epic.	Arquitecto de la nube
Proporcione la clave de Amazon S3.	Proporcione la ubicación del archivo .zip del código de Lambda en su bucket de S3,	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	sin barras diagonales iniciales (por ejemplo, `<folder>/<file-name>.zip`).	
Facilitar una dirección de correo electrónico	Proporcione una dirección de correo electrónico activa en la que desea recibir las notificaciones de Amazon SNS.	Arquitecto de la nube
Defina el nivel de registro.	Defina el nivel y la frecuencia de registro de la función de Lambda. `Info` designa mensajes informativos detallados sobre el progreso de la aplicación. `Error` designa los eventos de error que aún podrían permitir que la aplicación siguiera ejecutándose. `Warning` designa situaciones potencialmente dañinas.	Arquitecto de la nube
Introduzca las claves de etiquetas de DynamoDB requeridas.	Asegúrese de que las etiquetas estén separadas por comas, sin espacios entre ellas (por ejemplo, `ApplicationId,CreatedBy,Environment,Organization`). El evento CloudWatch Events busca estas etiquetas y envía una notificación si no las encuentra .	Arquitecto de la nube

Confirmar la suscripción.

Tarea	Descripción	Habilidades requeridas
Confirmar la suscripción.	Cuando la plantilla se implementa correctamente, envía un correo electrónico de suscripción a la dirección de correo electrónico que proporcionaste. Para recibir notificaciones de infracciones, debes confirmar esta suscripción de correo electrónico.	Arquitecto de la nube

Recursos relacionados

- Crear un bucket de S3
- Carga de archivos en un bucket de S3
- Recursos de etiquetado en DynamoDB
- Crear una regla de CloudWatch eventos que se active en una llamada a la API de AWS mediante AWS CloudTrail

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Implemente recuperación de desastres entre regiones con AWS DMS y Amazon Aurora

Creado por Mark Hudson (AWS)

Entorno: producción	Tecnologías: bases de datos	Servicios de AWS: AWS DMS; Amazon RDS; Amazon Aurora

Resumen

Los desastres naturales o provocados por el hombre pueden suceder en cualquier momento y afectar a la disponibilidad de los servicios y cargas de trabajo que se ejecutan en una determinada región de Amazon Web Services (AWS). Para mitigar estos riesgos, debe desarrollar un plan de recuperación de desastres (DR) que incorpore las capacidades integradas entre regiones de los servicios de AWS. En el caso de servicios de AWS que no proporcionan funcionalidad entre regiones de forma inherente, el plan de DR también debe proporcionar una solución para gestionar la conmutación por error entre regiones de AWS.

Este patrón le guía a través de una configuración de recuperación de desastres que incluye dos clústeres de bases de datos de Amazon Aurora compatibles con MySQL en una única región. Para satisfacer los requisitos de DR, los clústeres de bases de datos están configurados para usar la característica de base de datos global de Amazon Aurora, con una única base de datos que abarca múltiples regiones de AWS. Una tarea de AWS Database Migration Service (AWS DMS) replica datos entre los clústeres de la región local. Sin embargo, AWS DMS actualmente no admite la conmutación por error de tareas entre regiones. Este patrón incluye los pasos necesarios para evitar esa limitación y configurar AWS DMS de forma independiente en ambas regiones.

Requisitos previos y limitaciones

Requisitos previos

- Regiones de AWS principales y secundarias seleccionadas, compatibles con bases de datos globales de Amazon Aurora.
- Dos clústeres de bases de datos independientes de Amazon Aurora compatible con MySQL en una sola cuenta en la región principal.
- Clase de instancia de base de datos db.r5 o superior (recomendada).

- Una tarea de AWS DMS en la región principal que realice una replicación continua entre los clústeres de bases de datos existentes.
- Recursos regionales de DR disponibles para satisfacer los requisitos de creación de instancias de bases de datos. Para obtener más información, consulte Uso de una instancia de base de datos en una VPC.

Limitaciones

- Para ver la lista completa de limitaciones de las bases de datos globales de Amazon Aurora, consulte Limitaciones de las bases de datos globales de Amazon Aurora.

Versiones de producto

- Amazon Aurora compatible con MySQL edición 5.7 o 8.0. Para obtener más información, consulte versiones de Amazon Aurora.

Arquitectura

Pila de tecnología de destino

- Clúster de base de datos global de Amazon Aurora compatible con MySQL
- AWS DMS

Arquitectura de destino

El siguiente diagrama muestra una base de datos global para dos regiones de AWS, una con las bases de datos principales y de informes y la replicación de AWS DMS, y otra con las bases de datos principales y de informadores secundarias.

Automatizar y escalar

Puede usar AWS CloudFormation para crear la infraestructura necesaria en la región secundaria, como la nube privada virtual (VPC), las subredes y los grupos de parámetros. También puede usar AWS CloudFormation para crear los clústeres secundarios en la región DR y añadirlos a la base de datos global. Si utilizó CloudFormation plantillas para crear los clústeres de bases de datos en la

región principal, puede actualizarlas o ampliarlas con una plantilla adicional para crear el recurso de base de datos global. Para obtener más información, consulte Crear un clúster de base de datos de Amazon Aurora con dos instancias de base de datos y Crear un clúster de base de datos global para Aurora MySQL.

Por último, puede crear las tareas de AWS DMS en las regiones principal y secundaria utilizándolas CloudFormation después de que se produzcan los eventos de conmutación por error y devolución. Para obtener más información, consulte. AWS::DMS::ReplicationTask

Herramientas

- Amazon Aurora: Amazon Aurora es un motor de base de datos relacional completamente administrado compatible con MySQL y PostgreSQL. Este patrón utiliza la edición de Amazon Aurora compatible con MySQL.
- Bases de datos globales de Amazon Aurora: las bases de datos globales de Amazon Aurora están diseñadas para aplicaciones distribuidas por todo el mundo. Una única base de datos global de Amazon Aurora puede abarcar varias regiones de AWS. Replica sus datos sin afectar al rendimiento de la base de datos. También facilita las lecturas locales rápidas con baja latencia en cada región, y proporciona recuperación de desastres en caso de interrupciones en toda la región.
- AWS DMS: AWS Database Migration Service (AWS DMS) ofrece migración puntual o replicación continua. La tarea de replicación continua mantiene sincronizadas las bases de datos de origen y destino. Una vez configurada, la tarea de replicación continua aplica de forma constante los cambios del origen al destino con una latencia mínima. Todas las funciones de AWS DMS, como la validación y las transformaciones de datos, están disponibles para cualquier tarea de replicación.

Epics

Prepare los clústeres de bases de datos existentes en la región principal

Tarea	Descripción	Habilidades requeridas
Modifique el grupo de parámetros del clúster de bases de datos.	En el grupo de parámetros del clúster de base de datos existente, active el registro binario a nivel de fila configurando el parámetro `binlog_format` en el valor de fila.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	AWS DMS requiere el registro binario a nivel de fila para las bases de datos compatibles con MySQL al realizar replicación continua o captura de datos de cambios (CDC). Para obtener más información, consulte Usar una base de datos compatible con MySQL gestionada por AWS como origen de AWS DMS.	

Tarea	Descripción	Habilidades requeridas
Actualice el período de retención del registro binario de la base de datos.	Con un cliente MySQL instalado en el dispositivo del usuario final o una instancia de Amazon Elastic Compute Cloud (Amazon EC2), ejecute el siguiente procedimiento almacenado por Amazon Relational Database Service (Amazon RDS) en el nodo de escritura del clúster de base de datos principal. XX indica el número de horas que se retienen los registros. `call mysql.rds_set_configuration('binlog retention hours', XX)` Confirme la configuración ejecutando el siguiente comando. `call mysql.rds_show_configuration;` Las bases de datos compatibles con MySQL administradas por AWS purgan los registros binarios lo antes posible. Por lo tanto, el período de retención debe ser lo suficientemente prolongado como para garantizar que los registros no se purguen antes de ejecutar la tarea de AWS	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	DMS. Un valor de 24 horas suele ser suficiente, pero deberá basarse en el tiempo necesario para configurar la tarea de AWS DMS en la región de DR.	

Actualice la tarea de AWS DMS existente en la región principal

Tarea	Descripción	Habilidades requeridas
Registre el ARN de la tarea de AWS DMS.	Use el nombre de recurso de Amazon (ARN) para obtener el nombre de tarea de AWS DMS. Lo usará posterior mente. Para recuperar el ARN de la tarea de AWS DMS, visualice la tarea en la consola o ejecute el siguiente comando. `aws dms describe-replication-tasks` Un registro de ARN tiene el siguiente aspecto. `arn:aws:dms:us-east-1:<accountid>:task:AN6HFFMPM246XOZVEUHCNSOVF7MQCLTOZUIRAMY` Los caracteres que aparecen tras los últimos dos puntos	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	corresponden al nombre de la tarea que se usará en un paso posterior.	
Modifique la tarea de AWS DMS existente para registrar el punto de control.	El punto de comprobación que AWS DMS crea contiene información para que el motor de replicación sepa el punto de recuperación del flujo de cambios. Para registrar la información del punto de control, siga estos pasos en la consola: 1. Detenga las tareas de AWS DMS. 2. Utilice el editor JSON en la tarea para establecer el TaskRecoveryTableEnabled parámetro en true. 3. Inicie las tareas de AWS DMS.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Valide la información del punto de control.	Con un cliente MySQL conectado al punto de conexión de escritura del clúster, consulte la nueva tabla de metadatos en el clúster secundario de base de datos para comprobar que existe y contiene la información del estado de la replicación. Ejecute el siguiente comando de la . `select * from awsdms_control.awsdms_txn_state;` El nombre de la tarea de ARN se encuentra en la columna `Task_Name` de esta tabla.	Administrador de base de datos

Amplíe ambos clústeres de Amazon Aurora a una región de DR

Tarea	Descripción	Habilidades requeridas
Cree una infraestructura base en la región de DR.	Cree los componentes básicos necesarios para la creación y acceso a los clústeres de Amazon Aurora: • Virtual Private Cloud (VPC) (Nube virtual privada [VPC]) • Subredes • Grupo de seguridad	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	• Listas de control de acceso a la red • Subnet group (Grupo de subredes) • DB Parameter Group (Grupo de parámetros de base de datos) • Grupo de parámetros de clúster de base de datos Asegúrese de que la configuración de ambos grupos de parámetros coincida con la configuración de la región principal.	
Agregue la región de DR a ambos clústeres de Amazon Aurora.	Agregue una región secundaria (la región de DR) a los clústeres principales y secundarios de Amazon Aurora. Para mayor información, consulte Cómo agregar una región AWS a una base de datos global de Amazon Aurora.	Administrador de AWS

Realice una conmutación por error

Tarea	Descripción	Habilidades requeridas
Detenga las tareas de AWS DMS.	La tarea de AWS DMS en la región principal no funcionará correctamente tras la conmutación por error, y	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	deberá detenerla para evitar errores.	
Realice una conmutación por error gestionada.	Realice una conmutación por error gestionada del clúster de base de datos principal a la región de DR. Para instrucciones, consulte Ejecución de la conmutación por error planificada administrada para bases de datos globales de Amazon Aurora. Una vez finalizada la conmutación por error en el clúster de base de datos principal, realice la misma operación en el clúster de base de datos secundaria.	Administrador de AWS, administrador de base de datos
Cargue los datos en la base de datos principal.	Inserte los datos de prueba en el nodo de escritura de la base de datos principal del clúster de base de datos de DR. Estos datos se usarán para validar el correcto funcionamiento de la replicación.	Administrador de base de datos
Cree una instancia de replicación de AWS DMS.	Para crear la instancia de replicación de AWS DMS en la región de DR, consulte Crear una instancia de replicación.	Administrador de AWS, administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree los puntos de conexión de AWS DMS de origen y de destino.	Para crear los puntos de conexión de origen y destino de AWS DMS en la región de DR, consulte Crear puntos de conexión de origen y destino. El origen debe apuntar a la instancia de escritura del clúster de la base de datos principal. El origen debe apuntar a la instancia de escritura del clúster de la base de datos principal.	Administrador de AWS, administrador de base de datos
Obtenga el punto de control de replicación.	Para obtener el punto de control de replicación, consulte la tabla de metadatos con un cliente MySQL ejecutando la siguiente operación en el nodo de escritura del clúster de base de datos secundaria de la región de DR. `select * from awsdms_control.awsdms_txn_state;` En la tabla, busque el valor task_name que corresponde al ARN de la tarea de AWS DMS en la región principal que obtuvo en la segunda épica.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree una tarea de AWS DMS.	Desde la consola, cree una tarea de AWS DMS en la región de DR. En la tarea, especifique un método de migración para replicar únicamente los cambios de datos. Para obtener más información, consulte Crear una tarea. 1. En la configuración de la tarea, use el asistente para especificar lo siguiente: • Modo de inicio de CDC para transacciones de origen: habilite el modo de inicio de CDC personalizado • Punto de inicio de CDC personalizado para transacciones de origen: especifique un punto de control de recuperación 2. En la casilla Punto de control de recuperación, introduzca en la tabla `awsdms_txn_state` el valor del punto de control de replicación obtenido previamente mediante la consulta a la base de datos. 3. En la sección de configura ción de la tarea, selecciona	Administrador de AWS, administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	el editor JSON y establece el TaskRecoveryTableEnabledparámetro en true. Establezca la configuración Iniciar tarea de migración de la tarea de AWS DMS en Automáticamente al crear.	
Registre el ARN de la tarea de AWS DMS.	Utilice el ARN para obtener el nombre de la tarea tarea de AWS DMS para uso posterior . Para recuperar el ARN de la tarea de AWS DMS, ejecute el siguiente comando. `aws dms describe-replication-tasks`	Administrador de AWS, administrador de base de datos
Valide los datos replicados.	Consulte el clúster de base de datos secundaria en la región de DR para confirmar que los datos de prueba que cargó en el clúster de base de datos principal se han replicado.	Administrador de base de datos

Realice una conmutación por recuperación

Tarea	Descripción	Habilidades requeridas
Detenga las tareas de AWS DMS.	La tarea de AWS DMS en la región DR no funcionará correctamente tras la conmutación por error, y	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	deberá detenerla para evitar errores.	
Realice una conmutación por error gestionada.	Realice una conmutación por error el clúster de base de datos principal de la región principal. Para instrucciones, consulte Ejecución de la conmutación por error planificada administrada para bases de datos globales de Amazon Aurora. Una vez finalizada la conmutación por error en el clúster de la base de datos principal, realice la misma operación en el clúster de base de datos.	Administrador de AWS, administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Obtenga el punto de control de replicación.	Para obtener el punto de control de replicación, consulte la tabla de metadatos con un cliente MySQL ejecutando la siguiente operación en el nodo de escritura del clúster de base de datos secundaria de la región de DR. `select * from awsdms_control.awsdms_txn_state;` En la tabla, busque el valor `task_name` que corresponde al ARN de la tarea de AWS DMS en la región DR que obtuvo en la cuarta épica.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Actualice los puntos de conexión de origen y de destino de AWS DMS.	Una vez conmutados por error los clústeres de bases de datos, compruebe los clústeres de la región principal para determinar qué nodos son las instancias de escritura . A continuación, compruebe que los puntos de conexión de origen y destino de AWS DMS existentes en la región principal apunten a las instancias de escritura. Si no es así, actualice los puntos de conexión con los nombres del sistema de nombres de dominio (DNS) de la instancia de escritura.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Cree una tarea de AWS DMS.	Utilizando la consola, cree una tarea de AWS DMS en la región principal. En la tarea, especifique un método de migración para replicar únicamente los cambios de datos. Para obtener más información, consulte Crear una tarea. 1. En la configuración de tareas, use el asistente para especificar lo siguiente: • Modo de inicio de CDC para transacciones de origen: habilite el modo de inicio de CDC personalizado • Punto de inicio de CDC personalizado para transacciones de origen: especifique un punto de control de recuperación 2. En la casilla Punto de control de recuperación, introduzca en la tabla `awsdms_txn_state` el valor del punto de control de replicación obtenido previamente mediante la consulta a la base de datos.	Administrador de AWS, administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	3. También en la sección de configuración de tareas, selecciona el editor JSON y establece el TaskRecoveryTableEnabledparámetro en true. 4. Finalmente, establezca la tarea de AWS DMS Iniciar tarea de migración a Crear automáticamente.	
Registre el nombre de recurso de Amazon (ARN) de la tarea AWS DMS.	Utilice el ARN para obtener el nombre de la tarea tarea de AWS DMS para uso posterior . Para recuperar el ARN de tarea de AWS DMS, ejecute el siguiente comando: `aws dms describe-replication-tasks` Necesitará el nombre de la tarea cuando realice otra conmutación por error gestionada o en un escenario de DR.	Administrador de AWS, administrador de base de datos
Elimine las tareas de AWS DMS.	Elimine la tarea de AWS DMS original (actualmente detenida) en la región principal y la tarea de AWS DMS existente (actualmente detenida) en la región secundaria.	Administrador de AWS

Recursos relacionados

- Configuración de su clúster de base de datos de Amazon Aurora
- Uso de bases de datos globales de Amazon Aurora
- Trabajar con Amazon Aurora MySQL
- Trabajar con una instancia de replicación de AWS DMS
- Trabajar con puntos de conexión de AWS DMS
- Trabajar con tareas de AWS DMS
- ¿Qué es AWS CloudFormation?

Información adicional

En este ejemplo de DR se usan bases de datos globales de Amazon Aurora, ya que proporcionan un objetivo de tiempo de recuperación (RTO) efectivo de 1 segundo y un objetivo de punto de recuperación (RPO) de menos de 1 minuto, ambos inferiores a los de las soluciones replicadas tradicionales e ideales para escenarios de DR.

Las bases de datos globales de Amazon Aurora ofrecen muchas otras ventajas, entre las que se incluyen las siguientes:

- Lecturas globales con latencia local: los consumidores globales pueden acceder a la información en una región local y con latencia local.
- Clústeres de base de datos Amazon Aurora secundarios escalables: los clústeres secundarios se pueden escalar de forma independiente, y es posible añadir hasta 16 réplicas de solo lectura.
- Replicación rápida de clústeres de base de datos Aurora primarios a secundarios – La replicación realizada tiene poco impacto en el clúster principal. Se produce en la capa de almacenamiento, con latencias típicas de replicación entre regiones de menos de 1 segundo.

Este patrón también emplea AWS DMS para la replicación. Las bases de datos de Amazon Aurora ofrecen la posibilidad de crear réplicas de lectura, lo que puede simplificar el proceso de replicación y la configuración de DR. AWS DMS suele usarse para replicar cuando es necesario transformar los datos, o cuando la base de datos de destino requiere índices adicionales que la base de datos de origen no contiene.

Migre funciones y procedimientos de Oracle con más de 100 argumentos a PostgreSQL

Creado por Srinivas Potlachervoo (AWS)

Entorno: PoC o piloto	Origen: Oracle	Destino: PostgreSQL
Tipo R: redefinir la plataforma	Carga de trabajo: código abierto; Oracle	Tecnologías: Migración; bases de datos
Servicios de AWS; Amazon RDS; Amazon Aurora		

Resumen

Este patrón muestra cómo migrar funciones y procedimientos de Oracle Database que tienen más de 100 argumentos a PostgreSQL. Por ejemplo, puede usar este patrón para migrar funciones y procedimientos de Oracle a uno de los siguientes servicios de bases de datos de AWS compatibles con PostgreSQL:

- Amazon Relational Database Service (Amazon RDS) para PostgreSQL
- Edición compatible con Amazon Aurora PostgreSQL

PostgreSQL no admite funciones o procedimientos que tengan más de 100 argumentos. Como solución alternativa, puede definir un nuevo tipo de datos cuyos campos de tipo coincidan con los argumentos de la función de origen. A continuación, puede crear y ejecutar una función PL/pgSQL que use el tipo de datos personalizado como argumento.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una instancia de base de datos (DB) Oracle de Amazon RDS
- Una instancia de base de datos Amazon RDS para PostgreSQL o una instancia de base de datos Aurora compatible con PostgreSQL

Versiones de producto

- Instancia de base de datos Oracle de Amazon RDS, versión 10.2 y posteriores
- Instancia de base de datos Amazon RDS PostgreSQL, versión 9.4 y posteriores, o instancia de base de datos Aurora compatible con PostgreSQL, versión 9.4 y posteriores
- Oracle SQL Developer versión 18 y posteriores
- pgAdmin versión 4 y posteriores

Arquitectura

Pila de tecnología de origen

- Instancia de base de datos Oracle de Amazon RDS, versión 10.2 y posteriores

Pila de tecnología de destino

- Instancia de base de datos Amazon RDS PostgreSQL, versión 9.4 y posteriores, o instancia de base de datos Aurora compatible con PostgreSQL, versión 9.4 y posteriores

Herramientas

Servicios de AWS

- Amazon Relational Database Service (Amazon RDS) para PostgreSQL le ayuda a configurar, utilizar y escalar una base de datos relacional de PostgreSQL en la nube de AWS.
- La edición Amazon Aurora compatible con PostgreSQL es un motor de base de datos relacional compatible con ACID, completamente administrado, que le permite configurar, administrar y escalar implementaciones de PostgreSQL.

Otros servicios

- Oracle SQL Developer es un entorno de desarrollo integrado que simplifica el desarrollo y la administración de bases de datos de Oracle, tanto en implementaciones tradicionales como en implementaciones basadas en la nube.
- pgAdmin es una herramienta de gestión de código abierto para PostgreSQL. Proporciona una interfaz gráfica que permite crear, mantener y utilizar objetos de bases de datos.

Prácticas recomendadas

Asegúrese de que el tipo de datos creado coincida con los campos de tipos que se incluyen en la función o procedimiento de Oracle de origen.

Epics

Ejecute una función o procedimiento de Oracle con más de 100 argumentos

Tarea	Descripción	Habilidades requeridas
Cree o identifique una función o procedimiento de Oracle/PLSQL existente que tenga más de 100 argumentos.	Crear una función o procedimiento de Oracle/PLSQL con más de 100 argumentos. -o bien- Identifique una función o procedimiento Oracle/PLSQL existente que tenga más de 100 argumentos. Para obtener más información, consulte las secciones 14.7 Instrucción CREATE FUNCTION y 14.11 Instrucción CREATE PROCEDURE de la documentación de bases de datos de Oracle.	Conocimientos de Oracle/PL/SQL
Compilar la función o procedimiento de Oracle/PLSQL.	Compilar la función o procedimiento de Oracle/PLSQL. Para más información, consulte Compilación de una función en la documentación de la base de datos de Oracle.	Conocimientos de Oracle/PL/SQL

Tarea	Descripción	Habilidades requeridas
Ejecute la función de Oracle/PLSQL.	Ejecutar la función o procedimiento de Oracle/PLSQL. A continuación, guarde el resultado.	Conocimientos de Oracle/PL/SQL

Defina un nuevo tipo de datos que coincida con los argumentos de la función o procedimiento de origen

Tarea	Descripción	Habilidades requeridas
Defina un nuevo tipo de datos en PostgreSQL.	Defina un nuevo tipo de datos en PostgreSQL que incluya todos los campos que aparecen en los argumentos de la función o procedimiento de Oracle de origen. Para obtener más información, consulte CREATE TYPE en la documentación de PostgreSQL.	Conocimientos de PostgreSQL PL/pgSQL

Cree una función de PostgreSQL que incluya el nuevo argumento TYPE

Tarea	Descripción	Habilidades requeridas
Cree una función de PostgreSQL que incluya el nuevo tipo de datos.	Crear una función de PostgreSQL que incluya el nuevo argumento `TYPE`. Para ver un ejemplo de función, consulte la sección de Información adicional de este patrón.	Conocimientos de PostgreSQL PL/pgSQL

Tarea	Descripción	Habilidades requeridas
Compile la función PostgreSQL.	Compile la función en PostgreSQL. Si los campos del nuevo tipo de datos coinciden con los argumentos de la función o procedimiento de origen, la función se compilará correctamente.	Conocimientos de PostgreSQL PL/pgSQL
Ejecute la función de PostgreSQL.	Ejecute la función de PostgreSQL.	Conocimientos de PostgreSQL PL/pgSQL

Solución de problemas

Problema	Solución
La función devuelve el siguiente error: ERROR: error de sintaxis junto a “<statement>”	Asegúrese de que todas las instrucciones de la función terminen con punto y coma (`;`).
La función devuelve el siguiente error: ERROR: “<variable>” no es una variable conocida	Asegúrese de que la variable empleada en el cuerpo de la función aparezca en la sección `DECLARE` de la función.

Recursos relacionados

- Uso de Amazon Aurora PostgreSQL (Guía del usuario de Amazon Aurora para Aurora)
- CREATE TYPE (documentación de PostgreSQL)

Información adicional

Ejemplo de función PostgreSQL que incluye un argumento TYPE

```
CREATE OR REPLACE FUNCTION test_proc_new
```

```
(
    IN p_rec type_test_proc_args
)
RETURNS void
AS
$BODY$
BEGIN

    /*
    **************
    The body would contain code to process the input values.
    For our testing, we will display couple of values.
    ***************
    */
    RAISE NOTICE USING MESSAGE = CONCAT_WS('', 'p_acct_id: ', p_rec.p_acct_id);
    RAISE NOTICE USING MESSAGE = CONCAT_WS('', 'p_ord_id: ', p_rec.p_ord_id);
    RAISE NOTICE USING MESSAGE = CONCAT_WS('', 'p_ord_date: ', p_rec.p_ord_date);

END;
$BODY$
LANGUAGE plpgsql
COST 100;
```

Migrar las instancias de base de datos de Amazon RDS para Oracle a otras cuentas que usen AMS

Documento creado por Pinesh Singal (AWS)

Entorno: PoC o piloto	Origen: bases de datos: relacionales	Destino: Amazon RDS para Oracle en AWS Managed Services
Tipo R: volver a alojar	Carga de trabajo: Oracle	Tecnologías: Bases de datos; migración; almacenamiento y copia de seguridad
Servicios de AWS: Amazon RDS; AWS Managed Services		

Resumen

Este patrón muestra cómo migrar una instancia de base de datos de Amazon Relational Database Service (Amazon RDS) para Oracle de una cuenta de AWS a otra cuenta de AWS. El patrón se aplica a situaciones en las que la cuenta de AWS de origen no utiliza AWS Managed Services (AMS), pero la cuenta de destino sí utiliza AMS. Puede completar la migración mediante una solicitud de cambio (RFC) en AMS en lugar de utilizar la consola de administración de AWS para realizar operaciones de base de datos. Este enfoque proporciona un tiempo de inactividad mínimo para una base de datos de origen de Oracle de varios terabytes con un número elevado de transacciones. Así, por ejemplo, el tiempo de inactividad de una base de datos de 400 a 900 GB puede durar aproximadamente dos o tres horas. El tiempo de migración de la base de datos es directamente proporcional al tamaño de la instancia de base de datos de Amazon RDS para Oracle.

Importante: Este patrón requiere que tome una instantánea de la base de datos de la instancia de base de datos de Amazon RDS para Oracle en una cuenta de origen, copie la instantánea en una cuenta de destino que utilice AMS y, a continuación, cree una nueva instancia de base de datos a partir de esa instantánea mediante el aumento de las RFC.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa para la cuenta de origen
- Una cuenta de AWS activa que utilice AMS como cuenta de destino
- Una instancia de base de datos de Amazon RDS para Oracle, configurada y en funcionamiento

Limitaciones

- Las mismas propiedades o configuraciones de las instancias de base de datos de la cuenta de origen se copian a una nueva instancia de base de datos de destino en AMS.
- El método RFC que se utiliza en este enfoque de migración tiene características limitadas para admitir Amazon RDS para Oracle. Puede acceder a todas las funciones de Amazon RDS for Oracle mediante una plantilla de CloudFormation AWS para realizar la migración de la base de datos.
- Puede sufrir una interrupción de la aplicación durante varias horas porque la migración debe completarse durante el tiempo de inactividad programado. Durante el tiempo de inactividad, se detiene la instancia de base de datos en la cuenta de origen y, a continuación, se activa una nueva instancia de base de datos en la cuenta de destino.
- Este enfoque de migración no se aplica a la migración de una instancia de base de datos de una región de AWS a otra región dentro de la misma cuenta de AWS.

Versiones de producto

- Instancia de Oracle Database Standard Edition 2 (SE2) 12.1.0.2.v2 y posterior en Amazon RDS para Oracle
- Ya no se admite Amazon RDS para Oracle 11g (para obtener más información, consulte Amazon RDS para Oracle en la documentación de Amazon RDS).

Arquitectura

Pila de tecnología de origen

- Instancia de Oracle Database SE2 12.1.0.2.v2 en Amazon RDS para Oracle
- Grupo de subredes de Amazon RDS

- Grupo de opciones de Amazon RDS (si es necesario)
- Grupo de parámetros de Amazon RDS (si es necesario)
- Grupo de seguridad de Amazon Virtual Private Cloud (Amazon VPC)
- AWS Key Management Service (AWS KMS) con claves administradas por AWS o claves administradas por el cliente
- Rol de AWS Identity and Access Management (IAM) (si es necesario)

Pila de tecnología de destino

- Instancia de Oracle Database SE2 12.1.0.2.v2 en Amazon RDS para Oracle
- Grupo de subredes de Amazon RDS
- Grupo de opciones de Amazon RDS (si es necesario)
- Grupo de parámetros de Amazon RDS (si es necesario)
- Grupo de seguridad de Amazon VPC
- AWS Managed Services (AMS)
- AWS KMS con claves administradas por AWS y claves administradas por el cliente
- Rol de IAM (si es necesario)

Arquitectura de migración de origen y destino

El siguiente diagrama muestra la migración de una instancia de base de datos de Amazon RDS para Oracle de una cuenta de AWS a una instancia de base de datos de Amazon RDS para Oracle de otra cuenta de AWS que utiliza AMS.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Realice una instantánea de la base de datos de la instancia de base de datos de Amazon RDS para Oracle en la cuenta de origen.
2. Copie la instantánea en AMS en la cuenta de destino.
3. Cree una nueva instancia de base de datos de Amazon RDS para Oracle a partir de la instantánea de la cuenta de destino.

Automatizar y escalar

Puede automatizar y escalar la migración mediante el uso de CloudFormation plantillas y la creación de RFC en AMS. CloudFormation le permite utilizar todas las funciones de Amazon RDS for Oracle, incluida la posibilidad de configurar y restaurar la instancia de base de datos al crear una instancia de base de datos de Amazon RDS for Oracle a partir de una instantánea.

Herramientas

- Amazon Relational Database Service (Amazon RDS) para Oracle ayuda a configurar, utilizar y escalar una base de datos relacional de Oracle en la nube de AWS.
- AWS Key Management Service (AWS KMS) facilita poder crear y controlar claves criptográficas para proteger los datos.
- AWS Managed Services (AMS) ayuda a operar la infraestructura de AWS de forma más eficiente y segura.

Epics

Preparar la transición a la cuenta de destino

Tarea	Descripción	Habilidades requeridas
Crear una clave de AWS KMS personalizada.	1. Emita una RFC automatizada denominada Create KMS key (Crear clave KMS) para crear una clave KMS personalizada a partir de la cuenta de destino. 2. Comparta su clave KMS personalizada con la cuenta de origen. Nota: No puede compartir instancias de base de datos de Amazon RDS para Oracle que utilicen la clave administrada de AWS predeterminada para Amazon RDS (`aws/rds`). En su lugar,	AWS, AMS

Tarea	Descripción	Habilidades requeridas
	comparta la instancia de base de datos volviendo a cifrarla desde su clave de KMS.	
Crear un grupo de seguridad.	Emita una RFC automatizada denominada Create security group (Crear grupo de seguridad) para crear un grupo de seguridad para su VPC a partir de su cuenta de destino. Asegúrese de especificar lo siguiente: • Nuevo nombre de grupo de seguridad • Reglas de entrada y salida de TCP y UDP • Etiquetas estándar	AWS, AMS

Tarea	Descripción	Habilidades requeridas
(Opcional) Revise sus recursos de Amazon RDS.	Al crear una instancia de base de datos de Amazon RDS para Oracle se crean los recursos siguientes: • Grupo de subredes de Amazon RDS (basado en el ID de subred) • Amazon RDS (grupo de opciones de Amazon RDS, basado en la instantánea de la instancia de base de datos de origen) • Grupo de parámetros de Amazon RDS (basado en la instantánea de la instancia de base de datos) Si desea revisar los recursos de Amazon RDS que se crearon al crear la instancia de base de datos, puede conectarse a la instancia de base de datos de Oracle y buscar el grupo de subredes, el grupo de opciones y el grupo de parámetros en la consola de Amazon RDS.	AWS

Realizar la transición a la cuenta de origen

Tarea	Descripción	Habilidades requeridas
Detenga la aplicación.	Detenga la aplicación y sus servicios dependientes. Debe detener todo el tráfico a la base de datos de la cuenta de origen.	Propietario de la aplicación
Tome una instantánea manual.	De forma manual cree una instantánea de base de datos de la instancia de base de datos de Amazon RDS para Oracle en la cuenta de origen.	AWS
Detenga la instancia de la base de datos.	Detenga la instancia para base de datos de Amazon RDS para Oracle .	AWS
Copie la instantánea.	Copie la instantánea de base de datos en la misma cuenta de origen y, a continuación, utilice la clave KMS personalizada compartida desde la cuenta de destino para volver a cifrar el archivo de instantánea de base de datos copiado.	AWS
Comparta la instantánea.	Comparta la nueva instantánea (copiada con la clave KMS personalizada) con la cuenta de destino.	AWS

Realizar la transición a la cuenta de destino

Tarea	Descripción	Habilidades requeridas
Copie la instantánea.	Emita una RFC automatizada denominada Copy RDS snapshot (Copiar instantánea de RDS) para copiar la instantánea de base de datos en la misma cuenta de destino y utilice la clave KMS administrada por AWS predeterminada creada para volver a cifrarla. Esto es necesario para que la cuenta de destino sea la propietaria de la nueva instantánea y para permitir que la instancia de base de datos Amazon RDS para Oracle creada a partir de la instantánea se asocie al grupo de opciones, si es necesario.	AWS, AMS
Cree una instancia de base de datos a partir de la instantánea.	Emita una RFC automatizada denominada Create DB from snapshot (Crear base de datos a partir de una instantánea) para crear una instancia de base de datos de Amazon RDS para Oracle a partir de la instantánea. Asegúrese de especificar lo siguiente:	AWS, AMS

Tarea	Descripción	Habilidades requeridas
	• Nuevo ID de la instantánea creada en el paso anterior • ID de VPC • ID de subred • ID de instancia de RDS • Etiquetas estándar	
Adjunte la instancia al grupo de seguridad y lleve a cabo actualizaciones de la configura ción.	1. Emita una RFC manual denominada Update Other (Actualizar otras) para adjuntar la instancia de base de datos de Amazon RDS para Oracle que se creó anteriormente al grupo de seguridad de VPC que se creó anteriormente. 2. Realice cualquier cambio adicional en la configura ción de la instancia de base de datos de Amazon RDS para Oracle.	AWS, AMS

Tarea	Descripción	Habilidades requeridas
Pruebe la instancia de la base de datos.	Pruebe la nueva conectividad del punto de conexión de la instancia de base de datos Amazon RDS para Oracle; para ello, inicie sesión en cualquier servidor de instancias o aplicaciones alojado en el mismo grupo de seguridad y utilice telnet para conectarse al puerto 1521. Para obtener más información, consulte Connecting to an Amazon RDS DB instance (Conectarse a una instancia de base de datos de Amazon RDS) en la documentación de Amazon RDS. Nota: Si las credenciales de inicio de sesión del usuario principal están disponibles, puede probar la instancia de base de datos de Amazon RDS para Oracle iniciando sesión desde cualquier cliente de SQL (como Oracle SQL Developer).	AWS, Administrador de base de datos

Recursos relacionados

- AWS Managed Services (documentación de AWS)
- How RFCs work (Cómo funcionan las RFC) (documentación de AWS Managed Services)
- Sharing encrypted snapshots (Compartir instantáneas cifradas) (Guía del usuario de Amazon RDS)

- How can I share an encrypted Amazon RDS DB snapshot with another account? (¿Cómo puedo compartir una instantánea de base de datos de Amazon RDS cifrada con otra cuenta?) (Centro de conocimientos de AWS)
- What is Amazon Relational Database Service (Amazon RDS)? (¿Qué es Amazon Relational Database Service (Amazon RDS)?) (Guía del usuario de Amazon RDS)
- Amazon RDS para Oracle (Amazon RDS para Oracle) (Guía del usuario de Amazon RDS)
- Using the AMS consoles (Usar las consolas AMS) (Documentación de AWS Managed Services)

Información adicional

Roll back the migration (Revertir la migración)

Si desea revertir la migración, siga los pasos siguientes:

1. Emita una RFC manual (Update Other [Actualizar otras]) desde la cuenta de destino para eliminar la pila de bases de datos creada en la cuenta de destino.
2. Actualice la configuración de la aplicación para que apunte a la instancia de base de datos de Amazon RDS para Oracle en la cuenta de origen.
3. Inicie la instancia de base de datos de Amazon RDS para Oracle en la cuenta de origen.

Migrar las variables de enlace OUT de Oracle a una base de datos PostgreSQL

Creado por Bikash Chandra Rout (AWS) y Vinay Paladi (AWS)

Entorno: PoC o piloto	Origen: bases de datos relacionales	Destino: RDS/Aurora Postgresql
Tipo R: redefinir la plataforma	Carga de trabajo: Oracle	Tecnologías: bases de datos; migración
Servicios de AWS: Amazon Aurora; Amazon RDS; AWS SCT		

Resumen

Este patrón muestra cómo migrar variables de enlace de `OUT` de la base de datos Oracle a cualquiera de los siguientes servicios de base de datos de AWS compatibles con PostgreSQL:

- Amazon Relational Database Service (Amazon RDS) fpara PostgreSQL
- Edición compatible con Amazon Aurora PostgreSQL

PostgreSQL no admite variables de enlace de `OUT`. Para obtener la misma funcionalidad en sus sentencias de Python, puede crear una función PL/pgSQL personalizada que utilice en su lugar las variables `GET` y `SET` del paquete de variables. Para aplicar estas variables, el script de función contenedora de ejemplo que se proporciona en este patrón utiliza un paquete de extensiones de la Herramienta de conversión de esquemas de AWS (AWS SCT).

Nota: si la instrucción `EXECUTE IMMEDIATE` de Oracle es una `SELECT` instrucción que puede devolver una fila como máximo, se recomienda hacer lo siguiente:

- Coloque las variables de enlace (define) `OUT` en la cláusula `INTO`
- Coloque las variables de enlace `IN` en la cláusula `USING`

Para obtener más información, consulte EXECUTE IMMEDIATE statement en la documentación de Oracle.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos de origen Oracle Database 10g (o más reciente) en un centro de datos local
- Una instancia de base de datos Amazon RDS para PostgreSQL o una instancia de base de datos Aurora compatible con PostgreSQL

Arquitectura

Pila de tecnología de origen

- Base de datos Oracle Database 10g (o posterior) local

Pila de tecnología de destino

- Una instancia de ase de datos Amazon RDS para PostgreSQL o una instancia de base de datos Aurora compatible con PostgreSQL

Arquitectura de destino

El siguiente diagrama muestra un ejemplo de flujo de trabajo para migrar variables de enlace de 0UT de Oracle Database a una base de datos de AWS compatible con PostgreSQL:

En el diagrama, se muestra el siguiente flujo de trabajo:

1. AWS SCT convierte el esquema de la base de datos de origen y la mayoría del código personalizado a un formato compatible con la base de datos de AWS compatible con PostgreSQL de destino.
2. La función PL/pgSQL marca cualquier objeto de base de datos que no se pueda convertir automáticamente. A continuación, los objetos marcados se convierten manualmente para completar la migración.

Herramientas

- Amazon Aurora PostgreSQL-Compatible es un motor de base de datos relacional completamente administrado que le permite configurar, administrar y escalar implementaciones de PostgreSQL.
- Amazon Relational Database Service (Amazon RDS) para PostgreSQL ayuda a configurar, utilizar y escalar una base de datos relacional de PostgreSQL en la nube de AWS.
- Herramienta de conversión de esquemas de AWS (AWS SCT) simplifica las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado a un formato compatible con la base de datos de destino.
- pgAdmin es una herramienta de gestión de código abierto para PostgreSQL. Proporciona una interfaz gráfica que permite crear, mantener y utilizar objetos de bases de datos.

Epics

Migrar las variables de enlace OUT de Oracle mediante una función PL/pgSQL personalizada y AWS SCT

Tarea	Descripción	Habilidades requeridas
Conéctese a su base de datos de AWS compatible con PostgreSQL.	Una vez que haya creado su instancia de base de datos, puede usar cualquier aplicación cliente SQL estándar para conectarse a una base de datos en su clúster de base de datos. Por ejemplo, puede usar pgAdmin para conectarse a su instancia de base de datos. Para obtener más información, consulte cualquiera de los temas siguientes: • Conexión a una instancia de base de datos de Amazon	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	RDS en la Guía del usuario de Amazon RDS • Conexión a un clúster de base de datos de Amazon Aurora en la Guía del usuario de Amazon Aurora	
Añada el ejemplo del script de la función contenedora de este patrón al esquema principal de la base de datos de destino.	Copie el ejemplo del script de la función contenedora PL/pgSQL de la sección de información adicional de este patrón. A continuación, añada la función al esquema principal de la base de datos de destino. Para obtener más información, consulte CREATE FUNCTION en la documentación de PostgreSQL.	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
(Opcional) Actualice la ruta de búsqueda en el esquema principal de la base de datos de destino para que incluya el esquema Test_PG.	Para mejorar el rendimiento, puede actualizar la variable search_path de PostgreSQL para que incluya el nombre del esquema Test_pg. Si incluye el nombre del esquema en la ruta de búsqueda, no necesitará especificarlo cada vez que llame a la función PL/pgSQL. Para obtener más información, consulte la sección 5.9.3 La ruta de búsqueda de esquemas en la documentación de PostgreSQL.	Ingeniero de migraciones

Recursos relacionados

- Herramienta de conversión de esquemas de AWS
- Variables de enlace OUT (documentación de Oracle)
- Mejore el rendimiento de las consultas SQL mediante el uso de variables de enlace (Oracle Blog)

Información adicional

Ejemplo de función PL/pgSQL

```
/* Oracle */

CREATE or replace PROCEDURE test_pg.calc_stats_new1 (
                                                      a NUMBER,
                                                      b NUMBER,
                                                      result out NUMBER
                                                    )
```

```
IS
BEGIN
result:=a+b;
END;
/
/* Testing */
set serveroutput on
DECLARE
  a NUMBER := 4;
  b NUMBER := 7;
  plsql_block VARCHAR2(100);
  output number;
BEGIN
  plsql_block := 'BEGIN test_pg.calc_stats_new1(:a, :b,:output); END;';
  EXECUTE IMMEDIATE plsql_block USING a, b,out output;  -- calc_stats(a, a, b, a)
  DBMS_OUTPUT.PUT_LINE('output:'||output);
END;

output:11


PL/SQL procedure successfully completed.

--Postgres--

/* Example : 1 */
CREATE OR REPLACE FUNCTION test_pg.calc_stats_new1(
                                                    w integer,
                                                    x integer
                                                  )
RETURNS integer
AS
$BODY$
begin
      return w + x ;
end;
$BODY$
LANGUAGE  plpgsql;


CREATE OR REPLACE FUNCTION aws_oracle_ext.set_package_variable(
                                                                package_name name,
                                                                variable_name name,
```

```
                                                                    variable_value
 anyelement
                                                                )
    RETURNS void
    LANGUAGE 'plpgsql'

    COST 100
    VOLATILE
AS $BODY$
begin
    perform set_config
      ( format( '%s.%s',package_name, variable_name )
      , variable_value::text
      , false );
  end;
$BODY$;

CREATE OR REPLACE FUNCTION aws_oracle_ext.get_package_variable_record(
                                                                      package_name
 name,
                                                                      record_name name
                                                                    )
RETURNS text
LANGUAGE 'plpgsql'
    COST 100
    VOLATILE
AS $BODY$
begin
    execute 'select ' || package_name || '$Init()';

    return aws_oracle_ext.get_package_variable
        (
         package_name := package_name
        , variable_name := record_name || '$REC' );
end;
$BODY$;

--init()--
CREATE OR REPLACE FUNCTION test_pg.init()
RETURNS void
AS
$BODY$
BEGIN
if aws_oracle_ext.is_package_initialized('test_pg' ) then
```

```
      return;
    end if;
    perform aws_oracle_ext.set_package_initialized
      ('test_pg' );
PERFORM aws_oracle_ext.set_package_variable('test_pg', 'v_output', NULL::INTEGER);
PERFORM aws_oracle_ext.set_package_variable('test_pg', 'v_status', NULL::text);
END;
$BODY$
LANGUAGE  plpgsql;

/* callable for 1st Example */

DO $$
declare
v_sql text;
v_output_loc int;
a integer :=1;
b integer :=2;
BEGIN
perform  test_pg.init();
--raise notice 'v_sql %',v_sql;
execute 'do $a$ declare v_output_l int; begin select * from test_pg.calc_stats_new1('||
a||','||b||') into v_output_l;
PERFORM aws_oracle_ext.set_package_variable(''test_pg'', ''v_output'', v_output_l) ;
 end; $a$'  ;
v_output_loc := aws_oracle_ext.get_package_variable('test_pg', 'v_output');
raise notice 'v_output_loc %',v_output_loc;
END ;
$$

/*In above Postgres example we have set the value of v_output using v_output_l in the
 dynamic anonymous block to mimic the
  behaviour of oracle out-bind variable .*/

--Postgres Example : 2 --
CREATE OR REPLACE FUNCTION test_pg.calc_stats_new2(
 w integer,
 x integer,
inout status text,
 out result integer)
AS
$BODY$
DECLARE
begin
```

```
result :=  w + x ;
status := 'ok';
end;
$BODY$
LANGUAGE  plpgsql;

/* callable for 2nd Example */
DO $$
declare
v_sql text;
v_output_loc int;
v_staus text:= 'no';
a integer :=1;
b integer :=2;
BEGIN
perform  test_pg.init();
execute 'do $a$ declare v_output_l int; v_status_l text; begin select * from
 test_pg.calc_stats_new2('||a||','||b||','''||v_staus||''') into v_status_l,v_output_l;
PERFORM aws_oracle_ext.set_package_variable(''test_pg'', ''v_output'', v_output_l) ;
PERFORM aws_oracle_ext.set_package_variable(''test_pg'', ''v_status'', v_status_l) ;
end; $a$'  ;
v_output_loc := aws_oracle_ext.get_package_variable('test_pg', 'v_output');
v_staus := aws_oracle_ext.get_package_variable('test_pg', 'v_status');
raise notice 'v_output_loc %',v_output_loc;
raise notice 'v_staus %',v_staus;
END ;
$$
```

Migración de SAP HANA a AWS mediante SAP HSR con el mismo nombre de host

Creado por Pradeep Puliyampatta (AWS)

Entorno: producción	Origen: SAP HANA DB en las instalaciones	Destino: SAP HANA DB en AWS
Tipo R: volver a alojar	Carga de trabajo: SAP	Tecnologías: bases de datos; migración
Servicios de AWS: AWS Client VPN; AWS Direct Connect; Amazon EBS		

Resumen

Las migraciones de SAP HANA a Amazon Web Services (AWS) se pueden realizar mediante múltiples opciones, incluidas la copia de seguridad y restauración, la exportación e importación y la replicación del sistema SAP HANA (HSR). La selección de una opción concreta dependerá de la conectividad de red entre las bases de datos SAP HANA de origen y destino, el tamaño de la base de datos de origen, las consideraciones de tiempo de inactividad y otros factores.

La opción HSR de SAP para migrar las cargas de trabajo de SAP HANA a AWS funciona adecuadamente cuando hay una red estable entre los sistemas de origen y destino, y cuando toda la base de datos (instantánea de replicación de la base de datos de SAP HANA) se puede replicar por completo en 1 día, según lo estipulado por SAP en los requisitos de rendimiento de la red para SAP HSR. Los requisitos de tiempo de inactividad de este enfoque se limitan a realizar la adquisición en el AWS entorno de destino, realizar el backup de la base de datos de SAP HANA y realizar tareas posteriores a la migración.

SAP HSR admite el uso de diferentes nombres de host (nombres de host asignados a diferentes direcciones IP) para el tráfico de replicación entre los sistemas principal o de origen y secundario o de destino. Puede hacerlo definiendo esos conjuntos específicos de nombres de host en la sección `[system_replication_hostname_resolution]`, en `global.ini`. En esta sección, todos los

hosts de los sitios principal y secundario deben estar definidos en cada host. Para ver los pasos de configuración detallados, consulte la documentación de SAP.

Una conclusión clave de esta configuración es que los nombres de host del sistema principal deben ser diferentes de los nombres de host del sistema secundario. De lo contrario, se pueden producir los siguientes errores.

- `"each site must have a unique set of logical hostnames"`
- `"remoteHost does not match with any host of the source site. All hosts of source and target site must be able to resolve all hostnames of both sites correctly"`

Sin embargo, la cantidad de pasos posteriores a la migración se puede reducir utilizando el mismo nombre de host de SAP HANA DB en el entorno de destino. AWS

Este patrón proporciona una solución alternativa para usar el mismo nombre de host en los entornos de origen y destino cuando se emplea la opción SAP HSR. Con este patrón, puede usar la opción de cambio de nombre de host de SAP HANA. Debe asignar un nombre de host temporal a la base de datos de SAP HANA de destino para facilitar la exclusividad del nombre de host de SAP HSR. Una vez que la migración complete la adquisición del entorno SAP HANA de destino, puede volver a convertir el nombre de host del sistema de destino en el nombre de host del sistema de origen.

Requisitos previos y limitaciones

Requisitos previos

- Un activo. Cuenta de AWS
- Una nube privada virtual (VPC) con un punto de conexión de red privada virtual (VPN) o router.
- AWS Client VPN o AWS Direct Connect configurado para transferir archivos del origen al destino.
- Bases de datos de SAP HANA, tanto en el entorno de origen como en el de destino. El nivel de parche de la base de datos SAP HANA de destino debe ser igual o superior al nivel de parche de la base de datos SAP HANA de origen, dentro de la misma edición de la plataforma SAP HANA. Por ejemplo, no es posible configurar la replicación entre los sistemas HANA 1.0 y HANA 2.0. Para obtener más información, consulte la pregunta 15 en la nota de SAP: 1999880 — Preguntas frecuentes: replicación del sistema SAP HANA.
- Servidores de aplicaciones SAP en el entorno de destino.
- Volúmenes de Amazon Elastic Block Store (Amazon EBS) en el entorno de destino.

Limitaciones

En la siguiente lista de documentos de SAP se describen los problemas conocidos relacionados con esta solución alternativa, incluidas las limitaciones de la organización dinámica por niveles y las migraciones de escala horizontal de SAP HANA:

- 2956397 – Fallo al cambiar el nombre del sistema de base de datos SAP HANA
- 2222694 – Al intentar cambiar el nombre del sistema HANA, aparece el siguiente error: “Los archivos de origen no pertenecen al usuario sidadm original (uid = xxxx)”
- 2607227 – hdblcm: register_rename_system: No se pudo cambiar el nombre de la instancia de SAP HANA
- 2630562 – Error al cambiar el nombre de host de HANA, HANA no se inicia
- 2935639 – sr_register no usa el nombre de host especificado en system_replication_hostname_resolution en la sección global.ini
- 2710211 – Error: el sistema de origen y el sistema de destino tienen nombres de host lógicos superpuestos
- 2693441 – No se pudo cambiar el nombre de un sistema SAP HANA debido a un error
- 2519672 – HANA principal y secundario tienen sistemas diferentes (PKI, SSFS, datos y claves) o no se pueden comprobar
- 2457129 – No está permitido cambiar el nombre del host del sistema SAP HANA cuando la estratificación dinámica forma parte del entorno
- 2473002 – Uso de la replicación del sistema HANA para migrar un sistema de escala horizontal (SAP no impone restricciones a la hora de usar este enfoque de cambio de nombre de host para sistemas SAP HANA con capacidad de ampliación. Sin embargo, el procedimiento debe repetirse en cada host individual. Este enfoque también tiene otras limitaciones de migración de escala horizontal).

Versiones de producto

- Esta solución se aplica a las ediciones 1.0 y 2.0 de la plataforma de base de datos SAP HANA.

Arquitectura

Configuración de origen

Base de datos SAP HANA instalada en el entorno de origen. Todas las conexiones del servidor de aplicaciones e interfaces de base de datos de SAP usan el mismo nombre de host para las conexiones de los clientes. El siguiente diagrama muestra el ejemplo del nombre de host de origen `hdbhost` y su dirección IP correspondiente.

Configuración de destino

El entorno de Nube de AWS destino utiliza el mismo nombre de host para ejecutar una base de datos de SAP HANA. El entorno de destino en AWS incluye lo siguiente:

- Base de datos SAP HANA
- Servidores de aplicaciones SAP
- Volúmenes de EBS

Configuración intermedia

En el siguiente diagrama, se cambia temporalmente el nombre de host del entorno de AWS destino `temp-host` para que los nombres de host del origen y el de destino sean únicos. Una vez que la migración complete la adquisición en el entorno de destino, se cambia el nombre de host virtual del sistema de destino por el nombre original, `hdbhost`.

La configuración intermedia incluye una de las siguientes opciones:

- AWS Client VPN con un terminal Client VPN
- AWS Direct Connect conectándose a un router

Los servidores de aplicaciones SAP en el entorno de AWS destino se pueden instalar antes de la configuración de la replicación o después de la adquisición. Sin embargo, instalar los servidores de aplicaciones antes de configurar la replicación puede ayudar a reducir el tiempo de inactividad durante la instalación, configurar la alta disponibilidad y realizar copias de seguridad.

Herramientas

Servicios de AWS

- AWS Client VPNes un servicio de VPN gestionado y basado en clientes que le permite acceder de forma segura a AWS los recursos y recursos de su red local.
- AWS Direct Connectconecta su red interna a una AWS Direct Connect ubicación a través de un cable Ethernet de fibra óptica estándar. Con esta conexión, puede crear interfaces virtuales directamente con las públicas Servicios de AWS, sin tener en cuenta a los proveedores de servicios de Internet en su ruta de red.
- Amazon Elastic Block Store (Amazon EBS) proporciona volúmenes de almacenamiento a nivel de bloque para utilizarlos con instancias de Amazon Elastic Compute Cloud (Amazon EC2). Los volúmenes de EBS se comportan como dispositivos de bloques sin formatear. Puede montar estos volúmenes como dispositivos en sus instancias.

Otras herramientas

- Servidores de aplicaciones SAP: los servidores de aplicaciones SAP proporcionan a los programadores una forma de expresar la lógica empresarial. El servidor de aplicaciones SAP realiza el procesamiento de datos en función de la lógica empresarial. Los datos reales se almacenan en una base de datos, que es un componente independiente.
- SAP HANA cockpit y SAP HANA Studio: tanto SAP HANA cockpit como SAP HANA Studio proporcionan una interfaz administrativa para la base de datos de SAP HANA. En SAP HANA Studio, la consola de administración de SAP HANA es la vista del sistema que proporciona el contenido relevante para administrar la base de datos de SAP HANA.
- Replicación del sistema SAP HANA: la replicación del sistema SAP HANA (SAP HSR) es el procedimiento estándar que proporciona SAP para replicar las bases de datos de SAP HANA. Los ejecutables necesarios para SAP HSR forman parte del propio kernel del servidor SAP HANA.

Epics

Prepare el entorno de origen y destino

Tarea	Descripción	Habilidades requeridas
Instale y configure las bases de datos de SAP HANA.	En los entornos de origen y destino, asegúrese de que la base de datos de SAP HANA esté instalada y configurada de acuerdo con las prácticas	Administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas
	recomendadas de SAP HANA. Para obtener más información, consulte SAP HANA en AWS.	
Mapee la dirección IP.	En el entorno de destino, asegúrese de que el nombre de host temporal esté asignado a una dirección IP interna. 1. Para asignar una dirección IPv4 secundaria a la instancia de EC2 en la consola de administr ación de AWS, vaya a EC2, Instance, Actions, Networking, Manage IP address y Assign new IP address. 2. Para asignar la misma dirección al adaptador de red (NIC) de EC2, desde el sistema operativo y como usuario raíz, ejecute el comando `ip addr add <IP>/32 dev eth0` y sustituya `<IP>` por la dirección IP del paso 1.	Administración de AWS

Tarea	Descripción	Habilidades requeridas
Resuelva los nombres de host de destino.	En la base de datos secundaria de SAP HANA, confirme que ambos nombres de host (`hdbhost` y `temp-host`) están resueltos para las redes de replicación de SAP HANA actualizando los nombres de host correspondientes en el archivo `/etc/hosts` .	Administración de Linux
Realice copias de seguridad de las bases de datos SAP HANA de destino.	Use SAP HANA Studio o SAP HANA cockpit para realizar copias de seguridad en las bases de datos de SAP HANA.	Administrador de SAP Basis
Intercambie los certificados de PKI del sistema.	(Solo se aplica a SAP HANA 2.0 y versiones posteriores) Intercambie los certificados en el almacén seguro de infraestructura de clave pública (PKI) del sistema, en el almacén del sistema de archivos (SSFS) entre las bases de datos principal y secundaria. Para obtener más información, consulte la nota 2369981 de SAP: Pasos de configuración necesarios para la autenticación con la replicación del sistema SAP HANA.	Administrador de SAP Basis

Cambie el nombre de la base de datos SAP HANA de destino

Tarea	Descripción	Habilidades requeridas
Detenga las conexiones con los clientes de destino.	En el entorno de destino, apague los servidores de aplicaciones de SAP y otras conexiones de clientes.	Administrador de SAP Basis
Cambie el nombre de la base de datos de SAP HANA de destino por el nombre de host temporal.	1. Como usuario raíz, cambie el nombre del host de la base de datos SAP HANA de destino por el nombre de host temporal usando el `hdblcm` residente. `root $> cd /hana/shared/<SID/hdblcm` `root $> ./hdblcm` 2. Seleccione Opciones 9 `| rename_system | Rename the SAP HANA Database System`. 3. Proporcione el nombre nuevo: `temp-host .` 4. Puede validar otras opciones según sea necesario. Sin embargo, asegúrese de no confundir el cambio de nombre del host con un cambio de SID (Nota de SAP 2598814: hdblcm: error al cambiar el nombre del SID).	Administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas
	La detención y el inicio de la base de datos de SAP HANA se controlarán mediante `hdblcm`.	
Asigne redes de replicación.	En el archivo `global.ini` del sistema de origen, bajo el encabezado `[system_replication_hostname_resolution]` , proporcione los detalles de la red de replicación de origen y destino. A continuación, copie las entradas en el archivo `global.ini` del sistema de destino.	Administrador de SAP Basis
Habilite la replicación en el servidor principal.	Para habilitar la replicación en la base de datos de SAP HANA de origen, ejecute el siguiente comando. `hdbnsutil -sr_enable --name=siteA`	Administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas
Registre la base de datos de SAP HANA de destino como sistema secundario.	Para registrar la base de datos de SAP HANA de destino como sistema secundario de origen para SAP HSR, elija la replicación asíncrona. `(sid)adm $> HDB stop` `(sid)adm $> hdbnsutil -sr_register –name=siteB –remotehost=hdbhost /` `--remoteInstance=00 –replicationMode=async –operationMode=logreplay` `(sid)adm $> HDB start` También puede seleccionar la opción de registro `–online`. En ese caso, no necesita detener e iniciar la base de datos de SAP HANA.	Administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas
Valide la sincronización.	En la base de datos de SAP HANA de origen, compruebe que todos los registros se apliquen al sistema de destino (ya que se trata de una replicación asíncrona). Para verificar la replicaci ón, ejecute los siguientes comandos en el entorno de origen. `(sid)adm $> cdpy` `(sidadm $> python systemReplicationStatus.py`	Administrador de SAP Basis
Cierre la aplicación SAP de origen y la base de datos de SAP HANA.	Durante la transición a la migración, apague el sistema de origen (la aplicación SAP y la base de datos SAP HANA).	Administrador de SAP Basis
Realice la adquisición del destino.	Para realizar la adquisición del destino en AWS, ejecute el comando `hdbnsutil -sr_takeover` .	Administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas
En la base de datos de SAP HANA de destino, desactive la replicación.	Para borrar los metadatos de la replicación, detenga la replicación en el sistema de destino ejecutando el comando `hdbnsutil -sr_disable` . Nota: Según la Nota de SAP 2693441: No se pudo cambiar el nombre de un sistema SAP HANA debido a un error.	Administrador de SAP Basis
Realice una copia de seguridad de la base de datos SAP HANA de destino.	Una vez que la adquisición se haya realizado correctamente, recomendamos realizar una copia de seguridad completa de la base de datos de SAP HANA.	Administrador de SAP Basis

Revierta al nombre de host original en el sistema de destino

Tarea	Descripción	Habilidades requeridas
Revierta al nombre de host original el nombre de host de SAP HANA DB.	1. Para revertir el nombre de host de la base de datos de SAP HANA de destino al nombre de host virtual original, use `hdblcm` residente. `root $> cd /hana/shared/<SID>/hdblcm` `root $> ./hdblcm`	Administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas
	2. Seleccione Opciones 9 `| rename_system | Rename the SAP HANA Database System`. 3. Proporcione el nombre nuevo: `hdbhost`. Puede validar otras opciones según sea necesario. Sin embargo, asegúrese de no confundir el cambio de nombre del host con un cambio de SID (Nota de SAP 2598814: hdblcm: error al cambiar el nombre del SID).	
Ajuste hdbuserstore.	Adapte los detalles de `hdbuserstore` apuntando a los detalles de la fuente `schema/user` . Para ver los pasos detallados, consulte la documentación de SAP. Para validar este paso, ejecute el comando `R3trans -d`. El resultado debe reflejar una conexión correcta a la base de datos de SAP HANA.	Administrador de SAP Basis
Inicie las conexiones con los clientes.	En el entorno de destino, inicie los servidores de aplicaciones de SAP y otras conexiones de clientes.	Administrador de SAP Basis

Recursos relacionados

Referencias de SAP

SAP actualiza con frecuencia las referencias de documentación de SAP. Para mantenerse al día, consulte la Nota de SAP 2407186: Guías prácticas y documentos técnicos sobre la alta disponibilidad de SAP HANA.

Notas adicionales de SAP

- 2550327 – Cómo cambiar el nombre de un sistema SAP HANA
- 1999880 – Preguntas frecuentes: replicación del sistema SAP HANA
- 2078425 – Nota de solución de problemas para la herramienta de gestión del ciclo de vida de la plataforma SAP HANA hdblcm
- 2592227 – Cambio del sufijo FQDN en sistemas HANA
- 2048681 – Realización de tareas de administración de ciclo de vida de la plataforma SAP HANA en sistemas con varios hosts sin credenciales de SSH o root

Documentos de SAP

- Conexión de red de replicación del sistema
- Resolución del nombre de host para la replicación del sistema

AWS referencias

- Migración de SAP HANA de otras plataformas a AWS

Información adicional

Los cambios realizados por `hdblcm` como parte de la actividad de cambio de nombre de host se consolidan en el siguiente registro detallado.

Migrar SQL Server a AWS mediante grupos de disponibilidad distribuidos

Creado por Praveen Marthala (AWS)

Origen: SQL Server en las instalaciones	Destino: SQL Server en EC2	Tipo R: volver a alojar
Entorno: PoC o piloto	Tecnologías: bases de datos; migración	Carga de trabajo: Microsoft
Servicios de AWS: Amazon EC2		

Resumen

Los grupos de disponibilidad Always On de Microsoft SQL Server proporcionan una solución de alta disponibilidad (HA) y recuperación de desastres (DR) para SQL Server. Un grupo de disponibilidad consta de una réplica principal que acepta tráfico de lectura/escritura y hasta ocho réplicas secundarias que aceptan tráfico de lectura. Un grupo de disponibilidad se configura en un clúster de conmutación por error de Windows Server (WSFC) con dos o más nodos.

Los grupos de disponibilidad distribuida Always On de Microsoft SQL Server proporcionan una solución para configurar dos grupos de disponibilidad independientes entre dos WFSC independientes. Los grupos de disponibilidad que forman parte del grupo de disponibilidad distribuida no tienen que estar en el mismo centro de datos. Un grupo de disponibilidad puede estar en las instalaciones y el otro en la nube de Amazon Web Services (AWS) en instancias de Amazon Elastic Compute Cloud (Amazon EC2) de un dominio diferente.

Este patrón describe los pasos para usar un grupo de disponibilidad distribuido para migrar bases de datos de SQL Server locales que forman parte de un grupo de disponibilidad existente a SQL Server con grupos de disponibilidad configurados en Amazon EC2. Si sigue este patrón, puede migrar las bases de datos a la nube de AWS con un tiempo de inactividad mínimo durante la transición. Las bases de datos están altamente disponibles en AWS inmediatamente después de la transición. También puede usar este patrón para cambiar el sistema operativo subyacente de local a AWS y, al mismo tiempo, mantener la misma versión de SQL Server.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- AWS Site-to-Site VPN de AWS Direct Connect
- La misma versión de SQL Server instalada localmente y en los dos nodos de AWS

Versiones de producto

- SQL Server versión 2016 y posteriores
- SQL Server Enterprise Edition

Arquitectura

Pila de tecnología de origen

- Base de datos de Microsoft SQL Server con grupos de disponibilidad Always On en las instalaciones

Pila de tecnología de destino

- Base de datos de Microsoft SQL Server con grupos de disponibilidad Always On en Amazon EC2 en la nube de AWS

Arquitectura de migración

Terminología

- WSFC 1: WSFC en las instalaciones
- WSFC 2: WSFC en la nube de AWS
- AG 1: primer grupo de disponibilidad, que se encuentra en el WSFC 1
- AG 2: segundo grupo de disponibilidad, que se encuentra en el WSFC 2
- Réplica principal de SQL Server: nodo del AG 1 que se considera el principal global para todas las escrituras

- Reenviador de SQL Server: nodo de AG 2 que recibe datos de forma asíncrona desde la réplica principal de SQL Server
- Réplica secundaria de SQL Server: nodos en el AG 1 o el AG 2 que reciben datos de forma sincrónica desde la réplica principal o el reenviador

Herramientas

- AWS Direct Connect: AWS Direct Connect se utiliza para vincular su red interna con una ubicación de AWS Direct Connect de a través de cable de fibra óptica Ethernet de fibra óptica. Con esta conexión, puede crear interfaces virtuales directamente en servicios públicos de AWS, derivando a los proveedores de Internet a su ruta de acceso a la red.
- Amazon EC2: Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de AWS. Puede utilizar Amazon EC2 para lanzar tantos servidores virtuales como necesite, y puede escalar horizontalmente o reducir horizontalmente.
- VPN Site-to-Site de AWS: la VPN Site-to-Site de AWS permite crear una red privada virtual (VPN). site-to-site Puede configurar la VPN para que transmita el tráfico entre las instancias que lance en AWS y su propia red remota.
- Microsoft SQL Server Management Studio: Microsoft SQL Server Management Studio (SSMS) es un entorno integrado para administrar la infraestructura de SQL Server. Proporciona una interfaz de usuario y un grupo de herramientas con editores de scripts enriquecidos que interactúan con SQL Server.

Epics

Configurar un segundo grupo de disponibilidad en AWS

Tarea	Descripción	Habilidades requeridas
Crear un WSFC en AWS.	Cree WSFC 2 en instancia s de Amazon EC2 con dos nodos para HA. Utilizará este clúster de conmutación por error para crear el segundo grupo de disponibilidad (AG 2) en AWS.	Administrador de sistemas, administrador SysOps

Tarea	Descripción	Habilidades requeridas
Cree el segundo grupo de disponibilidad en el WSFC 2.	Con SSMS, cree el AG 2 en dos nodos del WSFC 2. El primer nodo del WSFC 2 actuará como reenviador. El segundo nodo del WSFC 2 actuará como réplica secundaria del AG 2. En este momento, no hay bases de datos disponibles en AG 2. Este es el punto de partida para configurar el grupo de disponibilidad distribuida.	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
Crear bases de datos sin opción de recuperación en AG 2.	Realice copias de seguridad de las bases de datos en el grupo de disponibilidad local (AG 1). Restaurar las bases de datos tanto en el reenviador como en la réplica secundaria del AG 2 sin opción de recuperación. Al restaurar las bases de datos, especifique una ubicación con suficiente espacio en disco para los archivos de datos de la base de datos y los archivos de registro. En este momento, las bases de datos se encuentran en estado de restauración. No forman parte del AG 2 ni del grupo de disponibilidad distribuida y no se sincronizan.	Administrador de base de datos, desarrollador

Configurar el grupo de disponibilidad distribuida

Tarea	Descripción	Habilidades requeridas
Cree el grupo de disponibilidad distribuida en AG 1.	Para crear el grupo de disponibilidad distribuida en el AG 1, utilice el `CREATE AVAILABILITY GROUP` con la `DISTRIBUTED` opción.	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
	1. Utilice las direcciones de `LISTENER_URL` punto de conexión para el AG 1 y el AG 2. 2. Para`AVAILABILITY-MODE`, use `ASYNCHRONOUS_COMMIT` para evitar la latencia de la red, si la hubiera. Esto no afectará al rendimiento de la base de datos. 3. En `FAILOVER_MODE` , utilice `MANUAL`. Es el único modo de disponibilidad que funciona con grupos de disponibilidad distribuidos. 4. Para restaurar las bases de datos manualmente en AG 2 y tener más control en bases de datos más grandes, utilice `MANUAL` para `SEEDING_MODE` .	

Tarea	Descripción	Habilidades requeridas
Cree el grupo de disponibilidad distribuida en AG 2.	Para crear el grupo de disponibilidad distribuida en AG 2, utilice `ALTER AVAILABILITY GROUP` con la opción `DISTRIBUTED`. 1. Utilice las direcciones de `LISTENER_URL` punto de conexión para el AG 1 y el AG 2. 2. Para`AVAILABILITY-MODE`, use `ASYNCHRONOUS_COMMIT` para evitar la latencia de la red, si la hubiera. Esto no afectará al rendimiento de la base de datos. 3. En `FAILOVER_MODE`, utilice `MANUAL`. Es el único modo de disponibilidad que funciona con grupos de disponibilidad distribuidos. 4. Para restaurar las bases de datos manualmente en AG 2 y tener más control en bases de datos más grandes, utilice `MANUAL` para `SEEDING_MODE`. El grupo de disponibilidad distribuida se crea entre el AG 1 y el AG 2.	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
	Las bases de datos del AG 2 aún no están configuradas para participar en el flujo de datos del AG 1 al AG 2.	
Añadir bases de datos al reenviador y a la réplica secundaria en AG 2.	Agregue las bases de datos al grupo de disponibilidad distribuida utilizando `ALTER DATABASE` con la opción `SET HADR AVAILABILITY GROUP` tanto en el reenviador como en la réplica secundaria en el AG 2. Esto inicia un flujo de datos asíncrono entre las bases de datos de la AG 1 y la AG 2. La principal global realiza las escrituras, envía los datos de forma sincrónica a la réplica secundaria en la AG 1 y envía los datos de forma asíncrona al reenviador en la AG 2. El reenviador del AG 2 envía los datos de forma sincrónica a la réplica secundaria del AG 2.	Administrador de base de datos, desarrollador

Supervise el flujo de datos asíncrono entre AG 1 y AG 2

Tarea	Descripción	Habilidades requeridas
Utilice registros de DMV y SQL Server.	Supervise el estado del flujo de datos entre dos grupos de disponibilidad mediante vistas	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
	de administración dinámica (DMV) y registros de SQL Server. Los DMV que son de interés para la supervisión incluyen `sys.dm_hadr_availability_replica_states` y `sys.dm_hadr_automatic_seeding`. Para conocer el estado de la sincronización del reenviador, supervise el estado sincronizado en el registro de SQL Server del reenviador.	

Realice actividades de transición para la migración final

Tarea	Descripción	Habilidades requeridas
Detener todo el tráfico hacia la réplica principal.	Detenga el tráfico entrante a la réplica principal en la AG 1 para que no se produzca ninguna actividad de escritura en las bases de datos y las bases de datos estén listas para la migración.	Propietario de la aplicación, desarrollador
Cambie el modo de disponibilidad del grupo de disponibilidad distribuida en AG 1.	En la réplica principal, establezca el modo de disponibilidad del grupo de disponibilidad distribuido en sincrónico.	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
	Tras cambiar el modo de disponibilidad a sincrónico, los datos se envían de forma sincrónica desde la réplica principal de la AG 1 al reenviador de la AG 2.	
Compruebe los LSN en ambos grupos de disponibilidad.	Compruebe los últimos números de secuencia de registro (LSN) tanto en el AG 1 como en el AG 2. Como no se está realizando ninguna escritura en la réplica principal del AG 1, los datos se sincronizan y los últimos LSN de ambos grupos de disponibilidad deberían coincidir.	Administrador de base de datos, desarrollador
Actualice AG 1 al rol secundario.	Al actualizar el AG 1 al rol secundario, el AG 1 pierde el rol de réplica principal y no acepta escrituras, y el flujo de datos entre dos grupos de disponibilidad se detiene.	Administrador de base de datos, desarrollador

Conmutación por error al segundo grupo de disponibilidad

Tarea	Descripción	Habilidades requeridas
Conmutar por error manualmente a AG 2.	En el reenviador de AG 2, modifique el grupo de disponibilidad distribuida para permitir la pérdida de datos. Como ya ha comprobado y	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
	confirmado que los últimos LSN del AG 1 y del AG 2 coinciden, la pérdida de datos no es motivo de preocupación. Al permitir la pérdida de datos en el reenviador de AG 2, las funciones de AG 1 y AG 2 cambian: • AG 2 pasa a ser el grupo de disponibilidad con la réplica principal y la réplica secundaria. • El AG 1 pasa a ser el grupo de disponibilidad con el reenviador y la réplica secundaria.	
Cambie el modo de disponibilidad del grupo de disponibilidad distribuida en AG 2.	En la réplica principal de AG 2, cambie el modo de disponibilidad a asíncrono. Esto cambia el movimiento de datos del AG 2 al AG 1, de sincrónico a asíncrono. Este paso es necesario para evitar la latencia de la red entre el AG 2 y el AG 1, si existe, y no afectará al rendimiento de la base de datos.	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
Comience a enviar tráfico a la nueva réplica principal.	Actualice la cadena de conexión para utilizar el punto de conexión de la URL del oyente en la AG 2 para enviar el tráfico a las bases de datos. El AG 2 ahora acepta escritura s y envía datos al reenviador en el AG 1, además de enviar los datos a su propia réplica secundaria en el AG 2. Los datos se mueven de forma asíncrona del AG 2 al AG 1.	Propietario de la aplicación, desarrollador

Realice actividades posteriores a la transición

Tarea	Descripción	Habilidades requeridas
Elimine el grupo de disponibi lidad distribuida en AG 2.	Supervise la migración durante el tiempo planifica do. A continuación, coloque el grupo de disponibilidad distribuida en la AG 2 para eliminar la configuración del grupo de disponibilidad distribuida entre la AG 2 y la AG 1. Esto elimina la configuración del grupo de disponibilidad distribuida y se detiene el flujo de datos del AG 2 al AG 1. En este momento, AG 2 está altamente disponible en AWS, con una réplica principal que	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
	realiza escrituras y una réplica secundaria en el mismo grupo de disponibilidad.	
Quite del servicio de los servidores en las instalaci ones.	Retire del servicio los servidores locales del WSFC 1 que forman parte del AG 1.	Administrador de sistemas, SysOps administrador

Recursos relacionados

- Grupos de disponibilidad distribuida
- SQL Docs: grupos de disponibilidad distribuida
- SQL Docs: grupos de disponibilidad Always On: una solución de alta disponibilidad y recuperación de desastres

Migre de Oracle 8i o 9i a Amazon RDS para Oracle con AWS DMS SharePlex

Creado por Ramu Jagini (AWS)

Entorno: PoC o piloto	Origen: bases de datos: relacionales	Destino: Amazon RDS
Tipo R: redefinir la plataforma	Carga de trabajo: código abierto; Oracle	Tecnologías: bases de datos; nativo en la nube; migración
Servicios de AWS: AWS DMS; Amazon RDS		

Resumen

Este patrón describe cómo migrar una base de datos Oracle 8i o 9i en las instalaciones a una base de datos de Amazon Relational Database Service (Amazon RDS) para Oracle. Puede utilizar este patrón para completar la migración con un tiempo de inactividad reducido si utiliza Quest SharePlex para la replicación sincrónica.

Debe usar una instancia de base de datos Oracle intermedia para la migración, ya que AWS Database Migration Service (AWS DMS) no admite Oracle 8i o 9i como entorno de origen. Puede utilizar la versión SharePlex 7.6.3 para replicar desde versiones anteriores de bases de datos Oracle a versiones posteriores de bases de datos Oracle. La instancia de base de datos Oracle intermedia es compatible como destino para SharePlex 7.6.3 y se admite como fuente para AWS DMS o versiones más recientes de. SharePlex Esta compatibilidad permite la replicación posterior de los datos en el entorno de destino de Amazon RDS para Oracle.

Tenga en cuenta que varios tipos de datos y funciones obsoletos pueden afectar a una migración de Oracle 8i o 9i a la versión más reciente de Oracle Database. Para mitigar este impacto, este patrón emplea Oracle 11.2.0.4 como versión de base de datos intermedia para ayudar a optimizar el código del esquema antes de migrar al entorno de destino de Amazon RDS para Oracle.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos Oracle 8i o 9i de origen en un entorno en las instalaciones
- Oracle Database 12c Release 2 (12CR2) para transición en Amazon Elastic Compute Cloud (Amazon EC2).
- Quest SharePlex 7.6.3 (versión comercial)

Limitaciones

- Limitaciones de RDS para Oracle

Versiones de producto

- Oracle 8i o 9i para la base de datos de origen
- Oracle 12CR2 para la base de datos de transición (debe coincidir con la versión de Amazon RDS para Oracle)
- Oracle 12CR2 o posterior para la base de datos de destino (Amazon RDS para Oracle)

Arquitectura

Pila de tecnología de origen

- Base de datos Oracle 8i o 9i
- SharePlex

Pila de tecnología de destino

- Amazon RDS para Oracle

Arquitectura de migración

El siguiente diagrama muestra cómo migrar una base de datos Oracle 8i o 9i de un entorno en las instalaciones a una instancia de base de datos de Amazon RDS para Oracle en la nube de AWS.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Habilite la base de datos de origen de Oracle con modo de registro de archivos, registro forzado y registro suplementario.
2. Restaure la base de datos provisional de Oracle desde la base de datos de origen de Oracle mediante Recovery Manager (RMAN) Recovery Manager (RMAN) y point-in-time FLASHBACK_SCN.
3. Configure SharePlex para leer los redo logs de la base de datos fuente de Oracle mediante (se utiliza `FLASHBACK_SCN` en RMAN).
4. Inicie SharePlex la replicación para sincronizar los datos de la base de datos de origen de Oracle con la base de datos provisional de Oracle.
5. Restaure la base de datos de destino de Amazon RDS para Oracle mediante EXPDP e IMPDP con `FLASHBACK_SCN`.
6. Configure AWS DMS y sus tareas de origen como base de datos transitoria de Oracle, y Amazon RDS para Oracle como base de datos de destino mediante `FLASHBACK_SCN` (se usa en EXPDP).
7. Inicie las tareas de AWS DMS para sincronizar los datos de la base de datos transitoria de Oracle con la base de datos de destino de Oracle.

Herramientas

- Amazon Relational Database Service (Amazon RDS) le ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS.
- AWS Database Migration Service (AWS DMS) le permite migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones.
- Quest SharePlex es una herramienta de replicación de datos de Oracle a Oracle para mover datos con un tiempo de inactividad mínimo y sin pérdida de datos.
- Recovery Manager (RMAN) es un cliente de Oracle Database que realiza tareas de copia de seguridad y recuperación en sus bases de datos. Simplifica en gran medida las copias de seguridad, la restauración y la recuperación de los archivos de bases de datos.
- Data Pump Export le ayuda a cargar datos y metadatos en un conjunto de archivos del sistema operativo denominado conjunto de archivos de volcado. El conjunto de archivos de volcado solo se puede importar mediante la utilidad Data Pump Import o el paquete DBMS_DATAPUMP.

Epics

Configuración SharePlex y la base de datos provisional de Oracle en Amazon EC2

Tarea	Descripción	Habilidades requeridas
Cree una instancia de EC2	1. Crear una instancia EC2. 2. Instale Oracle 12CR2 en la instancia de EC2 para que sirva como base de datos transitoria de Oracle.	Administración de Oracle
Prepare la base de datos transitoria.	Prepare la base de datos transitoria de Oracle para restaurarla como actualización en Oracle 12CR2 realizando la copia de seguridad en RMAN del entorno de origen de la base de datos Oracle 8i o 9i. Para obtener más informaci ón, consulte la Guía del usuario de Oracle 9i Recovery Manager y la Guía del usuario de copia de seguridad y recuperación de bases de datos en la documentación de Oracle.	Administración de Oracle
Configurar. SharePlex	Configure el SharePlex origen como una base de datos Oracle 8i o 9i local y configure el destino como la base de datos provisional Oracle 12CR2 alojada en Amazon EC2.	SharePlex, administración de Oracle

Configure Amazon RDS para Oracle como su entorno objetivo

Tarea	Descripción	Habilidades requeridas
Crear una instancia de base de datos de Oracle.	Cree una base de datos Amazon RDS para Oracle y, a continuación, conecte Oracle 12CR2 a la base de datos. Para más información, consulte Crear una instancia de base de datos de Oracle y conectarse a una base de datos en una instancia de base de datos en Oracle en la documentación de Amazon RDS.	Administrador de base de datos
Restaure Amazon RDS para Oracle desde la base de datos transitoria.	1. Realice una copia de seguridad de EXPDP del servidor de base de datos transitorio de Oracle mediante `FLASHBACK_SCN` . 2. Restaure Amazon RDS para Oracle desde la base de datos transitoria. Para obtener más informaci ón, consulte 54 DBMS_DATA PUMP en la documentación de Oracle.	Administrador de base de datos

Configure AWS DMS

Tarea	Descripción	Habilidades requeridas
Cree puntos de conexión para las bases de datos.	Cree un punto de conexión de origen para la base de datos transitoria de Oracle y un punto de conexión de destino para la base de datos Amazon RDS para Oracle. Para obtener más información, consulte ¿Cómo puedo crear puntos de conexión de origen o de destino con AWS DMS? en el Centro de conocimientos de AWS.	Administrador de base de datos
Crear una instancia de replicación.	Use AWS DMS para lanzar una instancia de replicación de la base de datos transitoria de Oracle en la base de datos Amazon RDS para Oracle. Para obtener más información, consulte el tema ¿Cómo crear una instancia de replicación de AWS DMS? en el Centro de conocimientos de AWS.	Administrador de base de datos
Crear e iniciar tareas de replicación.	Cree tareas de replicación de AWS DMS para la captura de datos de cambios (CDC) usando `FLASHBACK_SCN` de EXPDP (dado que la carga completa ya se ha realizado a través de EXPDP).	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Para obtener más información, consulte Crear una tarea en la documentación de AWS DMS.	

Transicione a Amazon RDS para Oracle

Tarea	Descripción	Habilidades requeridas
Detenga la carga de trabajo de la aplicación.	Detenga los servidores de aplicaciones y sus aplicaciones durante el período de transición previsto.	Desarrollador de aplicaciones, administrador de base de datos
Valide la sincronización de la base de datos transitoria de Oracle en las instalaciones con la instancia EC2.	Confirme que se hayan publicado todos los mensajes para las tareas de replicación desde la instancia de SharePlex replicación a la base de datos provisional de Oracle en Amazon EC2 realizando algunos cambios de registro en la base de datos de origen local. Para obtener más información, consulte 6.4.2 Cambiar un archivo de registro en la documentación de Oracle.	Administrador de base de datos
Valide la sincronización de la base de datos transitoria de Oracle con la base de datos Amazon RDS para Oracle.	Confirme que sus tareas de AWS DMS no presentan retrasos ni errores y, a continuación, compruebe el estado de validación de las tareas.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Detenga la replicación SharePlex de Amazon RDS.	Si tanto la replicación SharePlex de AWS DMS como la de AWS no muestran ningún error, detenga ambas replicaciones.	Administrador de base de datos
Reasigne la aplicación a Amazon RDS.	Comparta los detalles del punto de conexión de Amazon RDS para Oracle con el servidor de aplicaciones y sus aplicaciones y, a continuación, inicie la aplicación para reanudar las operaciones empresariales.	Desarrollador de aplicaciones, administrador de base de datos

Pruebe el entorno de destino de AWS

Tarea	Descripción	Habilidades requeridas
Pruebe el entorno de base de datos transitoria de Oracle en AWS.	1. Pruebe la SharePlex replicación y compruebe que no haya brechas de sincronización ni errores de replicación en la base de datos provisional de Oracle. 2. Verifique que la aplicación se comporta según lo esperado mediante los puntos de referencia definidos en el entorno en las instalaciones.	SharePlex, administración de Oracle
Pruebe el entorno de Amazon RDS.	1. Compruebe que todos los datos propagados a	Administración de Oracle

Tarea	Descripción	Habilidades requeridas
	Amazon RDS después de la replicación estén libres de errores. 2. Apunte otra aplicación a la instancia de base de datos de Amazon RDS y, a continuación, ejecute pruebas de rendimiento para verificar el comportamiento esperado. Para obtener más información, consulte Amazon RDS para Oracle en la documentación de Amazon RDS.	

Recursos relacionados

- Migre con confianza
- Amazon EC2
- Amazon RDS para Oracle
- AWS Database Migration Service (AWS DMS)
- Depuración de las migraciones a AWS DMS: qué hacer cuando las cosas van mal (parte 1)
- Depuración de las migraciones a AWS DMS: qué hacer cuando las cosas van mal (parte 2)
- Depuración de las migraciones a AWS DMS: ¿qué hacer cuando las cosas van mal? (Parte 3)
- SharePlex para la replicación de bases de datos
- SharePlex: replicación de bases de datos para cualquier entorno

Supervisar Amazon Aurora en busca de instancias sin cifrado

Documento creado por Mansi Suratwala (AWS)

Entorno: producción	Tecnologías: Seguridad, identidad, conformidad; almacenamiento y copia de seguridad; bases de datos	Carga de trabajo: código abierto; Todas las demás cargas de trabajo
Servicios de AWS: Amazon SNS; Amazon Aurora; AWS; CloudTrail Amazon CloudWatch; AWS Lambda		

Resumen

Este patrón proporciona una CloudFormation plantilla de Amazon Web Services (AWS) que puede implementar para configurar notificaciones automáticas cuando se crea una instancia de Amazon Aurora sin el cifrado activado.

Aurora es un motor de base de datos relacional completamente administrado compatible con MySQL y PostgreSQL. Con algunas cargas de trabajo, Aurora puede proporcionar hasta cinco veces el rendimiento de MySQL y hasta tres veces el rendimiento de PostgreSQL sin requerir cambios en la mayoría de las aplicaciones existentes.

La CloudFormation plantilla crea un evento de Amazon CloudWatch Events y una función de AWS Lambda. El evento usa AWS CloudTrail para monitorear la creación de cualquier instancia de Aurora o la restauración puntual de una instancia existente. El evento Cloudwatch Events inicia la función de Lambda, que comprueba si el cifrado está habilitado. Si el cifrado no está activado, la función de Lambda envía una notificación de Amazon Simple Notification Service (Amazon SNS) informándolo de la infracción.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa

Limitaciones

- Este control de servicio solo funciona con las instancias de Amazon Aurora. No admite otras instancias de Amazon Relational Database Service (Amazon RDS).
- La CloudFormation plantilla debe implementarse únicamente para `CreateDBInstance` y `RestoreDBClusterToPointInTim` e.

Versiones de producto

- Versiones de PostgreSQL compatibles con Amazon Aurora
- Versiones de MySQL compatibles con Amazon Aurora

Arquitectura

Pila de tecnología de destino

- Amazon Aurora
- AWS CloudTrail
- Amazon CloudWatch
- AWS Lambda
- Amazon Simple Storage Service (Amazon S3)
- Amazon SNS

Arquitectura de destino

Automatizar y escalar

Puedes usar la CloudFormation plantilla varias veces para diferentes regiones y cuentas. Debe ejecutarla solo una vez en cada región o cuenta.

Herramientas

Herramientas

- Amazon Aurora: Amazon Aurora es un motor de base de datos relacional completamente administrado compatible con MySQL y PostgreSQL.

- AWS CloudTrail: AWS le CloudTrail ayuda a gestionar la gobernanza, el cumplimiento y la auditoría operativa y de riesgos de su cuenta de AWS. Las acciones realizadas por un usuario, un rol o un servicio de AWS se registran como eventos en CloudTrail.
- Amazon CloudWatch Events: Amazon CloudWatch Events ofrece una near-real-time secuencia de eventos del sistema que describen los cambios en los recursos de AWS.
- AWS Lambda es un servicio informático que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo.
- Amazon S3 – Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos altamente escalable que se puede utilizar para una amplia gama de soluciones de almacenamiento, incluyendo sitios web, aplicaciones móviles, copias de seguridad y lagos de datos.
- Amazon SNS – Amazon Simple Notification Service (Amazon SNS) es un servicio gestionado que proporciona la entrega de mensajes mediante Lambda, HTTP, correo electrónico, notificaciones push móviles y mensajes de texto móviles (SMS).

Código

El archivo .zip del proyecto está disponible como adjunto.

Epics

Cree el bucket de S3 para el script de Lambda

Tarea	Descripción	Habilidades requeridas
Definir el bucket de S3.	Abra la consola de Amazon S3 y elija o cree un bucket de S3. Este bucket de S3 alojará el archivo .zip de código Lambda. Su bucket de S3 debe estar en la misma región que Aurora. El nombre del bucket de S3 no puede incluir barras diagonales iniciales.	Arquitecto de la nube

Cargue el código Lambda en el bucket de S3

Tarea	Descripción	Habilidades requeridas
Cargue el código Lambda.	Cargue el archivo .zip de código Lambda proporcio nado en la sección Archivos adjuntos en el bucket S3 que haya definido.	Arquitecto de la nube

Implemente la CloudFormation plantilla

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation plantilla.	En la CloudFormation consola, implementa la `RDS_Auror a_Encryption_At_Re st.yml` CloudFormation plantilla que se proporcio na como adjunto a este patrón. En la siguiente Epic, proporcione los valores de los parámetros.	Arquitecto de la nube

Complete los parámetros de la CloudFormation plantilla

Tarea	Descripción	Habilidades requeridas
Proporcione el nombre del bucket de S3.	Escriba el nombre de bucket de S3 que ha creado o elegido en la primera Epic.	Arquitecto de la nube
Proporcione la clave S3.	Proporcione la ubicación del archivo .zip de código Lambda en su bucket de S3 sin barras diagonales iniciales (por	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	ejemplo, `<directory>/<file-name>.zip`).	
Proporcione una dirección de correo electrónico.	Proporcione una dirección de correo electrónico activa en la que desea recibir las notificaciones de Amazon SNS.	Arquitecto de la nube
Defina el nivel de registro.	Defina el nivel y la frecuencia de registro de la función de Lambda. `Info` designa mensajes informativos detallados sobre el progreso de la aplicación. `Error` designa los eventos de error que aún podrían permitir que la aplicación siguiera ejecutándose. `Warning` designa situaciones potencialmente dañinas.	Arquitecto de la nube

Confirmar la suscripción

Tarea	Descripción	Habilidades requeridas
Confirmar la suscripción.	Cuando la plantilla se implementa correctamente, se envía un mensaje de correo electrónico de suscripción a la dirección de correo electrónico proporcionada. Debe confirmar esta suscripción de correo electrónico para	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	comenzar a recibir notificac iones.	

Recursos relacionados

- Crear un bucket de S3
- Cargar los archivos en un bucket de S3
- Creación de un clúster de base de datos de Amazon Aurora
- Crear una regla de CloudWatch eventos que se active en una llamada a la API de AWS mediante AWS CloudTrail

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Supervise GoldenGate los registros de Oracle mediante Amazon CloudWatch

Documento creado por Chithra Krishnamurthy (AWS)

Entorno: Producción	Tecnologías: bases de datos	Carga de trabajo: Oracle
Servicios de AWS: Amazon CloudWatch; Amazon SNS		

Resumen

Oracle GoldenGate proporciona replicación en tiempo real entre Amazon Relational Database Service (Amazon RDS) para bases de datos Oracle, o entre bases de datos Oracle alojadas en Amazon Elastic Compute Cloud (Amazon EC2). Admite la replicación unidireccional y bidireccional.

Cuando se utiliza GoldenGate para la replicación, la supervisión es fundamental para comprobar que el GoldenGate proceso está en funcionamiento y garantizar que las bases de datos de origen y destino estén sincronizadas.

Este patrón explica los pasos para implementar la CloudWatch supervisión de Amazon para un registro de GoldenGate errores y cómo configurar alarmas para enviar notificaciones de eventos específicos, por ejemplo, para `ABEND` que pueda tomar las medidas adecuadas para reanudar la replicación rápidamente. `STOP`

Requisitos previos y limitaciones

Requisitos previos

- GoldenGate instalado y configurado en una instancia EC2, para que pueda configurar la CloudWatch supervisión en esas instancias EC2. Si desea supervisar la replicación bidireccional GoldenGate en todas las regiones de AWS, debe instalar el CloudWatch agente en cada instancia de EC2 en la que se ejecute el GoldenGate proceso.

Limitaciones

- Este patrón explica cómo monitorear el GoldenGate proceso mediante el uso de. CloudWatch CloudWatch no supervisa el retraso en la replicación ni los problemas de sincronización de datos durante la replicación. Debe ejecutar consultas SQL independientes para controlar el retraso en la replicación o los errores relacionados con los datos, tal como se explica en la GoldenGate documentación.

Versiones de producto

- Este documento se basa en la implementación de Oracle GoldenGate 19.1.0.0.4 para Oracle en Linux x86-64. Sin embargo, esta solución es aplicable a todas las versiones principales de. GoldenGate

Arquitectura

Pila de tecnología de destino

- GoldenGate binarios para Oracle instalados en una instancia EC2
- Amazon CloudWatch
- Amazon Simple Notification Service (Amazon SNS)

Arquitectura de destino

Herramientas

Servicios de AWS

- Amazon CloudWatch es un servicio de supervisión que se utiliza en este patrón para supervisar los registros GoldenGate de errores.
- Amazon SNS es un servicio de notificación de mensajes que se utiliza en este patrón para enviar notificaciones por correo electrónico.

Otras herramientas

- Oracle GoldenGate es una herramienta de replicación de datos que puede utilizar para las bases de datos Amazon RDS for Oracle o las bases de datos Oracle alojadas en Amazon EC2.

Pasos de implementación de alto nivel

1. Cree un rol de AWS Identity and Access Management (IAM) para el CloudWatch agente.
2. Adjunte la función de IAM a la instancia EC2 en la que se generan los registros GoldenGate de errores.
3. Instale el CloudWatch agente en la instancia EC2.
4. Configure los archivos de configuración del CloudWatch agente: `awscli.conf` `yawslogs.conf`.
5. Inicie el CloudWatch agente.
6. Cree filtros de métricas en el grupo de registros.
7. Configure Amazon SNS.
8. Cree una alarma para los filtros de métricas. Amazon SNS envía alertas por correo electrónico cuando esos filtros capturan eventos.

Para obtener instrucciones, consulte la sección siguiente.

Epics

Paso 1. Cree un rol de IAM para el agente CloudWatch

Tarea	Descripción	Habilidades requeridas
Cree el rol de IAM.	El acceso a los recursos de AWS requiere permisos, por lo que debe crear funciones de IAM para incluir los permisos necesarios para que cada servidor ejecute el CloudWatch agente. Para crear el rol de IAM: 1. Inicie sesión en la consola de administración de AWS y abra la consola de IAM en https://console.aws.amazon.com/iam/.	AWS general

Tarea	Descripción	Habilidades requeridas
	2. En el panel de navegación, seleccione Roles y luego seleccione Crear rol. 3. En Trusted entity type (Tipo de entidad de confianza), seleccione AWS service. 4. En Common use cases (Casos de uso común), seleccione EC2 y, a continuación, Next. 5. En la lista de políticas, seleccione la casilla de verificación situada junto a CloudWatchAgentServerPolicy. Si es necesario, utilice el cuadro de búsqueda para encontrar la política. 6. Elija Siguiente. 7. En Role name (Nombre del rol), escriba un nombre para el rol nuevo (por ejemplo, `goldengate-cw-monitoring-role` o el nombre que prefiera). 8. (Opcional) En Role description (Descripción del rol), escriba una descripción. 9. Confirme que CloudWatchAgentServerPolicy aparece en el nombre de la política. 10. (Opcional) Agregue una o varias etiquetas (pares	

Tarea	Descripción	Habilidades requeridas
	clave-valor) para organizar o controlar el acceso a este rol o realizar su seguimiento y, a continuación, seleccione Create role (Crear rol).	

Paso 2. Adjunte la función de IAM a la instancia GoldenGate EC2

Tarea	Descripción	Habilidades requeridas
Adjunte la función de IAM a la instancia EC2 en la que se generan los registros de GoldenGate errores.	Los registros de errores generados por GoldenGate deben rellenarse CloudWatch y supervisarse, por lo que debe adjuntar la función de IAM que creó en el paso 1 a la instancia de EC2 en la que se está ejecutando. GoldenGate Para asociar un rol de IAM a una instancia: 1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/. 2. En el panel de navegación, elija Instances y, a continuación, busque la instancia en la que se GoldenGate está ejecutando. 3. Seleccione la instancia y, a continuación, Actions (Acciones), Security	AWS general

Tarea	Descripción	Habilidades requeridas
	(Seguridad), Modify IAM role (Modificar rol de IAM). 4. Seleccione el rol de IAM creado en el primer paso para asociarlo con la instancia y seleccione Save (Guardar).	

Pasos 3 a 5. Instale y configure el CloudWatch agente en la instancia EC2 de Goldengate

Tarea	Descripción	Habilidades requeridas
Instale el CloudWatch agente en la instancia EC2. GoldenGate	Para instalar el agente, ejecute el siguiente comando: `sudo yum install -y awslogs`	AWS general
Edite los archivos de configuración del agente.	1. Ejecute el siguiente comando de la . `sudo su -` 2. Edite este archivo para actualizar la región de AWS según sea necesario. `cat /etc/awslogs/conf [plugins] cwlogs = cwlogs [default] region = us-east-1` 3. Edite el archivo `/etc/awslogs/awslogs.conf` para actualiza	AWS general

Tarea	Descripción	Habilidades requeridas
	r el nombre del archivo, el nombre del grupo de registros y el formato de fecha y hora. Debe especificar la fecha y la hora para que coincidan con el formato de fecha`ggserror.log` ; de lo contrario, el flujo de registro no fluirá hacia. CloudWatch Por ejemplo: `datetime_format = %Y-%m-%dT%H:%M:%S%z` `file = /u03/oracle/oragg/ggserr.log` `log_group_name = goldengate_monitor`	
Inicie el agente. CloudWatch	Para iniciar el agente, utilice el comando siguiente. `$ sudo service awslogsd start` Tras iniciar el agente, podrá ver el grupo de registros en la CloudWatch consola. El flujo de registro incluirá el contenido del archivo.	AWS general

Paso 6. Crear filtros de métricas en el grupo de registros

Tarea	Descripción	Habilidades requeridas
Cree filtros de métricas para las palabras clave ABEND y STOPPED.	Al crear filtros de métricas para el grupo de registros , cada vez que los filtros se identifican en el registro de errores, se activa una alarma y se envía una notificación por correo electrónico basada en la configuración de Amazon SNS. Para crear un filtro de métricas: 1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/. 2. Elija el nombre del grupo de registros. 3. Elija Actions (Acciones) y, a continuación, seleccione Create metric filter (Crear filtro de métrica). 4. En Filter pattern (Patrón de filtro), especifique un patrón como `ABEND`. 5. Elija Next (Siguiente) y luego ingrese un nombre para el filtro de métricas. 6. En Detalles de la métrica, en Espacio de nombres de métricas, introduzca un	CloudWatch

Tarea	Descripción	Habilidades requeridas
	nombre para el espacio de CloudWatch nombres en el que se publicará la métrica. Si este espacio de nombres no existe todavía, asegúrese de que la opción Create new (Crear nuevo) esté seleccionada. 7. En Metric value (Valor de la métrica), especifique 1, ya que el filtro de métrica cuenta las ocurrencias de las palabras clave en el filtro. 8. Defina Unit como None (Ninguna). 9. Elija Create metric filter (Crear filtro de métricas) . Puede encontrar el filtro de métricas que ha creado desde el panel de navegación. 10. Cree otro filtro de métricas para el patrón `STOPPED`. Dentro de un grupo de registros, puede crear varios filtros de métricas y configurar las alarmas de forma individual.	

Paso 7. Configurar Amazon SNS

Tarea	Descripción	Habilidades requeridas
Cree un tema de SNS.	En este paso, configurará Amazon SNS para crear alarmas para los filtros de métricas. Para crear un tema de SNS: 1. Inicie sesión en la consola de Amazon SNS en https://console.aws.amazon.com/sns/home. 2. En Create topic (Crear tema), escriba el nombre de su tema como `goldengate-alert` y, a continuación, seleccione Next step (Paso siguiente). 3. En Tipo, seleccione Estándar. 4. Desplácese hasta el final del formulario y elija Create topic (Crear tema). En la consola se abre la página Details (Detalles) del nuevo tema.	Amazon SNS
Cree una suscripción.	Para crear una suscripción al tema: 1. En el panel de navegación izquierdo, elija Suscripciones.	Amazon SNS

Tarea	Descripción	Habilidades requeridas
	2. En la página Subscript ions (Suscripciones), elija Create subscription (Crear suscripción). 3. En la página Create subscription (Crear una suscripción), seleccione el campo Topic ARN (ARN del tema) para ver una lista de los temas de la cuenta de AWS. 4. Elija el tema que creó en el paso anterior. 5. En Protocolo, elija Correo electrónico. 6. En Endpoint (Punto de conexión), ingrese una dirección de correo electrónico que pueda utilizar para recibir notificac iones. 7. Seleccione Create subscript ion (Crear suscripción). La consola abre la página Details (Detalles) de la suscripción. 8. Revise la bandeja de entrada del correo electróni co en busca de un mensaje de AWS Notifications y, a continuación, seleccion e Confirm subscription (Confirmar la suscripción) en el correo electrónico.	

Tarea	Descripción	Habilidades requeridas
	En Amazon SNS, se abre su navegador web y se muestra una confirmación de suscripción con su ID de suscripción.	

Paso 8. Crear una alarma para enviar notificaciones a los filtros de métricas

Tarea	Descripción	Habilidades requeridas
Cree una alarma para el tema de SNS.	Para crear una alarma basada en un filtro de métricas del grupo de registros: 1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/. 2. En el panel de navegación, elija Logs (Registros) y, luego, Log groups (Grupos de registro). 3. Elija el grupo de registro que incluye el filtro de métricas. 4. Elija Metric filters (Filtros de métricas). 5. En la pestaña Metric filters (Filtros de métricas), seleccione la casilla del filtro de métricas en el que quiera basar la alarma. 6. Elija Crear alarma.	CloudWatch

Tarea	Descripción	Habilidades requeridas
	7. En Conditions, especifiq ue lo siguiente en cada sección: • En Threshold type (Tipo de umbral), elija Static (Estático). • En Whenever <metric-n ame> is . . ., seleccione Greater (Mayor que). • En than . . ., especifique 0. 8. Elija Siguiente. 9. En Notification: • En Alarm state trigger (Desencadenador de estado de alarma), elija In Alarm (En alarma). • En Send notification to following SNS topic (Enviar notificación para el tema de SNS siguiente), seleccione Select an existing topic (Seleccio nar un tema existente). • En la bandeja de correo electrónico, seleccion e el tema de Amazon SNS que creó en el paso anterior. 10. Elija Siguiente. 11. En Name and description (Nombre y descripción),	

Tarea	Descripción	Habilidades requeridas
	ingrese un nombre y una descripción para la alarma. Nota: En la descripci ón, puede especificar el nombre de la instancia para que el correo electrónico de notificación sea descriptivo. 12 En Preview and create (Previsualizar y crear), compruebe que su configuración sea correcta y seleccione Create alarm (Crear alarma). Tras estos pasos, cada vez que se detecten estos patrones en el archivo de registro de GoldenGate errores (`ggserr.log`) que está supervisando, recibirá una notificación por correo electrónico.	

Solución de problemas

Problema	Solución
El flujo de registro del registro de GoldenGate errores no fluye hacia él CloudWatch.	Compruebe el archivo `/etc/awslogs/awslogs.conf` para verificar el nombre del archivo, el nombre del grupo de registros y el formato de fecha y hora. Debe especificar la fecha/hora de modo que coincidan con el formato de fecha de `ggserror.log` . De lo

Problema	Solución
	contrario, el flujo de registro no fluirá hacia él CloudWatch.

Recursos relacionados

- CloudWatch Documentación de Amazon
- Recopilación de métricas y registros con el CloudWatch agente
- Documentación de Amazon SNS

Redefina la plataforma de Oracle Database Enterprise Edition a Standard Edition 2 en Amazon RDS para Oracle

Creado por Lanre showunmi (AWS) y Tarun Chawla (AWS)

Entorno: producción	Origen: en las instalaciones	Destino: Amazon RDS
Tipo R: redefinir la plataforma	Carga de trabajo: Oracle	Tecnologías: bases de datos
Servicios de AWS: Amazon RDS		

Resumen

Oracle Database Enterprise Edition (EE) es una opción popular para ejecutar aplicaciones en muchas empresas. Sin embargo, en algunos casos, las aplicaciones utilizan pocas o ninguna de las características de Oracle Database EE, por lo que no está justificado incurrir en enormes costos de licencia. Al migrar a Amazon RDS, puede ahorrar costos al cambiar la versión de dichas bases de datos a Oracle Database Standard Edition 2 (SE2).

Este patrón describe cómo cambiar la versión de Oracle Database EE a Oracle Database SE2 al migrar de una base de datos en las instalaciones a Amazon RDS para Oracle. Los pasos que se presentan en este patrón también se aplican si su base de datos EE Oracle ya se está ejecutando en Amazon RDS o en una instancia de Amazon Elastic Compute Cloud (Amazon EC2).

Para obtener más información, consulte la guía Recomendaciones de AWS sobre cómo evaluar el cambio de versión de las bases de datos de Oracle a la edición estándar 2 en AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Oracle Database Enterprise Edition
- Una herramienta de cliente, como Oracle SQL Developer o SQL*Plus, para conectarse a oo ejecutar comandos SQL en la base de datos de Oracle

- Usuario de base de datos para realizar la evaluación; por ejemplo, uno de los siguientes:
  - Usuario con privilegios suficientes para ejecutar la evaluación de la Herramienta de conversión de esquemas de AWS (AWS SCT)
  - Usuario con privilegios suficientes para ejecutar consultas SQL en las tablas del diccionario de bases de datos de Oracle
- Usuario de base de datos para realizar la migración de base de datos; por ejemplo, uno de los siguientes:
  - Usuario con privilegios suficientes para ejecutar AWS Database Migration Service (AWS DMS)
  - Usuario con privilegios suficientes para realizar la exportación e importación de Oracle Data Pump
  - Usuario con privilegios suficientes para ejecutar Oracle GoldenGate

Limitaciones

- Amazon RDS para Oracle tiene un tamaño máximo de la base de datos. Para obtener más información, consulte Almacenamiento de instancias de base de datos de Amazon RDS.

Versiones de producto

La lógica general descrita en este documento se aplica a las versiones de Oracle de la versión 9i y posteriores. Para ver las versiones compatibles de las bases de datos autogestionadas y de Amazon RDS para Oracle, consulte la documentación de AWS DMS.

Para identificar el uso de características en los casos en que no se admite AWS SCT, ejecute consultas SQL en la base de datos de origen. Para migrar desde versiones anteriores de Oracle en las que no se admiten AWS DMS y Oracle Data Pump, utilice las utilidades de exportación e importación de Oracle.

Para obtener una lista actualizada de las versiones y ediciones compatibles, consulte Oracle en Amazon RDS en la documentación de AWS. Para obtener más información sobre los precios y las clases de instancias compatibles, consulte Precios de Amazon RDS para Oracle.

Arquitectura

Pila de tecnología de origen

- Oracle Database Enterprise Edition que se ejecuta en las instalaciones o en Amazon EC2

Pila de tecnología de destino con herramientas nativas de Oracle

- Amazon RDS para Oracle ejecuta Oracle Database SE2

1. Exporte datos mediante Oracle Data Pump.
2. Copie los archivos de volcado a Amazon RDS a través de un enlace a una base de datos.
3. Importe los archivos de volcado a Amazon RDS mediante Oracle Data Pump.

Pila de tecnología de destino con AWS DMS

- Amazon RDS para Oracle ejecuta Oracle Database SE2
- AWS DMS

1. Exporte datos mediante Oracle Data Pump con FLASHBACK_SCN.
2. Copie los archivos de volcado a Amazon RDS a través de un enlace a una base de datos.
3. Importe los archivos de volcado a Amazon RDS mediante Oracle Data Pump.
4. Utilice la captura de datos de cambio de AWS DMS (CDC).

Herramientas

Servicios de AWS

- AWS Database Migration Service (AWS DMS) le permite migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones.
- Amazon Relational Database Service (Amazon RDS) lo ayuda a configurar, utilizar y escalar una base de datos (DB) relacional en la nube de AWS. Este patrón utiliza Amazon RDS para Oracle.
- AWS SCT ofrece una interfaz de usuario basada en proyectos para evaluar, convertir y copiar automáticamente el esquema de base de datos de su base de datos de Oracle de origen a un formato compatible con Amazon RDS para Oracle. AWS SCT le permite analizar los posibles ahorros de costos que se pueden lograr al cambiar el tipo de licencia de Enterprise Edition a Standard Edition de Oracle. La sección Evaluación de licencias y soporte en la nube del informe

SCT de AWS proporciona información detallada sobre las características de Oracle en uso para que pueda tomar una decisión informada al migrar a Amazon RDS para Oracle.

Otras herramientas

- Las utilidades de importación y exportación nativas de Oracle admiten mover datos de Oracle dentro y fuera de las bases de datos de Oracle. Oracle ofrece dos tipos de utilidades de importación y exportación de bases de datos: Oracle Export and Import (para versiones anteriores) y Oracle Data Pump Export and Import (disponible en Oracle Database 10g y versiones posteriores).
- Oracle GoldenGate ofrece capacidades de replicación en tiempo real para que pueda sincronizar su base de datos de destino después de una carga inicial. Esta opción puede ayudar a reducir el tiempo de inactividad de las aplicaciones durante la puesta en marcha.

Epics

Realice una evaluación previa a la migración

Tarea	Descripción	Habilidades requeridas
Valide los requisitos de la base de datos para sus aplicaciones.	Asegúrese de que sus aplicaciones estén certificadas para ejecutarse en Oracle Database SE2. Consulte directamente con el proveedor del software, el desarrollador o la documentación de la aplicación.	Desarrollador de aplicaciones, administrador de bases de datos, propietario de la aplicación
Investigue el uso de las características de EE directamente en la base de datos.	Para determinar el uso de la característica EE, lleve a cabo alguna de las siguientes operaciones: • Genere un informe de evaluación de AWS SCT para su base de datos	Administrador de base de datos, propietario de la aplicación, desarrollador de la aplicación

Tarea	Descripción	Habilidades requeridas
	Oracle EE. El informe le indica qué características de su base de datos EE actual deberían eliminarse si desea cambiar el tio de licencia. • Si tiene una cuenta de Oracle Support, obtenga y ejecute el script `options_packs_usage_statistics.sql` del documento de soporte 1317265.1 para generar un informe de las opciones y características que se utilizan en la base de datos Oracle. • Consulte DBA_FEATURE_USAGE_STATISTICS para ver los detalles de todas las características que están en uso.	

Tarea	Descripción	Habilidades requeridas
Identifique el uso de las características de EE para las actividades operativas.	Los administradores de bases de datos o aplicaciones a veces utilizan características exclusivas de EE para sus actividades operativas. Algunos ejemplos comunes incluyen las actividades de mantenimiento en línea (reconstrucción de índices, movimiento de tablas) y el uso del paralelismo en los trabajos por lotes. Estas dependencias se pueden mitigar modificando las operaciones siempre que sea posible. Identifique el uso de estas características y tome una decisión basada en el coste en comparación con los beneficios. Utilice la tabla de comparación de características de Oracle Database EE y SE2 como guía para identificar las características que están disponibles en Oracle Database SE2.	Desarrollador de aplicaciones, administrador de bases de datos, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Revise los patrones de carga de trabajo de la base de datos EE Oracle.	La base de datos Oracle SE2 restringe automáticamente el uso a un máximo de 16 subprocesos de CPU en cualquier momento. Si su base de datos Oracle EE tiene licencia para utilizar el paquete de diagnóstico de Oracle, utilice la herramien ta Automatic Workload Repository (AWR), o las vistas DBA_HIST_*, para analizar los patrones de carga de trabajo de la base de datos y determinar si el límite máximo de 16 subprocesos de la CPU afectará negativamente a los niveles de servicio al pasar a SE2. Asegúrese de que su evaluación cubra los períodos de máxima actividad, como el procesamiento al final del día, del mes o del año.	Administrador de base de datos, propietario de la aplicación, desarrollador de aplicaciones

Prepare la infraestructura de destino en AWS

Tarea	Descripción	Habilidades requeridas
Implemente y configure la infraestructura de redes.	Cree una nube privada virtual (VPC) y subredes, grupos de	Administrador de AWS, arquitecto de nube, administr

Tarea	Descripción	Habilidades requeridas
	seguridad y listas de control de acceso a la red.	ador de redes, DevOps ingeniero
Aprovisione la base de datos Amazon RDS para Oracle SE2.	Aprovisione la base de datos Amazon RDS para Oracle SE2 de destino para cumplir con los requisitos de rendimiento, disponibilidad y seguridad de sus aplicaciones. Recomendamos zonas de disponibilidad múltiples para las cargas de trabajo de producción. Sin embargo, para mejorar el rendimiento de la migración, puede aplazar la activación de zonas de disponibilidad múltiples hasta después de la migración de datos.	Administrador de nube, arquitecto de nube, DBA, DevOps ingeniero, administrador de AWS
Personalice el entorno de Amazon RDS.	Configure parámetros y opciones personalizados y habilite una supervisión adicional. Para obtener más información, consulte Prácticas recomendadas para migrar a Amazon RDS para Oracle.	Administrador de AWS, administrador de sistemas de AWS, administrador de la nube, administrador de bases de datos, arquitecto de la nube

Realice la migración, el simulacro y las pruebas de la aplicación

Tarea	Descripción	Habilidades requeridas
Migre los datos (simulacro).	Migre los datos de la base de datos Oracle EE de origen a	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	la instancia de base de datos Amazon RDS para Oracle SE2 mediante el enfoque que mejor se adapte a su entorno específico. Seleccione una estrategia de migración en función de factores como el tamaño, la complejidad y el período de inactividad disponible. Use una de las siguientes o una combinación de ellas: • Herramientas nativas de Oracle, como Oracle Data Pump (recomendada), las utilidades Oracle Import-Export y Oracle. GoldenGate • AWS DMS, que utiliza toda la carga con replicación continua a través de CDC.	
Validar la base de datos objetivo.	Realice una validación posterior a la migración del almacenamiento de la base de datos y de los objetos de código. Revise los registros de migración y solucione los problemas detectados. Para obtener más información, consulte la guía Migración de bases de datos de Oracle a la nube de AWS.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Pruebe las aplicaciones.	Los administradores de aplicaciones y bases de datos deben realizar pruebas funcionales, de rendimien to y operativas según corresponda. Para obtener más información, consulte Prácticas recomendadas para migrar a Amazon RDS para Oracle. Por último, obtenga la aprobación de las partes interesadas sobre los resultados de las pruebas.	Desarrollador de aplicaciones, propietario de aplicaciones, ingeniero de migraciones, jefe de migraciones

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Actualice los datos de Oracle Database EE.	Seleccione un enfoque de actualización de datos en función del requisito de disponibilidad de la aplicació n. Para obtener más informaci ón, consulte los métodos de migración en Estrategias de migración de bases de datos de Oracle a AWS. Por ejemplo, puede lograr un tiempo de inactividad prácticamente nulo mediante el uso de herramientas como Oracle GoldenGate o AWS	Propietario de aplicaciones, jefe de transición, administr ador de base de datos, ingeniero de migraciones, jefe de migraciones

Tarea	Descripción	Habilidades requeridas
	DMS con replicación continua. Si el período de inactividad lo permite, puede realizar la transición final de los datos mediante métodos fuera de línea, como Oracle Data Pump o las utilidades Original Export-Import.	
Dirija las aplicaciones a la instancia de la base de datos de destino.	Actualice los parámetros de conexión en las aplicaciones y otros clientes para que se dirijan a la base de datos Amazon RDS para Oracle SE2.	Desarrollador de aplicaciones, propietario de aplicaciones, ingeniero de migraciones, jefe de migraciones, jefe de transición
Realice actividades posteriores a la migración.	Realice tareas posteriores a la migración de datos, como habilitar las zonas de disponibilidad múltiples, la validación de datos y otras comprobaciones.	Administrador de base de datos, ingeniero de migraciones
Realice una supervisión posterior a la transición.	Utilice herramientas como Amazon CloudWatch y Amazon RDS Performance Insights para supervisar la base de datos Amazon RDS for Oracle SE2.	Desarrollador de aplicaciones, propietario de aplicaciones, administrador de AWS, administrador de bases de datos, ingeniero de migraciones

Recursos relacionados

Recomendaciones de AWS

- Migración de bases de datos de Oracle a la nube de AWS (guía)

- Evalúe cambiar la versión de las bases de datos de Oracle a Standard Edition 2 en AWS (guía)
- Migre una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle (patrón)
- Migre una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle mediante Oracle Data Pump (patrón)

Publicaciones de blog

- Migración de bases de datos de Oracle con un tiempo de inactividad prácticamente nulo mediante AWS DMS
- Análisis del manejo del rendimiento en Oracle SE mediante Amazon RDS para Oracle
- Administración de su plan SQL en Oracle SE con Amazon RDS para Oracle
- Implementación del particionamiento de tablas en Oracle Standard Edition: primera parte

Replicar bases de datos de unidades centrales en AWS mediante Precisely Connect

Creado por Lucio Pereira (AWS), Balaji Mohan (AWS) y Sayantan Giri (AWS)

Entorno: producción	Origen: unidad central en las instalaciones	Destino: bases de datos AWS
Tipo R: renovar arquitectura	Carga de trabajo: todas las demás cargas de trabajo	Tecnologías: bases de datos; nativo en la nube; unidad central; modernización
Servicios de AWS: Amazon DynamoDB; Amazon Keyspaces; Amazon MSK; Amazon RDS; Amazon ElastiCache		

Resumen

Este patrón describe los pasos para replicar datos de bases de datos de unidades centrales a los almacenes de datos de Amazon casi en tiempo real mediante Precisely Connect. El patrón implementa una arquitectura basada en eventos con Amazon Managed Streaming para Apache Kafka (Amazon MSK) y conectores de bases de datos personalizados en la nube para mejorar la escalabilidad, la resiliencia y el rendimiento.

Precisely Connect es una herramienta de replicación que captura datos de sistemas de unidades centrales heredados y los integra en entornos en la nube. Los datos se replican desde las unidades centrales a AWS mediante la captura de datos de cambios (CDC) mediante flujos de mensajes prácticamente en tiempo real con canalizaciones de datos heterogéneas de baja latencia y alto rendimiento.

Este patrón también abarca una estrategia de recuperación de desastres para canalizaciones de datos resilientes con replicación de datos multirregional y enrutamiento de conmutación por error.

Requisitos previos y limitaciones

Requisitos previos

- Una base de datos de unidad central existente, por ejemplo, IBM DB2, IBM Information Management System (IMS) o Virtual Storage Access Method (VSAM), que desee replicar en la nube de AWS
- Una cuenta de AWS activa.
- AWS Direct Connect o red privada virtual de AWS (AWS VPN) desde su entorno corporativo a AWS
- Una nube privada virtual con una subred a la que pueda acceder su plataforma antigua

Arquitectura

Pila de tecnología de origen

Un entorno de unidad central que incluya al menos una de las siguientes bases de datos:

- Base de datos IBM IMS
- Base de datos IBM DB2
- Archivos VSAM

Pila de tecnología de destino

- Amazon MSK
- Amazon Elastic Kubernetes Service (Amazon EKS) y Amazon EKS Anywhere
- Docker
- Una base de datos relacional o NoSQL de AWS como la siguiente:
  - Amazon DynamoDB
  - Amazon Relational Database Service (Amazon RDS) para Oracle, Amazon RDS para PostgreSQL o Amazon Aurora
  - Amazon ElastiCache para Redis
  - Amazon Keyspaces (para Apache Cassandra)

Arquitectura de destino

Replicación de datos de unidad central en bases de datos de AWS

El siguiente diagrama ilustra la replicación de datos de mainframe en una base de datos de AWS, como DynamoDB, Amazon RDS, Amazon o Amazon Keyspaces ElastiCache. La replicación se produce prácticamente en tiempo real mediante el uso de Precisely Capture y Publisher en su entorno de unidad central en las instalaciones, Precisely Dispatcher en Amazon EKS Anywhere en su entorno distribuido en las instalaciones y Precisely Apply Engine y los conectores de base de datos en la nube de AWS.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Precisely Capture obtiene los datos de unidad central de los registros CDC y los mantiene en un almacenamiento transitorio interno.
2. Precisely Publisher escucha los cambios en el almacenamiento de datos interno y envía los registros de los CDC a Precisely Dispatcher a través de una conexión TCP/IP.
3. Precisely Dispatcher recibe los registros de los CDC de Publisher y los envía a Amazon MSK. Dispatcher crea claves de Kafka en función de la configuración del usuario y de varias tareas de trabajo para enviar los datos en paralelo. Dispatcher envía un acuse de recibo a Publisher cuando los registros se han almacenado en Amazon MSK.
4. Amazon MSK guarda los registros de los CDC en el entorno de nube. El tamaño de las particiones de los temas depende de los requisitos de rendimiento del sistema de procesamiento de transacciones (TPS). La clave de Kafka es obligatoria para seguir ordenando transformaciones y transacciones.
5. Precisely Apply Engine escucha los registros de CDC de Amazon MSK y transforma los datos (por ejemplo, filtrándolos o mapeándolos) en función de los requisitos de la base de datos de destino. Puede añadir una lógica personalizada a los scripts de Precisely SQD. (SQD es el lenguaje propiedad de Precisely). Precisely Apply Engine transforma cada registro de CDC al formato Apache Avro o JSON y lo distribuye a diferentes temas según sus necesidades.
6. Los temas de Kafka de destino contienen los registros CDC en varios temas según la base de datos de destino, y Kafka facilita la ordenación de las transacciones en función de la clave de Kafka definida. Las claves de partición se alinean con las particiones correspondientes para permitir un proceso secuencial.
7. Los conectores de bases de datos (aplicaciones Java personalizadas) escuchan los registros CDC de Amazon MSK y los almacenan en la base de datos de destino.

8. Puede seleccionar una base de datos de destino en función de sus requisitos. Este patrón es compatible con bases de datos NoSQL y relacionales.

Recuperación de desastres

La continuidad empresarial es clave para el éxito de su organización. La nube de AWS proporciona capacidades de alta disponibilidad (HA) y recuperación de desastres (DR), y respalda los planes de conmutación por error y alternativos de su organización. Este patrón sigue una estrategia de DR activa/pasiva y proporciona una guía de alto nivel para implementar una estrategia de DR que cumpla con sus requisitos de RTO y RPO.

En el siguiente diagrama, se ilustra el flujo de trabajo de DR.

En el diagrama se muestra lo siguiente:

1. Se requiere una conmutación por error semiautomática si se produce algún error en la Región de AWS 1. En caso de que se produzca un error en la Región 1, el sistema debe iniciar los cambios de enrutamiento para conectar a Precisely Dispatcher con la Región 2.
2. Amazon MSK replica los datos mediante la duplicación entre regiones. Por este motivo, durante la conmutación por error, hay que promover al clúster de Amazon MSK de la región 2 como líder principal.
3. Precisely Apply Engine y los conectores de bases de datos son aplicaciones sin estado que pueden funcionar en cualquier región.
4. La sincronización de la base de datos depende de la base de datos de destino. Por ejemplo, DynamoDB puede usar tablas globales ElastiCache y almacenes de datos globales.

Procesamiento de baja latencia y alto rendimiento mediante conectores de bases de datos

Los conectores de bases de datos son componentes fundamentales en este patrón. Los conectores siguen un enfoque basado en el oyente para recopilar datos de Amazon MSK y enviar las transacciones a la base de datos mediante un procesamiento de alto rendimiento y baja latencia para aplicaciones de misión crítica (niveles 0 y 1). En el siguiente diagrama se ilustra este proceso.

Este patrón permite desarrollar una aplicación personalizada con un consumo de un solo subproceso mediante un motor de procesamiento de subprocesos múltiples.

1. El proceso principal del conector consume los registros CDC de Amazon MSK y los envía al grupo de subprocesos para su procesamiento.
2. Los subprocesos del grupo de subprocesos procesan los registros de los CDC y los envían a la base de datos de destino.
3. Si todos los subprocesos están ocupados, la cola de subprocesos mantiene en espera los registros de la CDC.
4. El subproceso principal espera a que se borren todos los registros de la cola de subprocesos y envía las compensaciones a Amazon MSK.
5. Los subprocesos secundarios gestionan los errores. Si se producen errores durante el procesamiento, los mensajes fallidos se envían al tema DLQ (cola de mensajes fallidos).
6. Los subprocesos secundarios inician actualizaciones condicionales (consulte Expresiones de condición en la documentación de DynamoDB), en función de la marca de tiempo del mainframe, para evitar cualquier duplicación o actualización en la base de datos. out-of-order

Para obtener información sobre cómo implementar una aplicación de consumidor de Kafka con capacidades de subprocesos múltiples, consulte la entrada del blog Consumo de mensajes multiprocesos con el consumidor de Apache Akfka en el sitio web de Confluent.

Herramientas

Servicios de AWS

- Amazon Managed Streaming para Apache Kafka (Amazon MSK) es un servicio completamente administrado que le permite crear y ejecutar aplicaciones que utilizan Apache Kafka para procesar datos de streaming.
- Amazon Elastic Kubernetes Service (Amazon EKS) lo ayuda a ejecutar Kubernetes en AWS sin necesidad de instalar ni mantener su propio plano de control o nodos de Kubernetes.
- Amazon EKS Anywhere le permite implementar, usar y administrar los clústeres de Kubernetes que se ejecutan en sus propios centros de datos.
- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- Amazon Relational Database Service (Amazon RDS) lo ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS.
- Amazon le ElastiCache ayuda a configurar, gestionar y escalar entornos de caché en memoria distribuidos en la nube de AWS.

- Amazon Keyspaces (para Apache Cassandra) es un servicio de base de datos administrada que le permite migrar, ejecutar y escalar sus cargas de trabajo de Cassandra en la nube de AWS.

Otras herramientas

- Precisely Connect integra los datos de los sistemas de unidad central heredados, como los conjuntos de datos de VSAM o las bases de datos de unidad central de IBM, en plataformas de datos y nube de próxima generación.

Prácticas recomendadas

- Encuentre la mejor combinación de particiones Kafka y conectores multiprocesos para lograr un equilibrio óptimo entre rendimiento y coste. Varias instancias de Precisely Capture y Dispatcher pueden aumentar el coste debido al mayor consumo de MIPS (millones de instrucciones por segundo).
- Evite añadir lógica de manipulación y transformación de datos a los conectores de bases de datos. Para ello, utilice Precisely Apply Engine, que proporciona tiempos de procesamiento en microsegundos.
- Cree solicitudes periódicas o llamadas de comprobación de estado a la base de datos (latidos) en los conectores de la base de datos para calentar la conexión con frecuencia y reducir la latencia.
- Implemente una lógica de validación de grupos de subprocesos para comprender las tareas pendientes en la cola de subprocesos y espere a que se completen todos los subprocesos antes del siguiente sondeo de Kafka. Esto ayuda a evitar la pérdida de datos si un nodo, contenedor o proceso se bloquea.
- Exponga las métricas de latencia a través de puntos de conexión de estado para mejorar las capacidades de observabilidad mediante paneles y mecanismos de rastreo.

Epics

Prepare el entorno de origen (en las instalaciones)

Tarea	Descripción	Habilidades requeridas
Configure el proceso de la unidad central (por lotes o en	1. Identifique el entorno de unidad central.	Ingeniero de unidad central

Tarea	Descripción	Habilidades requeridas
línea) para iniciar el proceso de CDC desde las bases de datos de la unidad central.	2. Identifique las bases de datos de unidad central que participarán en el proceso de los CDC. 3. En el entorno de unidad central, desarrolle un proceso que lance la herramienta de los CDC para capturar los cambios en la base de datos fuente. Para obtener instrucciones, consulte la documentación de su unidad central. 4. Documente el proceso de los CDC, incluida la configuración. 5. Implemente el proceso en entornos de prueba y producción.	
Active los flujos de registro de la base de datos de unidad central.	1. Configure los flujos de registro en el entorno de unidad central para capturar los registros de los CDC. Para obtener instrucciones, consulte la documentación de su unidad central. 2. Pruebe los flujos de registro para asegurarse de que capturan los datos necesarios. 3. Implemente los flujos de registro en entornos de prueba y producción.	Especialista en bases de datos para unidad central

Tarea	Descripción	Habilidades requeridas
Utilice el componente Capture para capturar los registros de los CDC.	1. Instale y configure el componente Precisely Capture en el entorno de la unidad central. Para obtener instrucciones, consulte la documentación de Precisely. 2. Pruebe la configuración para asegurarse de que el componente Capture funciona correctamente. 3. Configure un proceso de replicación para replicar los registros de los CDC capturados mediante el componente Capture. 4. Documente la configuración de Capture para cada base de datos de origen. 5. Desarrolle un sistema de supervisión para garantizar que el componente Capture recopile los registros correctamente a lo largo del tiempo. 6. Implemente la instalación y las configuraciones en los entornos de prueba y producción.	Ingeniero de unidad central, Precisely Connect SME

Tarea	Descripción	Habilidades requeridas
Configure el componente Publisher para que escuche al componente Capture.	1. Instale y configure el componente Precisely Publisher en el entorno de la unidad central. Para obtener instrucciones, consulte la documentación de Precisely. 2. Pruebe la configuración para asegurarse de que el componente Publisher funciona correctamente. 3. Configure un proceso de replicación para publicar los registros de CDC en el componente Precisely Dispatcher de Publisher. 4. Documente la configuración de Publisher. 5. Desarrolle un sistema de supervisión para garantizar que el componente Publisher recopile los registros correctamente a lo largo del tiempo. 6. Implemente la instalación y las configuraciones en los entornos de prueba y producción.	Ingeniero de unidad central, Precisely Connect SME

Tarea	Descripción	Habilidades requeridas
Aprovisione Amazon EKS Anywhere en el entorno distribuido en las instalaciones.	1. Instale Amazon EKS Anywhere en la infraestructura en las instalaciones y asegúrese de que esté configurado correctamente. Para obtener instrucciones, consulte la documentación de Amazon EKS Anywhere. 2. Configure un entorno de red seguro para el clúster de Kubernetes, incluidos los firewalls. 3. Implemente y pruebe la implementación de la aplicación de muestra en el clúster Amazon EKS Anywhere. 4. Implemente capacidades de escalado automático para el clúster. 5. Desarrolle e implemente procedimientos de copia de seguridad y recuperación de desastres.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Implemente y configure el componente Dispatcher en el entorno distribuido para que publique los temas en la nube de AWS.	1. Configure y organice en contenedores el componente Precisely Dispatcher. Para obtener instrucciones, consulte la documentación de Precisely. 2. Implemente la imagen de Docker de Dispatcher en el entorno en las instalaciones de Amazon EKS Anywhere. 3. Configure una conexión segura entre la nube de AWS y Dispatcher. 4. Desarrolle un sistema de supervisión para garantizar que el componente Dispatcher recopile los registros correctamente a lo largo del tiempo. 5. Implemente la instalación y las configuraciones en los entornos de prueba y producción.	DevOps ingeniero, Precisely Connect SME

Prepare el entorno de destino (AWS)

Tarea	Descripción	Habilidades requeridas
Aprovisione un clúster de Amazon EKS en la región de AWS designada.	1. Inicie sesión en su cuenta de AWS y configúrela para asegurarse de que cuenta con los permisos necesario	DevOps ingeniero, administrador de redes

Tarea	Descripción	Habilidades requeridas
	s para crear y administrar el clúster de Amazon EKS. 2. Cree una nube privada virtual (VPC) y subredes en la región de AWS seleccionada. Para obtener instrucciones, consulte la documentación de Amazon EKS. 3. Cree y configure los grupos de seguridad de red necesarios para permitir las comunicaciones entre el clúster de Amazon EKS y otros recursos de la VPC. Para obtener más informaci ón, consulte la documenta ción de Amazon EKS. 4. Cree el clúster de Amazon EKS y configúrelo con el tamaño de grupo de nodos y los tipos de instancias correctos. 5. Valide el clúster de Amazon EKS mediante la implement ación de una aplicación de muestra.	

Tarea	Descripción	Habilidades requeridas
Aprovisione un clúster de MSK y configure los temas de Kafka aplicables.	1. Configure su cuenta de AWS para asegurarse de que cuenta con los permisos necesarios para crear y administrar el clúster de MSK. 2. Cree y configure los grupos de seguridad de red necesarios para permitir las comunicaciones entre el clúster MSK y otros recursos de la VPC. Para obtener más información, consulte la documentación de Amazon VPC. 3. Cree el clúster de MSK y configúrelo para que incluya los temas de Kafka que utilizará la aplicación. Para obtener más información, consulte la documentación de Amazon MSK.	DevOps ingeniero, administrador de red

Tarea	Descripción	Habilidades requeridas
Configure el componente Apply Engine para que escuche los temas de Kafka replicados.	1. Configure y organice en contenedores el componente Precisely Apply Engine. 2. Implemente la imagen de Docker de Apply Engine en el clúster de Amazon EKS de su cuenta de AWS. 3. Configure Apply Engine para que escuche los temas de MSK. 4. Desarrolle y configure un script SQD en Apply Engine para gestionar el filtrado y la transformación. Para obtener más información, consulte la documentación de Precisely. 5. Implemente Apply Engine en entornos de prueba y producción.	Precisely Connect SME

Tarea	Descripción	Habilidades requeridas
Aprovisione instancias de base de datos en la nube de AWS.	1. Configure su cuenta de AWS para asegurarse de que cuenta con los permisos necesarios para crear y administrar los clústeres y tablas de bases de datos. Para obtener instrucciones, consulte la documentación de AWS del servicio de base de datos de AWS que desee utilizar. (Consulte los enlaces en la sección de recursos). 2. Cree una VPC y subredes en la región de AWS seleccionada. 3. Cree y configure los grupos de seguridad de red necesarios para permitir las comunicaciones entre las instancias de bases de datos y otros recursos de la VPC. 4. Cree las bases de datos y configúrelas para que incluyan las tablas que utilizará la aplicación. 5. Diseñe y valide los esquemas de las bases de datos.	Ingeniero de datos, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Configure e implemente conectores de bases de datos para que escuchen los temas publicados por Apply Engine.	1. Diseñe conectores de bases de datos para conectar los temas de Kafka con las bases de datos de AWS que creó en los pasos anteriores. 2. Desarrolle los conectores en función de la base de datos de destino. 3. Configure los conectores para que escuchen los temas de Kafka publicados por Apply Engine. 4. Implemente los conectores en el clúster de Amazon EKS.	Desarrollador de aplicaciones, arquitecto de la nube, ingeniero de datos

Configure la continuidad empresarial y la recuperación de desastres

Tarea	Descripción	Habilidades requeridas
Defina los objetivos de recuperación de desastres para sus aplicaciones empresariales.	1. Defina los objetivos de RPO y RTO para las canalizaciones de datos CDC en función de las necesidades de su empresa y del análisis de impacto. 2. Defina los procedimientos de comunicación y notificación para garantizar que todas las partes interesadas conozcan el plan de recuperación de desastres.	Arquitecto de la nube, ingeniero de datos, propietario de aplicaciones

Tarea	Descripción	Habilidades requeridas
	3. Determine el presupuesto y los recursos necesarios para implementar el plan de recuperación de desastres. 4. Documente los objetivos de recuperación de desastres , incluidos los objetivos de RPO y RTO.	

Tarea	Descripción	Habilidades requeridas
Diseñe estrategias de recuperación de desastres basadas en un RTO/RPO definido.	1. Determine las estrategias de recuperación de desastres más adecuadas para las canalizaciones de CDC en función de su jerarquía de importancia y sus requisitos de recuperación. 2. Defina la arquitectura y la topología de la recuperación de desastres. 3. Defina los procedimientos de conmutación por error y conmutación por recuperación de las canalizaciones de CDC para garantizar que puedan conmutar de forma rápida y sin problemas a la región de respaldo. 4. Documente las estrategias y los procedimientos de recuperación de desastres y asegúrese de que todas las partes interesadas comprendan claramente el diseño.	Arquitecto de la nube, ingeniero de datos

Tarea	Descripción	Habilidades requeridas
Aprovisione clústeres y configuraciones de recuperación de desastres.	1. Aprovisione una región de AWS secundaria para la recuperación de desastres. 2. En la región de AWS secundaria, cree un entorno que sea idéntico a la región de AWS principal. 3. Configure Apache Kafka MirrorMaker entre las regiones principal y secundaria. Para obtener más información, consulte la documentación de Amazon MSK. 4. Configure las aplicaciones en espera en la región secundaria. 5. Configure las replicaciones de bases de datos entre las regiones principal y secundaria.	DevOps ingeniero, administrador de redes, arquitecto de nube

Tarea	Descripción	Habilidades requeridas
Ponga a prueba la capacidad de recuperación de desastres de la canalización de CDC.	1. Defina el alcance y los objetivos de la prueba de recuperación de desastres de la canalización de CDC, incluidos los escenarios de prueba y el RTO que deben lograrse. 2. Identifique el entorno y la infraestructura de prueba para realizar la prueba de recuperación de desastres. 3. Prepare los conjuntos de datos y el script de la prueba para simular los escenarios de error. 4. Verifique la integridad y la coherencia de los datos para garantizar que no se pierdan datos.	Propietario de aplicaciones, ingeniero de datos, arquitecto de la nube

Recursos relacionados

Recursos de AWS

- Amazon DynamoDB
- Expresiones de condición con Amazon DynamoDB
- Amazon EKS
- Amazon EKS Anywhere
- Amazon ElasticCache
- Amazon Keyspaces
- Amazon MSK
- Amazon RDS y Amazon Aurora

- Amazon VPC

Recursos de Precisely Connect

- Descripción general de Precisely Connect
- Captura de datos de cambio con Precise Connect

Recursos Confluent

- Consumo de mensajes multiproceso con Apache Kafka Consumer

Programe trabajos para Amazon RDS para PostgreSQL y Aurora PostgreSQL mediante Lambda y Secrets Manager

Creado por Yaser Raja (AWS)

Entorno: PoC o piloto	Origen: bases de datos: relacionales	Destino: PostgreSQL en AWS
Tipo R: N/D	Carga de trabajo: código abierto	Tecnologías: bases de datos
Servicios de AWS: AWS Lambda; Amazon RDS; AWS Secrets Manager; Amazon Aurora		

Resumen

En el caso de las bases de datos en las instalaciones y las bases de datos alojadas en las instancias de Amazon Elastic Compute Cloud (Amazon EC2), los administradores de bases de datos suelen utilizar la utilidad cron para programar los trabajos.

Por ejemplo, un trabajo de extracción de datos o un trabajo de purga de datos se puede programar fácilmente mediante con cron. Para estos trabajos, las credenciales de la base de datos suelen tener una codificación rígida o estar almacenadas en un archivo de propiedades. Sin embargo, al migrar a Amazon Relational Database Service (Amazon RDS) o a Amazon Aurora PostgreSQL Compatible Edition, pierde la capacidad de iniciar sesión en la instancia host para programar trabajos cron.

Este patrón describe cómo usar AWS Lambda y AWS Secrets Manager para programar trabajos para Amazon RDS para PostgreSQL y bases de datos compatibles con Aurora PostgreSQL tras la migración.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.

- Una base de datos compatible con Amazon RDS para PostgreSQL o Aurora PostgreSQL

Limitaciones

- Un trabajo debe completarse en 15 minutos, que es el límite de tiempo de espera de la función de Lambda. Para conocer los límites, consulte la documentación de AWS Lambda.
- El código de trabajo debe escribirse en un lenguaje compatible con Lambda.

Arquitectura

Pila de tecnología de origen

Esta pila incluye tareas escritas en lenguajes como Bash, Python y Java. Las credenciales de la base de datos se almacenan en el archivo de propiedades y el trabajo se programa usando cron de Linux.

Pila de tecnología de destino

Esta pila tiene una función de Lambda que usa las credenciales almacenadas en Secrets Manager para conectarse a la base de datos y realizar la actividad. La función Lambda se inicia en el intervalo programado mediante Amazon CloudWatch Events.

Arquitectura de destino

Herramientas

- AWS Lambda es un servicio informático que permite ejecutar código sin aprovisionar ni administrar servidores. AWS Lambda ejecuta el código solo cuando es necesario y amplia la capacidad de manera automática, pasando de pocas solicitudes al día a miles por segundo. Solo se paga el tiempo de computación que se consume; no hay ningún cargo mientras el código no se ejecuta. Con AWS Lambda puede ejecutar código para prácticamente cualquier tipo de aplicación o servicio backend, sin ningún esfuerzo de administración. AWS Lambda ejecuta el código en una infraestructura informática de alta disponibilidad y realiza todas las tareas de administración de los recursos informáticos, incluidos el mantenimiento del servidor y del sistema operativo, el aprovisionamiento de capacidad y el escalado automático, así como la monitorización del código y las funciones de registro. Lo único que tiene que hacer es proporcionar el código en uno de los lenguajes que admite AWS Lambda.

- Amazon CloudWatch Events ofrece una transmisión casi en tiempo real de los eventos del sistema que describen los cambios en los recursos de AWS. Con reglas sencillas que puede configurar rápidamente, puede hacer coincidir los eventos y dirigirlos a una o más funciones o transmisiones de destino. CloudWatch Los eventos se dan cuenta de los cambios operativos a medida que se producen. Responde a estos cambios operativos y toma medidas correctoras según sea necesario, enviando mensajes para responder al entorno, activando funciones, realizando cambios y captando información de estado. También puedes usar CloudWatch Events para programar acciones automatizadas que se inicien automáticamente en determinados momentos mediante expresiones cron o rate.
- AWS Secrets Manager le ayuda a proteger los secretos para acceder a sus aplicaciones, servicios y recursos de TI. Puede rotar, administrar y recuperar fácilmente credenciales de bases de datos, claves de API y otros datos confidenciales durante todo su ciclo de vida. Los usuarios y las aplicaciones recuperan secretos mediante una llamada a las API de Secrets Manager, la cual elimina la necesidad de realizar codificación rígida sobre la información confidencial en texto sin formato. Secrets Manager ofrece una rotación de secretos con una integración incorporada para Amazon RDS, Amazon Redshift y Amazon DocumentDB. El servicio se puede extender a otros tipos de secretos, incluidas las claves de API y los tokens de OAuth. Secrets Manager le permite controlar el acceso a los datos confidenciales mediante permisos específicos y auditar la rotación de secretos de forma centralizada para los recursos de la nube de AWS, los servicios de terceros y aquellos en las instalaciones.

Epics

Almacenar credenciales de base de datos en Secrets Manager

Tarea	Descripción	Habilidades requeridas
Creación de un usuario de una base de datos para la función de Lambda.	Es una buena práctica utilizar usuarios de bases de datos independientes para las distintas partes de la aplicación. Si ya existe un usuario de base de datos independiente para sus trabajos cron, utilícelo. De lo contrario, cree un nuevo usuario de	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	base de datos. Para obtener más información, consulte Administración de usuarios y roles de PostgreSQL (entrada del blog de AWS).	
Almacene las credenciales de las bases de datos como un secreto en Secrets Manager.	Siga las instrucciones de Crear un secreto de base de datos (documentación de Secrets Manager).	DBA, DevOps

Autor del código para la función de Lambda

Tarea	Descripción	Habilidades requeridas
Elija un lenguaje de programación compatible con AWS Lambda.	Para obtener una lista de los lenguajes compatibl es, consulte los tiempos de ejecución de Lambda (documentación de Lambda).	Desarrollador
Escriba la lógica para obtener las credenciales de la base de datos de Secrets Manager.	Para ver un código de muestra, consulte Cómo proporcionar credenciales de base de datos de forma segura a las funciones de Lambda usando AWS Secrets Manager (entrada del blog de AWS).	Desarrollador
Escriba la lógica para realizar la actividad programada de la base de datos.	Migre el código existente para el trabajo de programación que está utilizando en las instalaciones a la función AWS de Lambda. Para	Desarrollador

Tarea	Descripción	Habilidades requeridas
	más información, consulte Implementación de funciones de Lambda (documentación de Lambda).	

Implemente el código y cree la función de Lambda

Tarea	Descripción	Habilidades requeridas
Cree el paquete de implementación de funciones de Lambda.	Este paquete contiene el código y sus dependencias. Para obtener más información, consulte Paquetes de implementación (documentación de Lambda).	Desarrollador
Crear la función de Lambda.	En la consola de AWS Lambda, elija Create function (Crear función), introduzca el nombre de una función, elija el entorno de tiempo de ejecución y, a continuación, elija Create function (Crear función).	DevOps
Cargue el paquete de implementación.	Elija la función de Lambda que creó para abrir su configuración. Puede escribir el código directamente en la sección de códigos o cargar el paquete de implementación. Para cargar su paquete, vaya a la sección Function code (Código de función), elija el Code entry type (tipo de	DevOps

Tarea	Descripción	Habilidades requeridas
	entrada de código) para cargar un archivo .zip y, a continuación, seleccione el paquete.	
Configure la función de Lambda según sus requisitos.	Por ejemplo, puede establecer el parámetro Tiempo de espera a la duración que espera que dure la función de Lambda. Para obtener más información, consulte Configuración de las opciones de las funciones (documentación de Lambda).	DevOps
Establezca los permisos para que el rol de la función de Lambda acceda a Secrets Manager.	Para obtener instrucciones, consulte Uso de secretos en las funciones AWS de Lambda (documentación de Secrets Manager).	DevOps
Probar la función de Lambda.	Inicie la función manualmente para asegurarse de que funciona según lo esperado.	DevOps

Programe la función Lambda mediante eventos CloudWatch

Tarea	Descripción	Habilidades requeridas
Cree una regla para ejecutar su función de Lambda de manera programada.	Programe la función Lambda mediante CloudWatch Eventos. Para obtener instrucciones, consulte Programar funciones de Lambda mediante CloudWatc	DevOps

Tarea	Descripción	Habilidades requeridas
	h eventos (tutorial sobre CloudWatch eventos).	

Recursos relacionados

- AWS Secrets Manager
- Introducción a Lambda
- Creación de una regla de CloudWatch eventos que se active en un evento
- Límites de AWS Lambda
- Consulte su base de datos de AWS desde su aplicación sin servidor (entrada del blog)

Proteja y optimice el acceso de los usuarios a una base de datos de federación DB2 en AWS mediante contextos de confianza

Creado por Sai Parthasaradhi (AWS)

Entorno: PoC o piloto	Tecnologías: bases de datos, seguridad, identidad, cumplimiento	Carga de trabajo: IBM
Servicios de AWS: Amazon EC2		

Resumen

Muchas empresas están migrando sus cargas de trabajo de la unidad central antigua a Amazon Web Services (AWS). Esta migración incluye el cambio de las bases de datos de IBM Db2 para z/OS a Db2 para Linux, Unix y Windows (LUW) en Amazon Elastic Compute Cloud (Amazon EC2). Durante una migración gradual en las instalaciones a AWS, es posible que los usuarios necesiten acceder a los datos de IBM Db2 z/OS y de Db2 LUW en Amazon EC2 hasta que todas las aplicaciones y bases de datos se hayan migrado por completo a Db2 LUW. En estos escenarios de acceso remoto a los datos, la autenticación de los usuarios puede resultar difícil porque las diferentes plataformas utilizan diferentes mecanismos de autenticación.

Este patrón explica cómo configurar un servidor de federación en Db2 para LUW con Db2 para z/OS como base de datos remota. El patrón utiliza un contexto de confianza para propagar la identidad de un usuario de Db2 LUW a Db2 z/OS sin volver a autenticarse en la base de datos remota. Para obtener más información sobre los contextos de confianza, consulte la sección Información adicional.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una instancia Db2 ejecutándose en una instancia Amazon EC2
- Una base de datos remota de Db2 para z/OS que se ejecuta en las instalaciones

- La red en las instalaciones conectada a AWS a través de AWS Site-to-Site VPN o AWS Direct Connect

Arquitectura

Arquitectura de destino

Herramientas

Servicios de AWS

- Amazon Elastic Compute Cloud (Amazon EC2) brinda capacidad de computación escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- AWS Site-to-Site VPN le ayuda a transferir el tráfico entre las instancias que lance en AWS y su propia red remota.

Otros servicios

- db2cli es el comando de la interfaz de la línea de comandos (CLI) interactiva de Db2.

Epics

Habilite la federación en la base de datos Db2 LUW que se ejecuta en AWS

Tarea	Descripción	Habilidades requeridas
Habilite la federación en la base de datos DB2 LUW.	Para habilitar la federación en DB2 LUW, ejecute el siguiente comando. `update dbm cfg using federated YES`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Reinicie la base de datos.	Para reiniciar la base de datos, ejecute el comando siguiente: `db2stop force;` `db2start;`	Administrador de base de datos

Cataloga la base de datos remota

Tarea	Descripción	Habilidades requeridas
Catalogue el subsistema remoto Db2 z/OS.	Para catalogar la base de datos remota de Db2 z/OS en Db2 LUW que se ejecuta en AWS, utilice el siguiente comando de ejemplo. `catalog TCPIP NODE tcpnode REMOTE mainframehost SERVER mainframeport`	Administrador de base de datos
Catalogue la base de datos remota.	Para catalogar la base de datos remota, utilice el siguiente comando de ejemplo. `catalog db dbnam1 as ndbnam1 at node tcpnode`	Administrador de base de datos

Cree la definición de servidor remoto

Tarea	Descripción	Habilidades requeridas
Recopile las credenciales de usuario para la base de datos remota de Db2 z/OS.	Antes de continuar con los siguientes pasos, recopile la siguiente información: • Nombre del subsistema Db2 z/OS: el nombre del Db2 z/OS catalogado en el LUW del paso anterior (por ejemplo, `ndbnam1`) • Versión Db2 z/OS: la versión del subsistema Db2 z/OS (por ejemplo, `12`) • ID de usuario de Db2 z/OS: el usuario con el privilegi o BIND, que se necesita para crear únicamente la definición de servidor (por ejemplo, `dbuser1`) • Contraseña de Db2 z/OS: la contraseña de `dbuser1` (por ejemplo, `dbpasswd`) • Usuario proxy de Db2 z/OS: el ID del usuario proxy, que se utilizará para establecer una conexión de confianza (por ejemplo, `zproxy`) • Contraseña de proxy de Db2 z/OS: la contraseña del usuario `zproxy` (por ejemplo, `zproxy`)	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree la capa DRDA.	Ejecute el siguiente comando para crear una capa DRDA. `CREATE WRAPPER DRDA;`	Administrador de base de datos
Cree la definición del servidor.	Para crear la definición del servidor, ejecute el siguiente comando de ejemplo. `CREATE SERVER ndbserver TYPE DB2/ZOS VERSION 12 WRAPPER DRDA AUTHORIZATION "dbuser1" PASSWORD "dbpasswd" OPTIONS ( DBNAME 'ndbnam1',FED_PROXY_USER 'ZPROXY' );` En esta definición, `FED_PROXY_USER` especifica el usuario proxy que se utilizará para establecer conexiones de confianza a la base de datos Db2 z/OS. El ID de usuario y la contraseña de autorización solo son necesarios para crear el objeto de servidor remoto en la base de datos de Db2 LUW. No se utilizarán más adelante durante el tiempo de ejecución.	Administrador de base de datos

Crear asignaciones de usuarios

Tarea	Descripción	Habilidades requeridas
Cree un asignación de usuarios para el usuario proxy.	Para crear un asignación de usuarios para el usuario proxy, ejecute el siguiente comando. `CREATE USER MAPPING FOR ZPROXY SERVER ndbserver OPTIONS (REMOTE_AUTHID 'ZPROXY', REMOTE_PASSWORD 'zproxy');`	Administrador de base de datos
Cree asignaciones de usuarios para cada usuario en Db2 LUW.	Cree asignaciones de usuarios para todos los usuarios de la base de datos de Db2 LUW en AWS que necesiten acceder a datos remotos a través del usuario proxy. Ejecute el siguiente comando para crear las asignaciones de usuario. `CREATE USER MAPPING FOR PERSON1 SERVER ndbserver OPTIONS (REMOTE_AUTHID 'USERZID', USE_TRUSTED_CONTEXT 'Y');` La expresión especifica que un usuario de Db2 LUW (`PERSON1`) puede establecer una conexión de confianza con la base de datos remota de Db2 z/OS (`USE_TRUSTED_CONTEXT 'Y'`). Una	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	vez establecida la conexión a través del usuario proxy, el usuario puede acceder a los datos mediante el ID de usuario de Db2 z/OS (`REMOTE_AUTHID 'USERZID'`).	

Cree el objeto de contexto de confianza

Tarea	Descripción	Habilidades requeridas
Cree el objeto de contexto de confianza.	Para crear el objeto de contexto de confianza en la base de datos remota de Db2 z/OS, utilice el siguiente comando de ejemplo. `CREATE TRUSTED CONTEXT CTX_LUW_ZOS BASED UPON CONNECTIO N USING SYSTEM AUTHID ZPROXY ATTRIBUTES ( ADDRESS '10.10.10.10' ) NO DEFAULT ROLE ENABLE WITH USE FOR PUBLIC WITHOUT AUTHENTIC ATION;` En esta definición, `CTX_LUW_ZOS` es un nombre arbitrario para el objeto de contexto de confianza. El	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	objeto contiene el ID del usuario proxy y la dirección IP del servidor desde el que debe originarse la conexión de confianza. En este ejemplo, el servidor de la base de datos Db2 LUW en AWS. También puede utilizar el nombre de dominio en lugar de la dirección IP. La cláusula `WITH USE FOR PUBLIC WITHOUT AUTHENTICATION` indica que se permite cambiar el ID de usuario en una conexión de confianza para cada ID de usuario. No es necesario proporcionar una contraseña.	

Recursos relacionados

- Instalación de control de acceso a los recursos de IBM (RACF)
- Federación IBM Db2 LUW
- Contextos de confianza

Información adicional

Contextos de confianza de Db2

Un contexto de confianza es un objeto de base de datos de Db2 que define una relación de confianza entre un servidor federado y un servidor de base de datos remoto. Para definir una relación de confianza, el contexto de confianza especifica los atributos de confianza. Existen tres tipos de atributos de confianza:

- El ID de autorización del sistema que realiza la solicitud de conexión inicial a la base de datos

- La dirección IP o el nombre de dominio desde los que se realiza la conexión
- La configuración de cifrado para las comunicaciones de datos entre el servidor de la base de datos y el cliente de la base de datos

Se establece una conexión de confianza cuando todos los atributos de una solicitud de conexión coinciden con los atributos especificados en cualquier objeto de contexto de confianza definido en el servidor. Existen dos tipos diferentes de conexiones de confianza: implícitas y explícitas. Una vez establecida una conexión de confianza implícita, el usuario hereda un rol que no está disponible para él fuera del ámbito de esa definición de conexión de confianza. Una vez establecida una conexión de confianza explícita, los usuarios pueden conectarse a la misma conexión física, con o sin autenticación. Además, a los usuarios de Db2 se les pueden asignar roles que especifiquen privilegios que solo se utilizarán dentro de la conexión de confianza. Este patrón utiliza una conexión de confianza explícita.

Contexto de confianza en este patrón

Una vez completado el patrón, la PERSON1 de Db2 LUW accede a los datos remotos de Db2 z/OS mediante un contexto de confianza federado. La conexión de PERSON1 se establece a través de un usuario proxy si la conexión se origina en la dirección IP o el nombre de dominio que se especifica en la definición del contexto de confianza. Una vez establecida la conexión, el ID de usuario de Db2 z/OS correspondiente a PERSON1 se cambia sin necesidad de volver a autenticarse, y el usuario puede acceder a los datos u objetos en función de los privilegios de Db2 configurados para ese usuario.

Ventajas de los contextos de confianza federados

- Este enfoque mantiene el principio del privilegio mínimo al eliminar el uso de un ID de usuario o de aplicación común, que requeriría un conjunto de todos los privilegios que requieren todos los usuarios.
- La identidad real del usuario que realiza la transacción tanto en la base de datos federada como en la remota siempre se conoce y se puede auditar.
- El rendimiento mejora porque la conexión física se reutiliza entre los usuarios sin necesidad de que el servidor federado vuelva a autenticarse.

Envíe notificaciones para una instancia de base de datos de Amazon RDS para SQL Server mediante un servidor SMTP en las instalaciones y el Correo de base de datos

Creado por Nishad Mankar (AWS)

Entorno: PoC o piloto	Tecnologías: bases de datos, gestión y gobernanza	Carga de trabajo: Microsoft
Servicios de AWS: Amazon RDS		

Resumen

Correo de base de datos (documentación de Microsoft) envía mensajes de correo electrónico, como notificaciones o alertas, desde una base de datos de Microsoft SQL Server mediante un servidor de Protocolo simple de transferencia de correo (SMTP). La documentación del Amazon Relational Database Service (Amazon RDS) para Microsoft SQL Server proporciona instrucciones para utilizar Amazon Simple Email Service (Amazon SES) como servidor SMTP para el Correo de base de datos. Para obtener más información, consulte Uso de Database Mail en Amazon RDS for SQL Server. Como configuración alternativa, este patrón explica cómo configurar la base de datos para enviar correos electrónicos desde una instancia de base de datos (DB) de Amazon RDS para SQL Server mediante un servidor SMTP en las instalaciones como servidor de correo.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una instancia de base de datos de Amazon RDS que ejecute una edición Standard o Enterprise de SQL Server
- La dirección IP o el nombre de host del servidor SMTP local.
- Una regla de grupo de seguridad entrante que permite las conexiones a la instancia de base de datos de Amazon RDS para SQL Server desde la dirección IP del servidor SMTP

- Una conexión, como una conexión AWS Direct Connect, entre la red en las instalaciones y la nube privada virtual (VPC) que contiene la instancia de base de datos de Amazon RDS

Limitaciones

- No se admiten las ediciones Express de SQL Server.
- Para obtener más información sobre las limitaciones, consulte Limitaciones en Uso del Correo de base de datos en Amazon RDS para SQL Server en la documentación de Amazon RDS.

Versiones de producto

- RDS admite las versiones Standard y Enterprise de SQL Server

Arquitectura

Pila de tecnología de destino

- Instancia de base de datos de Amazon RDS para SQL Server
- Amazon Route 53 (Amazon Route 53)
- Correo electrónico de base de datos
- Host local del servidor SMTP
- Microsoft SQL Server Management Studio (SSMS)

Arquitectura de destino

La siguiente imagen muestra la arquitectura de destino para este patrón. Cuando se produce un evento o una acción que inicia una notificación o alerta relativa a la instancia de base de datos, Amazon RDS para SQL Server utiliza el Correo de base de datos para enviar una notificación por correo electrónico. Correo de base de datos utiliza el servidor SMTP en las instalaciones para enviar el correo electrónico.

Herramientas

Servicios de AWS

- Puede utilizar Amazon Relational Database Service (Amazon RDS) para configurar, utilizar y escalar una base de datos relacional de SQL Server en la nube de AWS.
- Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad.

Otras herramientas

- Correo de base de datos es una herramienta que envía mensajes de correo electrónico, como notificaciones y alertas, desde el motor de base de datos de SQL Server a los usuarios.
- SQL Server Management Studio (SSMS) es una herramienta para administrar SQL Server, que incluye el acceso, la configuración y la administración de los componentes de SQL Server. En este patrón, utiliza SSMS para ejecutar los comandos SQL para configurar Correo de base de datos en una instancia de base de datos de Amazon RDS para SQL Server.

Epics

Habilite la conectividad de red con el servidor SMTP en las instalaciones

Tarea	Descripción	Habilidades requeridas
Elimine Multi-AZ de la instancia de base de datos de RDS.	Si utiliza una instancia de base de datos Multi-AZ, convierta la instancia Multi-AZ en una instancia Single-AZ. Cuando termine de configurar el Correo de base de datos, convertirá la instancia de base de datos de nuevo a una implementación Multi-AZ. La configuración de Database Mail funciona entonces tanto en el nodo primario como en el secundario. Para más información, consulte Eliminación de Multi-AZ de una instancia de base	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	de datos de Microsoft SQL Server.	
Cree una lista de direcciones IP o de punto de conexión de Amazon RDS en el servidor SMTP en las instalaciones.	El servidor SMTP está fuera de la red de AWS. En el servidor SMTP en las instalaciones, cree una lista de permisos que permita al servidor comunicarse con el punto de conexión saliente o la dirección IP de la instancia de Amazon RDS o la instancia de Amazon Elastic Compute Cloud (Amazon EC2) alojada en Amazon RDS. Este procedimiento varía de una organización a otra. Para obtener más información sobre el punto de conexión de la instancia de base de datos, consulte Búsqueda del punto de conexión y el número de puerto de la instancia de base de datos.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Elimine las restricciones del puerto 25.	En todas las instancias EC2, AWS restringe el tráfico en el puerto 25 por defecto. Para eliminar la restricción del puerto 25, haga lo siguiente: 1. Inicie sesión con su cuenta de AWS y, a continuación, abra el formulario de Solicitud para eliminar las limitaciones de envío de correo electrónico. 2. Introduzca su dirección de correo electrónico para que AWS Support pueda ponerse en contacto con usted para informarle sobre las actualizaciones de su solicitud. 3. Proporcione la información requerida en el campo de Descripción del caso de uso. 4. Elija Enviar. Nota: • Si tiene instancias en más de una región de AWS, envíe una solicitud por separado para cada región. • Su solicitud de transacción puede tardar hasta 48 horas en procesarse.	AWS general

Tarea	Descripción	Habilidades requeridas
Añada una regla de Route 53 para resolver las consultas de DNS para el servidor SMTP.	Utilice Route 53 para resolver las consultas de DNS entre los recursos de AWS y el servidor SMTP en las instalaciones. Debe crear una regla que reenvíe las consultas de DNS al dominio del servidor SMTP, por ejemplo `example.com` . Para obtener instrucciones, consulte Creación de reglas de reenvío en la documentación de Route 53.	Administrador de red

Configuración de Correo de base de datos en la instancia de base de datos de Amazon RDS para SQL Server

Tarea	Descripción	Habilidades requeridas
Habilitación de Database Mail.	Cree un grupo de parámetros para el Correo de base de datos, defina el parámetro `database mail xps` en `1`, a continuación, asocie el grupo de parámetros del Correo de base de datos a la instancia de base de datos de RDS de destino. Para obtener instrucciones, consulte la Habilitación de Database Mail en la documentación de Amazon RDS. No continúe con la sección de Configuración del correo de base de datos de estas instrucciones. La	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	configuración del servidor SMTP en las instalaciones es diferente a la de Amazon SES.	
Conéctese a la instancia de base de datos.	Desde un host bastión, utilice Microsoft SQL Server Management Studio (SSMS) para conectarse a la instancia de base de datos de Amazon RDS para SQL Server. Para obtener instrucciones, consulte Conexión de una instancia de base de datos que ejecuta el motor de base de datos de Microsoft SQL Server. Si encuentra algún error, consulte las referencias para la solución de problemas de conexión en la sección de Recursos relacionados.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Crear el perfil	En SSMS, inserte la siguiente instrucción SQL para crear el perfil del Correo de base de datos. Reemplace los siguientes valores: • Para `profile_name` , escriba un nombre para el nuevo perfil. • Para `description` , escriba una breve descripci ón del nuevo perfil. Para obtener más información acerca de este procedimiento almacenado y sus argumento s, consulte sysmail_add_profil e_sp en la documentación de Microsoft. `EXECUTE msdb.dbo. sysmail_add_profil e_sp @profile_name = 'SQL Alerts profile', @description = 'Profile used for sending outgoing notifications using OM SMTP Server.';`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Añada las entidades principal es al perfil.	Introduzca la siguiente instrucción SQL para añadir directores públicos o privados al perfil de correo de la base de datos. Una entidad principal es una entidad que puede solicitar recursos de SQL Server. Reemplace los siguientes valores: • Para `profile_name` , inserte el nombre del perfil que creó anteriormente. • Para `principal_name` , inserte el nombre del usuario o rol de base de datos. Este valor debe corresponder a un usuario de autenticación de SQL Server, un usuario de autenticación de Windows o un grupo de autenticación de Windows. Para obtener más información acerca de este procedimiento almacenado y sus argumento s, consulte sysmail_add_princi palprofile_sp en la documenta ción de Microsoft. `EXECUTE msdb.dbo. sysmail_add_princi palprofile_sp`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`@profile_name = 'SQL Alerts profile', @principal_name = 'public', @is_default = 1 ;`	

Tarea	Descripción	Habilidades requeridas
Crear la cuenta	Inserte la siguiente instrucción SQL para crear el perfil de la cuenta de Database Mail. Reemplace los siguientes valores: • For `account_name` , escriba un nombre para la nueva cuenta. • Para `description` , escriba una breve descripción de la nueva cuenta. • Para `email_address` , introduzca la dirección de correo electrónico desde la que desea enviar los mensajes de correo de la base de datos. • Para `display_address` , especifique un nombre para mostrar y usarlo en los mensajes salientes de esta cuenta, por ejemplo `SQL Server Automated Notification` . También puede utilizar el valor que ha introducido para `email_address` . • Para `mailserver_name` , introduzca el nombre o la dirección IP del servidor de correo SMTP. • Para `port`, deje el valor de `25`.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	• Para `enable_ssl` , deje el valor en `1` o introduzca `0` si no desea que el Correo de base de datos cifre las comunicaciones mediante SSL. • Para `username`, introduzca el nombre de usuario de registro en el servidor de correo SMTP. Si el servidor no requiere autenticación, inserte `NULL`. • Para `password`, introduzca la contraseña para acceder al servidor de correo SMTP. Si el servidor no requiere autenticación, inserte `NULL`. Para obtener más información acerca de este procedimiento almacenado y sus argumentos, consulte sysmail_add_account_sp en la documentación de Microsoft. `EXECUTE msdb.dbo.sysmail_add_account_sp` `@account_name = 'SQL Alerts account',` `@description = 'Database Mail account for sending outgoing notifications.',` `@email_address = 'xyz@example.com',`	

Tarea	Descripción	Habilidades requeridas
	`` @display_name = 'xyz@example.com', @mailserver_name = 'test_smtp.example .com', @port = 25, @enable_ssl = 1, @username = 'SMTP-use rname', @password = 'SMTP-pas sword'; ```	

Tarea	Descripción	Habilidades requeridas
Agregue la cuenta al perfil	Inserte la siguiente instrucción SQL para agregar la cuenta de Database Mail al perfil de Database Mail. Reemplace los siguientes valores: • Para `profile_name` , inserte el nombre del perfil que creó anteriormente. • Para `account_name` , inserte el nombre de la cuenta que creó anteriorm ente. Para obtener más información acerca de este procedimiento almacenado y sus argumento s, consulte sysmail_add_profil eaccount_sp en la documenta ción de Microsoft. `EXECUTE msdb.dbo. sysmail_add_profil eaccount_sp @profile_name = 'SQL Alerts profile', @account_name = 'SQL Alerts account', @sequence_number = 1;`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
(Opcional) Añada Multi-AZ a la instancia de base de datos de RDS.	Si desea añadir Multi-AZ con Replicación de bases de datos (DBM) o Grupos de disponibilidad siempre activados (AG), consulte las instrucciones de Añadir Multi-AZ a una instancia de base de datos de Microsoft SQL Server.	Administrador de base de datos

Recursos relacionados

- Uso de Database Mail en Amazon RDS para SQL Server (documentación de Amazon RDS)
- Trabajar con archivos adjuntos (documentación de Amazon RDS)
- Solución de problemas de conexión a la instancia de base de datos de SQL Server (documentación de Amazon RDS)
- No se puede conectar a la instancia de base de datos de Amazon RDS (documentación de Amazon RDS)

Configurar la recuperación de desastres para SAP en IBM Db2 en AWS

Entorno: producción	Tecnologías: Bases de datos; Operaciones	Carga de trabajo: SAP
Servicios de AWS: Amazon EC2; AWS Elastic Disaster Recovery		

Resumen

Este patrón describe los pasos para configurar un sistema de recuperación de desastres (DR) para cargas de trabajo de SAP con IBM Db2 como plataforma de base de datos ejecutada en la nube de Amazon Web Services (AWS). El objetivo es proporcionar una solución de bajo costo para garantizar la continuidad empresarial en caso de interrupción.

El patrón emplea el enfoque de prueba piloto. Al implementar una prueba piloto de DR en AWS, puede reducir el tiempo de inactividad y mantener la continuidad empresarial. Este enfoque piloto se centra en configurar un entorno de DR mínimo en AWS, con un sistema SAP y una base de datos Db2 en espera sincronizada con el entorno de producción.

Esta solución es escalable. Puede ampliarla a un entorno de recuperación de desastres a gran escala si lo necesita.

Requisitos previos y limitaciones

Requisitos previos

- Una instancia de SAP que se ejecuta en una instancia de Amazon Elastic Compute Cloud (Amazon EC2)
- Base de datos Db2 de IBM
- Un sistema operativo compatible con la matriz de disponibilidad de producto (PAM) de SAP
- Diferentes nombres de host de bases de datos físicas para los hosts de bases de datos de producción y espera

- Un bucket de Amazon Simple Storage Service (Amazon S3) en cada región de AWS con la replicación entre regiones (CRR) habilitada

Versiones de producto

- Base de datos IBM Db2, versión 11.5.7 o posterior

Arquitectura

Pila de tecnología de destino

- Amazon EC2
- Amazon Simple Storage Service (Amazon S3)
- Nube privada virtual de Amazon (VPC peering)
- Amazon Route 53
- Recuperación de desastres de alta disponibilidad (HADR) en IBM Db2

Arquitectura de destino

Esta arquitectura implementa una solución de DR para cargas de trabajo de SAP con Db2 como plataforma de base de datos. La base de datos de producción se implementa en la región 1 de AWS, y la base de datos de espera se implementa en una segunda región. La base de datos de espera se denomina sistema DR. La base de datos Db2 admite varias bases de datos de espera (hasta tres). Emplea el HADR de Db2 para configurar la base de datos de recuperación de desastres y automatizar el envío de registros entre las bases de datos de producción y espera.

Si la disponibilidad de la región 1 se interrumpe a causa de un desastre, la base de datos en espera de la región de DR asume la función de base de datos de producción. Los servidores de aplicaciones de SAP se pueden crear con antelación mediante AWS Elastic Disaster Recovery o con una imagen de máquina de Amazon (AMI) para satisfacer los requisitos del objetivo de tiempo de recuperación (RTO). Este patrón emplea un AMI.

El HADR de Db2 implementa una configuración de producción en espera en la que producción actúa como servidor principal al que se conectan todos los usuarios. Todas las transacciones se escriben en archivos de registro que se transfieren al servidor en espera mediante TCP/IP. El servidor en espera actualiza su base de datos local enviando los registros transferidos, lo que ayuda a garantizar la sincronización con el servidor de producción.

El emparejamiento de VPC permite que las instancias de la región de producción y la región de DR puedan comunicarse entre sí. Amazon Route 53 dirige a los usuarios finales a las aplicaciones de Internet.

1. Cree una AMI del servidor de aplicaciones en la región 1 y copie la AMI en la región 2. Use la AMI para lanzar servidores en la Región 2 en caso de desastre.
2. Configure la replicación HADR de Db2 entre la base de datos de producción (en la región 1) y la base de datos en espera (en la región 2).
3. En caso de desastre, cambie el tipo de instancia EC2 para que coincida con la instancia de producción.
4. En la Región 1, `LOGARCHMETH1` se establece en `db2remote: S3 path`.
5. En la Región 2, `LOGARCHMETH1` se establece en `db2remote: S3 path`.
6. La replicación entre regiones se realiza entre los buckets de S3.

Herramientas

Servicios de AWS

- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esta red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS. Este patrón emplea interconexión de VPC.

Prácticas recomendadas

- La red desempeña un papel crucial a la hora de decidir el modo de replicación HADR. Para la recuperación de desastres en todas las regiones de AWS, le recomendamos que use el modo Db2 HADR ASYNC o SUPERASYNC.
- Para obtener más información sobre los modos de replicación de Db2 HADR, consulte la documentación de IBM.
- Puede usar la consola de administración de AWS o la interfaz de la línea de comandos de AWS (AWS CLI) para crear una nueva AMI de su sistema SAP existente. A continuación, puede usar la AMI para recuperar su sistema SAP existente o crear un clon.
- La Automatización de AWS Systems Manager puede ayudar con las tareas comunes de mantenimiento e implementación de instancias EC2 y otros recursos de AWS.
- AWS proporciona varios servicios nativos para supervisar y gestionar la infraestructura y las aplicaciones en AWS. CloudTrail Se pueden usar servicios como Amazon CloudWatch y AWS para monitorear la infraestructura subyacente y las operaciones de API, respectivamente. Para obtener más información, consulte SAP en AWS: IBM Db2 HADR con Pacemaker.

Epics

Prepare el entorno

Tarea	Descripción	Habilidades requeridas
Compruebe el sistema y los registros.	1. Confirme que el SAP de producción en el sistema Db2 esté configurado. 2. Confirme que la copia de seguridad de registros esté habilitada y configurada para guardar los registros en el bucket de S3. Puede comprobarlo mediante el parámetro `LOGARCHMETH1` de Db2.	Administrador de AWS, administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas
	3. Cree una AMI del servidor de aplicaciones adicional.	

Configure los servidores y la replicación

Tarea	Descripción	Habilidades requeridas
Cree los servidores de SAP y de bases de datos.	1. Para implementar la infraestructura en la región de DR, utilice un CloudFormation script de AWS o una AMI de la instancia de producción. En este enfoque de prueba piloto, puede usar una instancia EC2 más pequeña de la misma familia que la instancia de producción. Por ejemplo, si su tipo de instancia de producción es `r6i.12xlarge` , puede usar el tipo de instancia `r6i.xlarge` para la compilación de DR. De cualquier modo, asegúrese de asignar la misma capacidad de almacenam iento a la instancia de DR para restaurar la copia de seguridad de la base de datos de producción. 2. Cree puntos de montaje para `/sapmnt/<SID>/` en Amazon Elastic File	Administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas
	System (Amazon EFS) y asegúrese de que está configurado para replicarse desde el sistema principal. 3. Realice una copia de seguridad completa de la base de datos (online u offline) del sistema de producción. Usará esta copia de seguridad para crear la base de datos de DR. 4. En el sistema de DR, use el método de copia del sistema SAP Software Provisioning Manager (SWPM) indicado en Uso de copia del sistema con copia de seguridad/restauración para HA/DR para crear el sistema SAP de DR. 5. Cuando SWPM lo solicite, restaure la base de datos de DR con la copia de seguridad que recuperó de producción. La base de datos de DR estará en estado pendiente de avance de transacciones. El estado pendiente de avance de transacciones se establece de forma predeterminada una vez restaurada la	

Tarea	Descripción	Habilidades requeridas
	copia de seguridad completa. El estado pendiente de avance de transacciones indica que la base de datos está en proceso de restauración, y que es posible que se necesite aplicar algunos cambios. Para obtener más información, consulte la documentación de IBM.	

Tarea	Descripción	Habilidades requeridas
Compruebe la configuración.	1. Para configurar el archivado de registros para HADR, tanto las bases de datos de producción como las de DR deben poder recuperar los registros automáticamente de todas las ubicaciones de archivo de registros. Compruebe que el parámetro `LOGARCHMETH1` de la base de datos de DR esté establecido en la misma ubicación que en la base de datos de producción. Si no se puede acceder a la misma ubicación debido a las limitaciones regionales, asegúrese de que el sistema de DR pueda recuperar automáticamente los registros del sistema principal. 2. Para habilitar los puertos TCP/IP para permitir la replicación de bases de datos, modifique `/etc/services` en producción y DR agregando las dos siguientes entradas. En el código, `<SID>` hace referencia a la ID de sistema (SID) de la base	Administrador de AWS, administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas
	de datos Db2 (por ejemplo, PR1). `<SID>_HADR_1 55001/tcp # DB2 HADR Port1` `<SID>_HADR_2 55002/tcp # DB2 HADR Port2` Confirme que ambos puertos permiten el tráfico entrante y saliente entre las bases principal y en espera. 3. Compruebe `/etc/hosts` en los hosts de producción y DR para asegurarse de que los nombres de host de los hosts de producción y espera apuntan a las direcciones IP correctas.	

Tarea	Descripción	Habilidades requeridas
Configure la replicación desde la base de datos de producción a la base de datos de DR (mediante el modo ASYNC).	1. En la base de datos de producción, ejecute los siguientes comandos para actualizar los parámetros. `db2 UPDATE DB CFG FOR <SID> USING HADR_LOCAL_HOST HOST1` `db2 UPDATE DB CFG FOR <SID> USING HADR_LOCAL_SVC <SID>_HADR_1` `db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_HOST HOST2` `db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_SVC <SID>_HADR_2` `db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_INST db2<sid>` `db2 UPDATE DB CFG FOR <SID> USING HADR_TIMEOUT 120` `db2 UPDATE DB CFG FOR <SID> USING HADR_SYNCMODE ASYNC` `db2 UPDATE DB CFG FOR <SID> USING HADR_SPOOL_LIMIT 1000` `db2 UPDATE DB CFG FOR <SID> USING HADR_PEER_WINDOW 240` `db2 UPDATE DB CFG FOR <SID> USING indexrec RESTART logindexbuild ON` 2. En la base de datos DR, ejecute los siguientes	Administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas
	comandos para actualizar los parámetros. `db2 UPDATE DB CFG FOR <SID> USING HADR_LOCAL_HOST HOST2` `db2 UPDATE DB CFG FOR <SID> USING HADR_LOCAL_SVC <SID>_HADR_2` `db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_HOST HOST1` `db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_SVC <SID>_HADR_1` `db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_INST db2<sid>` `db2 UPDATE DB CFG FOR <SID> USING HADR_TIMEOUT 120` `db2 UPDATE DB CFG FOR <SID> USING HADR_SYNCMODE ASYNC` `db2 UPDATE DB CFG FOR <SID> USING HADR_SPOOL_LIMIT 1000` `db2 UPDATE DB CFG FOR <SID> USING HADR_PEER_WINDOW 240` `db2 UPDATE DB CFG FOR <SID> USING indexrec RESTART logindexbuild ON` Estos parámetros son necesarios para proporcionar información de HADR a ambas bases de datos. En la base de datos Db2,	

Tarea	Descripción	Habilidades requeridas
	HADR se activa en función de los valores de cada uno de los parámetros estableci dos anteriormente. Para más información sobre estos parámetros, consulte la documentación de IBM. 3. Inicie primero HADR en la base de datos de espera recién creada ejecutando el siguiente comando. `db2 deactivate db <SID>` `db2 start hadr on db <SID> as standby` 4. Inicie HADR en la base de datos de producción ejecutando el siguiente comando. `db2 deactivate db <SID>` `db2 start hadr on db <SID> as primary` 5. Compruebe si las bases de datos Db2 en producción y en espera están sincroniz adas, y si el envío de registros está en curso. Para supervisar el estado de la replicación de HADR, ejecute el comando db2pd.	

Tarea	Descripción	Habilidades requeridas
	`db2pd -d <SID> -hadr` Para más información sobre la monitorización de HADR, consulte la documentación de IBM.	

Pruebe las tareas de conmutación por error de DR

Tarea	Descripción	Habilidades requeridas
Planifique el tiempo de inactividad empresarial de producción para la prueba de DR.	Asegúrese de planificar el tiempo de inactividad empresarial necesario en el entorno de producción para probar el escenario de conmutación por error de DR.	Administrador de SAP Basis
Crear un usuario de prueba.	Cree un usuario de prueba (o cualquier cambio de prueba) que pueda validarse en el host de DR para confirmar la replicación del registro tras la conmutación por error de DR.	Administrador de SAP Basis
En la consola, detenga las instancias de EC2 de producción.	En este paso se inicia un cierre imprevisto para simular un escenario de desastre.	Administrador de sistemas de AWS
Escale verticalmente la instancia de EC2 de DR para adecuarla a los requisitos.	En la consola de EC2, cambie el tipo de instancia en la región de DR. 1. Detenga la instancia: si la instancia se está ejecutand	Administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas
	o, debe detenerla para poder cambiar el tipo de instancia. En la consola de EC2, seleccione la instancia y elija Detener. 2. Modifique el tipo de instancia: en la consola de EC2, seleccione la instancia y elija Acciones, Configuración de instancia y Cambiar tipo de instancia. Seleccione el tipo de instancia que coincida con la instancia principal y elija Aplicar. 3. Iniciar la instancia: una vez finalizado el cambio de tipo de instancia, inicie la instancia desde la consola de EC2 seleccionando la instancia y pulsando Iniciar. 4. Para iniciar la base de datos Db2, utilice el comando siguiente. `db2start` `db2 start HADR on db <SID> as standby`	

Tarea	Descripción	Habilidades requeridas
Inicie la toma de control.	Desde el sistema de DR (`host2`), inicie el proceso de toma de control y active la base de datos de recuperación de desastres como principal. `db2 takeover hadr on database <SID> by force` Si lo desea, puede configurar los siguientes parámetros para ajustar automáticamente la asignación de memoria de la base de datos en función del tipo de instancia. El valor `INSTANCE_MEMORY` se puede decidir en función de la parte dedicada de la memoria que se va a asignar a la base de datos Db2. `db2 update db cfg for <SID> using INSTANCE_MEMORY <FIXED VALUE> IMMEDIATE;` `db2 get db cfg for <SID> | grep -i DATABASE_MEMORY AUTOMATIC IMMEDIATE;` `db2 update db cfg for <SID> using self_tuning_mem ON IMMEDIATE;` Verifique el cambio usando los siguientes comandos.	Administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas
	`db2 get db cfg for <SID> | grep -i MEMORY` `db2 get db cfg for <SID> | grep -i self_tuning_mem`	
Inicie el servidor de aplicaciones para SAP en la región de DR.	Con la AMI que creó en el sistema de producción, lance un nuevo servidor de aplicaciones adicional en la región de DR.	Administrador de SAP Basis
Realice la validación antes de iniciar la aplicación SAP.	1. Valide las entradas `/etc/hosts` y `/etc/fstab`. 2. Monte `/sapmnt/<SID>/` en el sistema de DR. 3. Valide que el sistema de archivos de DR `/sapmnt/<SID>/` esté sincronizado con el `/sapmnt/<SID>/` de producción. 4. Inicie sesión con el usuario `<sid>adm`, ejecute `R3trans -d` y verifique el resultado del archivo `trans.log`. El archivo `trans.log` se genera en la misma ubicación en la que se ejecutó el comando `R3trans -d`.	Administrador de AWS, administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas
Inicie la aplicación SAP en el sistema de DR.	Inicie la aplicación SAP en el sistema de DR utilizando el usuario `<sid>adm`. Use el siguiente código, en el que XX representa el número de instancia de su servidor ABAP SAP Central Services (ASCS) de SAP, y YY representa el número de instancia de su servidor de aplicación SAP. `sapconrol -nr XX -function StartService <SID>` `sapconrol -nr XX -function StartSystem` `sapconrol -nr YY -function StartService <SID>` `sapconrol -nr YY -function StartSystem`	Administrador de SAP Basis
Realice la validación de SAP.	Esto se lleva a cabo como una prueba de DR para proporcionar pruebas o comprobar que la replicación de los datos en la región de DR se realiza correctamente.	Ingeniero de pruebas

Lleve a cabo tareas de conmutación por recuperación en DR

Tarea	Descripción	Habilidades requeridas
Inicie los servidores de bases de datos y SAP de producció n.	En la consola, inicie las instancias de EC2 que alojan SAP y la base de datos en el sistema de producción.	Administrador de SAP Basis
Iniciar la base de datos de producción y configurar HADR.	Inicie sesión en el sistema de producción (`host1`) y compruebe que la base de datos está en modo de recuperación ejecutando el siguiente comando. `db2start` `db2 start HADR on db P3V as standby` `db2 connect to <SID>` Compruebe que el estado de HADR sea `connected` . El estado de la replicación debe ser `peer`. `db2pd -d <SID> -hadr` Si la base de datos no es incoherente y no se encuentra en estado `connected` y `peer`, es posible que sea necesario realizar una copia de seguridad y una restaurac ión para que la base de datos (en `host1`) se sincronice con la base de datos actualmen	Administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas
	te activa (`host2` en la región de DR). En ese caso, restaure la copia de seguridad de la base de datos de la región de DR `host2` a la base de datos de la región de producción `host1`.	

Tarea	Descripción	Habilidades requeridas
Conmute por recuperación la base de datos a la región de producción.	En un business-as-usual escenario normal, este paso se realiza en un tiempo de inactividad programado. Las aplicaciones que se ejecutan en el sistema de DR se detienen, y la base de datos se conmuta por recuperac ión a la región de producción (región 1) para reanudar las operaciones desde la región de producción. 1. Inicie sesión en el servidor de aplicaciones SAP de la región de DR y detenga la aplicación de SAP. 2. Desmonte `/sapmnt/<SID>` del sistema de DR y asegúrese de que los cambios se replican de forma inversa al sistema de producción `/sapmnt/<SID>` . 3. Inicie sesión en el servidor de base de datos (`host1`) de la región de producción y tome el control. `db2 takeover hadr on database <SID>` 4. Compruebe el estado de HADR: `HADR_ROLE` debe	Administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas
	ser PRIMARY en host1 y StandBy en host2. `db2pd -d <SID> -hadr`	
Realice la validación antes de iniciar la aplicación SAP.	1. Valide las entradas /etc/hosts y /etc/fstab . 2. Monte /sapmnt/<SID>/ en el sistema de producción. 3. Asegúrese de que esté sincronizado con el sistema de DR /sapmnt/<SID>/ . 4. Inicie sesión con el usuario <sid>adm, ejecute R3trans -d y verifique el resultado del archivo trans.log . El archivo trans.log se genera en la misma ubicación en la que se ejecutó el comando R3trans -d.	Administrador de AWS, administrador de SAP Basis

Tarea	Descripción	Habilidades requeridas
Inicie la aplicación de SAP.	1. Inicie la aplicación SAP en el sistema de producción con el usuario `<sid>adm`. Use el siguiente código, en el que XX representa el número de instancia de su servidor SAP ASCS, y YY representa el número de instancia de su servidor de aplicación SAP. `sapconrol -nr XX -function StartService <SID>` `sapconrol -nr XX -function StartSystem` `sapconrol -nr YY -function StartService <SID>` `sapconrol -nr YY -function StartSystem` 2. Para confirmar que los servidores de aplicaciones están disponibles, inicie sesión en SAP y realice las comprobaciones ejecutando las transacciones SICK y SM51.	Administrador de SAP Basis

Resolución de problemas

Problema	Solución
Archivos de registro de clave y comandos para solucionar problemas relacionados con HADR	• `db2 get db cfg | grep -i hadr`

Problema	Solución
	• `db2pd -d sid -hadr` • `Db2diag.log` (Por lo general, este archivo se encuentra dentro del directorio `db2dump`, y la ruta de `db2dump` está definida por el parámetro `DIAGPATH`).
Nota de SAP para la resolución de problemas de HADR en Db2 UDB	Consulte la nota de SAP 1154013 - DB6: problemas de base de datos en entorno HADR. (Necesitará las credenciales del portal SAP para acceder a esta nota).

Recursos relacionados

- Enfoques de recuperación de desastres para bases de datos Db2 en AWS (publicación del blog)
- SAP en AWS: IBM Db2 HADR con Pacemaker
- Procedimiento paso a paso para configurar la replicación de HADR entre bases de datos DB2
- Wiki de HADR Db2

Información adicional

Con este patrón puede configurar un sistema de recuperación de desastres para un sistema SAP que se ejecute en una base de datos Db2. En una situación de desastre, la empresa debería poder mantener sus requisitos de Objetivo de tiempo de recuperación (RTO) y Objetivo de punto de recuperación (RPO):

- El RTO es la máxima demora aceptable entre la interrupción del servicio y el restablecimiento del servicio. Este valor determina el período de tiempo que se considera aceptable cuando el servicio no está disponible.
- El RPO es la cantidad máxima de tiempo aceptable desde el último punto de recuperación de datos. Esto determina qué se considera una pérdida de datos aceptable entre el último punto de recuperación y la interrupción del servicio.

Para consultar las preguntas frecuentes relacionadas con HADR, consulte la Nota de SAP #1612105 - DB6: preguntas frecuentes sobre recuperación de desastres con alta disponibilidad (HADR) de Db2. (Necesitará las credenciales del portal SAP para acceder a esta nota).

Configure una arquitectura HA/DR para Oracle E-Business Suite en Amazon RDS Custom con una base de datos en espera activa

Creado por Simon Cunningham (AWS) y Nitin Saxena

Entorno: producción	Tecnologías: bases de datos; infraestructura	Carga de trabajo: Oracle
Servicios de AWS: Amazon RDS		

Resumen

Este patrón describe cómo puede diseñar su solución Oracle E-Business en Amazon Relational Database Service (Amazon RDS) Custom para lograr una alta disponibilidad (HA) y recuperación de desastres (DR) configurando una base de datos de réplicas de lectura de Amazon RDS Custom en otra zona de disponibilidad de Amazon Web Services (AWS) y convirtiéndola en una base de datos en espera activa. La creación de la réplica de lectura de Amazon RDS Custom está totalmente automatizada mediante la consola de administración de AWS.

Este patrón no describe los pasos para añadir niveles de aplicaciones y sistemas de archivos compartidos adicionales, que también pueden formar parte de una arquitectura de HA/DR. Para obtener más información sobre estos temas, consulte las siguientes notas de soporte de Oracle: 1375769.1, 1375670.1 y 1383621.1 (sección 5, Opciones de clonación avanzadas). (El acceso requiere una cuenta de Oracle Support).

Para migrar el sistema E-Business Suite a una arquitectura de un solo nivel y zona de disponibilidad única en Amazon Web Services (AWS), consulte el patrón Migrar Oracle E-Business Suite a Amazon RDS Custom.

Oracle E-Business Suite es una solución de planificación de recursos empresariales (ERP) que automatiza procesos de toda la empresa, como finanzas, recursos humanos, cadena de suministro y fabricación. Ofrece una arquitectura de tres niveles: cliente, aplicación y base de datos. Anteriormente, tenía que ejecutar la base de datos de Oracle E-Business Suite en una instancia de Amazon Elastic Compute Cloud (Amazon EC2) autogestionada, pero ahora puede beneficiarse de Amazon RDS Custom.

Requisitos previos y limitaciones

Requisitos previos

- Una instalación existente de E-Business Suite en Amazon RDS Custom; consulte el patrón Migrar Oracle E-Business Suite a Amazon RDS Custom
- Si quiere cambiar la réplica de lectura a una de solo lectura y utilizarla para transferir los informes a los que están en espera, adquiera una licencia de base de datos Oracle Active Data Guard (consulte la lista de precios comerciales de Oracle Technology)

Limitaciones

- Limitaciones y configuraciones no compatibles con las bases de datos Oracle en Amazon RDS Custom
- Limitaciones asociadas a las réplicas de lectura de Amazon RDS Custom para Oracle

Versiones de producto

Para ver las versiones de Oracle Database y clases de instancia compatibles con Amazon RDS Custom, consulte Requisitos y limitaciones de Amazon RDS Custom para Oracle.

Arquitectura

El siguiente diagrama ilustra una arquitectura representativa de E-Business Suite en AWS que incluye varias zonas de disponibilidad y niveles de aplicaciones en una configuración activa/pasiva. La base de datos usa una instancia de base de datos de Amazon RDS Custom y una réplica de lectura de Amazon RDS Custom. La réplica de lectura utiliza Active Data Guard para replicarse en otra zona de disponibilidad. También puede usar la réplica de lectura para descargar el tráfico de lectura en la base de datos principal y para generar informes.

Para obtener más información, consulte Trabajar con réplicas de lectura para Amazon RDS Custom para Oracle en la documentación de Amazon RDS.

La réplica de lectura de Amazon RDS Custom se crea de forma predeterminada cuando está montada. Sin embargo, si desea transferir algunas de sus cargas de trabajo de solo lectura a la base de datos en espera para reducir la carga de la base de datos principal, puede cambiar manualmente

el modo de las réplicas montadas a las de solo lectura siguiendo los pasos de la sección Epics. Un caso de uso típico sería ejecutar los informes desde la base de datos en espera. Para cambiar a una base de datos de solo lectura se requiere una licencia de base de datos en espera activa.

Al crear una réplica de lectura en AWS, el sistema utiliza el agente Oracle Data Guard de forma clandestina. Esta configuración se genera automáticamente y se configura en el modo de máximo rendimiento de la siguiente manera:

```
DGMGRL> show configuration
Configuration - rds_dg
  Protection Mode: MaxPerformance
  Members:
  vis_a - Primary database
    vis_b - Physical standby database
Fast-Start Failover: DISABLED
Configuration Status:
SUCCESS   (status updated 58 seconds ago)
```

Herramientas

Servicios de AWS

- Amazon RDS Custom para Oracle es un servicio de base de datos administrado para aplicaciones heredadas, personalizadas y empaquetadas que requieren acceso al sistema operativo y al entorno de base de datos subyacentes. Amazon RDS Custom automatiza las tareas y operaciones de administración de bases de datos y le permite, como administrador de bases de datos, acceder y personalizar el entorno de base de datos y el sistema operativo.

Otras herramientas

- Oracle Data Guard es una herramienta que le ayuda a crear y gestionar las bases de datos en espera de Oracle. Este patrón utiliza Oracle Data Guard para configurar una base de datos en espera activa en Amazon RDS Custom.

Epics

Crear una réplica de lectura

Tarea	Descripción	Habilidades requeridas
Crear una réplica de lectura para la instancia de base de datos de Amazon RDS Custom.	Para crear una réplica de lectura, siga las instrucciones de la documentación de Amazon RDS y utilice la instancia de base de datos de Amazon RDS Custom que creó (consulte la sección Requisitos previos) como base de datos de origen. De forma predeterminada, la réplica de lectura de Amazon RDS Custom se crea como física en espera y está en el estado montada. Esto tiene la intención de garantizar el cumplimiento de la licencia de Oracle Active Data Guard. Siga los siguientes pasos para convertir la réplica de lectura al modo de solo lectura.	Administrador de base de datos

Cambie la réplica de lectura a un modo de espera activo de solo lectura

Tarea	Descripción	Habilidades requeridas
Conéctese a la réplica de lectura de Amazon RDS Custom.	Utilice los siguientes comandos para convertir la base de datos física en espera en una base de datos en espera activa.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Importante: estos comandos requieren una licencia de espera activa de Oracle. Para obtener una licencia, póngase en contacto con su represent ante de Oracle. `$ sudo su - rdsdb` `-bash-4.2$ sql` `SQL> select process,s` `tatus,sequence# from v` `$managed_standby;` `PROCESS STATUS` `SEQUENCE#` `--------- ------------` `----------` `ARCH CLOSING` `3956` `ARCH CONNECTED` `0` `ARCH CLOSING` `3955` `ARCH CLOSING` `3957` `RFS IDLE` `0` `RFS IDLE` `3958` `MRP0 APPLYING_LOG` `3958` `SQL> select name,` `database_role,` `open_mode from v` `$database;` `NAME DATABASE_` `ROLE OPEN_MODE`	

Tarea	Descripción	Habilidades requeridas
	--------- --------- ------- --------- ----------- VIS PHYSICAL STANDBY MOUNTED SQL> alter database recover managed standby database cancel; Database altered. Open the standby database SQL> alter database open; Database altered. SQL> select name, database_role, open_mode from v$database; NAME DATABASE_ ROLE OPEN_MODE --------- --------- ------- --------- ----------- VIS PHYSICAL STANDBY READ ONLY	

Tarea	Descripción	Habilidades requeridas
Inicie la recuperación multimedia con la aplicación de un registro en tiempo real.	Para activar la característica de aplicación de registros en tiempo real, utilice los siguientes comandos. Estos convierten y validan la base de datos en espera (réplica de lectura) como una base de datos en espera activa, de modo que pueda conectarse y ejecutar consultas de solo lectura. `SQL>  alter database recover managed standby database using current logfile disconnect from session;` `Database altered`	Administrador de base de datos
Compruebe el estado de la base de datos.	Para comprobar el estado de la base de datos, use el comando siguiente. `SQL> select name, database_role, open_mode from v$database;` `NAME DATABASE_ROLE OPEN_MODE` `--------- ---------- ----------` `VIS PHYSICAL STANDBY READ ONLY WITH APPLY`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Marque el modo de reaplicación.	Para comprobar el modo de reaplicación, utilice el siguiente comando. `SQL> select process,status,sequence# from v$managed_standby;` `PROCESS STATUS SEQUENCE#` `--------- ------------ ----------` `ARCH CLOSING 3956` `ARCH CONNECTED 0` `ARCH CLOSING 3955` `ARCH CLOSING 3957` `RFS IDLE 0` `RFS IDLE 3958` `MRP0 APPLYING_LOG 3958` `SQL> select open_mode from v$database;` `OPEN_MODE` `--------------------` `READ ONLY WITH APPLY`	Administrador de base de datos

Recursos relacionados

- Migre Oracle E-Business Suite a Amazon RDS Custom (Recomendaciones de AWS)
- Uso de Amazon RDS Custom (documentación de Amazon RDS)

- Trabajo con réplicas de lectura para Amazon RDS Custom para Oracle (documentación de Amazon RDS)
- Amazon RDS Custom para Oracle: Nuevas capacidades de control en el entorno de bases de datos (blog de AWS News)
- Migración de Oracle E-Business Suite a AWS (documento técnico de AWS)
- Arquitectura de Oracle E-Business Suite en AWS (documento técnico de AWS)

Configure la replicación de datos entre Amazon RDS para MySQL y MySQL en Amazon EC2 mediante GTID

Creado por Rajesh Madiwale (AWS)

Entorno: PoC o piloto	Tecnologías: bases de datos	Carga de trabajo: código abierto

Resumen

Este patrón describe cómo configurar replicación de datos en la nube de Amazon Web Services (AWS) entre una instancia de base de datos Amazon Relational Database Service (Amazon RDS) para MySQL y una base de datos MySQL en una instancia de Amazon Elastic Compute Cloud (Amazon EC2) mediante la replicación del identificador global de transacciones (GTID) nativo de MySQL.

Con GTID, las transacciones se identifican y rastrean cuando se confirman en el servidor de origen, y se aplican mediante réplicas. No es necesario consultar los archivos de registro al iniciar una nueva réplica durante la conmutación por error.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una instancia de Amazon Linux implementada

Restricciones

- Esta configuración requiere que un equipo interno ejecute las consultas de solo lectura.
- Las versiones de MySQL de origen y de destino deben ser las mismas.
- La replicación se configura en la misma región de AWS y en la misma nube privada virtual (VPC).

Versiones de producto

- Versiones de Amazon RDS 5.7.23 y posteriores, que son aquellas compatibles con GTID

Arquitectura

Pila de tecnología de origen

- Amazon RDS para MySQL

Pila de tecnología de destino

- MySQL en Amazon EC2

Arquitectura de destino

Herramientas

Servicios de AWS

- Amazon Elastic Compute Cloud (Amazon EC2) brinda capacidad de computación escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon Relational Database Service (Amazon RDS) para MySQL lo ayuda a configurar, utilizar y escalar una base de datos relacional de MySQL en la nube de AWS.

Otros servicios

- Los identificadores de transacciones globales (GTID) son indentificadores únicos generados por transacciones confirmadas por MySQL.
- mysqldump es una utilidad de cliente para realizar copias de seguridad lógicas mediante la generación de instrucciones SQL que se pueden ejecutar para reproducir las definiciones de los objetos de la base de datos de origen y los datos de las tablas.
- mysql es el cliente de línea de comandos de MySQL.

Epics

Cree y preparar la instancia de base de datos de Amazon RDS para MySQL

Tarea	Descripción	Habilidades requeridas
Cree la instancia de RDS para MySQL.	Para crear la instancia de RDS para MySQL, siga los pasos de la documentación de Amazon RDS y use los valores de los parámetros que se describen en la siguiente tarea.	DBA, ingeniero DevOps
Habilite la configuración relacionada con GTID en el grupo de parámetros de la base de datos.	Habilite los siguientes parámetros en el grupo de parámetros de base de datos de Amazon RDS para MySQL. Establezca `enforce_gtid_consistency` en on y `gtid-mode` en on.	Administrador de base de datos
Reinicie la instancia de Amazon RDS para MySQL.	Es necesario reiniciar los parámetros para que se apliquen los cambios.	Administrador de base de datos
Cree un usuario y concédale permisos de replicación.	Ejecute los siguientes comandos para instalar MySQL. `CREATE USER 'repl'@'%' IDENTIFIED BY 'xxxx';` `GRANT REPLICATI ON slave ON *.* TO 'repl'@'%' ;` `FLUSH PRIVILEGES;`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas

Instale y prepare MySQL en la instancia de Amazon EC2

Tarea	Descripción	Habilidades requeridas
Instalar MySQL en Amazon Linux.	Ejecute los siguientes comandos para instalar MySQL. `sudo yum update` `sudo wget https://dev.mysql.com/get/mysql57-community-release-el7-11.noarch.rpm` `sudo yum localinstall mysql57-community-release-el7-11.noarch.rpm` `sudo yum install mysql-community-server` `sudo systemctl start mysqld`	Administrador de base de datos
Inicie sesión en MySQL en la instancia de EC2 y cree la base de datos.	El nombre de la base de datos debe ser el mismo que el nombre de la base de datos de Amazon RDS para MySQL. En el ejemplo siguiente, el nombre de la base de datos es `replication` . `create database replication;`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Edite el archivo de configuración de MySQL y reinicie la base de datos.	Edite el archivo`my.conf` que se encuentra en `/etc/` añadiendo los siguientes parámetros. `server-id=3` `gtid_mode=ON` `enforce_gtid_consistency=ON` `replicate-ignore-db=mysql` `binlog-format=ROW` `log_bin=mysql-bin` A continuación, reinicie el servicio `mysqld`. `systemctl mysqld restart`	Administrador de base de datos

Configure la replicación

Tarea	Descripción	Habilidades requeridas
Exporte el volcado de datos de la base de datos Amazon RDS para MySQL.	Para exportar el volcado de Amazon RDS para MySQL, use el siguiente comando. `mysqldump --single-transaction -h mydb.xxxxxxx.amazonaws.com -uadmin -p --databases replication > replication-db.sql`	Administrador de base de datos
Restaure el archivo de volcado de .sql en la base	Para importar el volcado a la base de datos de MySQL en	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
de datos MySQL de Amazon EC2.	Amazon EC2, use el siguiente comando. `mysql -D replication -uroot -p < replication-db.sql`	
Configure la base de datos MySQL en Amazon EC2 como réplica.	Para iniciar la replicación y comprobar su estado, inicie sesión en la base de datos MySQL de Amazon EC2 y ejecute el siguiente comando. `CHANGE MASTER TO MASTER_HOST="mydb.xxxxxxx.amazonaws.com", MASTER_USER="repl", MASTER_PASSWORD="rep123", MASTER_PORT=3306, MASTER_AUTO_POSITION = 1;` `START SLAVE;` `SHOW SLAVE STATUS\G`	Administrador de base de datos

Recursos relacionados

- Guía del usuario de Amazon EC2 para instancias de Linux
- Instalación de MySQL en Linux mediante el repositorio MySQL Yum
- Replicación con identificadores de transacción global
- Uso de reproducción basada en GTID de RDS para Amazon RDS para MySQL

Funciones de transición para una PeopleSoft aplicación de Oracle en Amazon RDS Custom for Oracle

Creado por sampath kathirvel (AWS)

Entorno: producción	Tecnologías: bases de datos; infraestructura	Carga de trabajo: Oracle
Servicios de AWS: Amazon RDS		

Resumen

Para ejecutar la solución de planificación de recursos PeopleSoft empresariales (ERP) de Oracle en Amazon Web Services (AWS), puede utilizar Amazon Relational Database Service (Amazon RDS) o Amazon RDS Custom for Oracle, que admite aplicaciones heredadas, personalizadas y empaquetadas que requieren acceso al sistema operativo (SO) y al entorno de base de datos subyacentes. Para conocer los factores clave a tener en cuenta durante la planificación de una migración, consulte Estrategias de migración de bases de datos Oracle en Recomendaciones de AWS.

Este patrón se centra en los pasos para realizar un cambio de Oracle Data Guard, o transición de funciones, para una base de datos de PeopleSoft aplicaciones que se ejecuta en Amazon RDS Custom como base de datos principal con una base de datos de réplica de lectura. El patrón incluye los pasos para configurar la conmutación por error de inicio rápido (FSFO). Durante este proceso, las bases de datos de la configuración de Oracle Data Guard siguen funcionando en sus nuevos roles. Los casos de uso típicos de transición a Oracle Data Guard son simulacros de recuperación de desastres (DR), actividades de mantenimiento programadas de las bases de datos y parches progresivos de aplicación de parches en espera. Para obtener más información, consulte la publicación de blog Reducir los tiempos de inactividad al parchear bases de datos en Amazon RDS Custom.

Requisitos previos y limitaciones

Requisitos previos

- Finalización del proceso Add HA to Oracle PeopleSoft on Amazon RDS Custom mediante un patrón de réplica de lectura.

Limitaciones

- Limitaciones y configuraciones no compatibles con las RDS Custom for Oracle
- Limitaciones asociadas a las réplicas de lectura de Amazon RDS Custom para Oracle

Versiones de producto

- Para ver las versiones de la base de datos Oracle compatibles con Amazon RDS Custom, consulte RDS Custom para Oracle.
- Para ver las clases de instancias de la base de datos Oracle compatibles con Amazon RDS Custom, consulte Compatibilidad de clases de instancias de base de datos con RDS Custom para Oracle.

Arquitectura

Pila de tecnología

- Amazon RDS Custom para Oracle

Arquitectura de destino

El diagrama siguiente muestra una instancia de base de datos de Amazon RDS Custom y una réplica de lectura de Amazon RDS Custom. Oracle Data Guard proporciona transición de roles durante la conmutación por error para la DR.

Para ver una arquitectura representativa con Oracle PeopleSoft en AWS, consulte Configurar una PeopleSoft arquitectura de alta disponibilidad en AWS.

Herramientas

Servicios de AWS

- Amazon RDS Custom para Oracle es un servicio de base de datos administrado para aplicaciones heredadas, personalizadas y empaquetadas que requieren acceso al sistema operativo y al entorno de base de datos subyacentes.
- AWS Secrets Manager ayuda a reemplazar las credenciales codificadas en el código, incluidas las contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación. En este patrón, recupera las contraseñas de usuario de la base de datos de Secrets Manager para `RDS_DATAGUARD` con el nombre secreto `do-not-delete-rds-custom-+<<RDS Resource ID>>+-dg`.

Otros servicios

- Oracle Data Guard le ayuda a crear, mantener, gestionar y supervisar las bases de datos en espera. Este patrón emplea Oracle Data Guard Maximum Performance para la transición de roles (transición de Oracle Data Guard).

Prácticas recomendadas

Para su implementación de producción, le recomendamos lanzar la instancia de observación en una tercera zona de disponibilidad, separada de los nodos principal y de réplica de lectura.

Epics

Inicie la transición de rol

Tarea	Descripción	Habilidades requeridas
Detenga la automatización de la base de datos, tanto en la base de datos principal como en la réplica.	Si bien el marco de automatización de RDS Custom no interfiere en el proceso de transición de rol, se recomienda pausar la automatización durante la transición a Oracle Data Guard. Para pausar y reanudar la automatización de la base de datos de RDS Custom, siga	Administrador de la nube, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	las instrucciones indicadas en Pausar y reanudar la automatización de RDS Custom.	

Tarea	Descripción	Habilidades requeridas
Compruebe el estado de Oracle Data Guard.	Para comprobar el estado de Oracle Data Guard, inicie sesión en la base de datos principal. Este patrón incluye código para usar una base de datos de contenedor (CDB) multiusuario o una instancia de no CDB. No CDB `-bash-4.2$ dgmgrl RDS_DATAGUARD@RDS_CUSTOM_ORCL_A` `DGMGRL for Linux: Release 19.0.0.0.0 - Production on Mon Nov 28 20:55:50 2022` `Version 19.10.0.0.0` `Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved.` `Welcome to DGMGRL, type "help" for informati on.` `Password:` `Connected to "ORCL_A"` `Connected as SYSDG.` `DGMGRL> show configura tion` `Configuration - rds_dg` `Protection Mode: MaxAvailability` `Members:` `orcl_a - Primary database` `orcl_d - Physical standby database`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 59 seconds ago) DGMGRL> CDB CDB-bash-4.2$ dgmgrl C##RDS_DATAGUARD@R DS_CUSTOM_RDSCDB_A DGMGRL for Linux: Release 19.0.0.0.0 - Production on Wed Jan 18 06:13:07 2023 Version 19.16.0.0.0 Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved. Welcome to DGMGRL, type "help" for informati on. Password: Connected to "RDSCDB_A " Connected as SYSDG. DGMGRL> show configura tion Configuration - rds_dg Protection Mode: MaxAvailability Members: rdscdb_a - Primary database rdscdb_b - Physical standby database Fast-Start Failover: Disabled Configuration Status:	

Tarea	Descripción	Habilidades requeridas
	`SUCCESS (status updated 52 seconds ago)` `DGMGRL>`	
Verifique el rol de instancia.	Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon RDS. En la sección Replicación de la base de datos, en la pestaña Conectividad y seguridad, verifique el rol de instancia para la instancia principal y la réplica. El rol principal debe coincidir con la base de datos principal de Oracle Data Guard, y el rol de réplica debe coincidir con la base de datos física en espera de Oracle Data Guard.	Administrador de la nube, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
Realice la transición.	Para realizar la transición, conéctese a DGMGRL desde el nodo principal. No CDB `DGMGRL> switchover to orcl_d;` `Performing switchover NOW, please wait...` `Operation requires a connection to database "orcl_d"` `Connecting ...` `Connected to "ORCL_D"` `Connected as SYSDG.` `New primary database "orcl_d" is opening...` `Operation requires start up of instance "ORCL" on database "orcl_a"` `Starting instance "ORCL"...` `Connected to an idle instance.` `ORACLE instance started.` `Connected to "ORCL_A"` `Database mounted.` `Database opened.` `Connected to "ORCL_A"` `Switchover succeeded, new primary is "orcl_d"` `DGMGRL>` CDB `DGMGRL> switchover to rdscdb_b`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`Performing switchover NOW, please wait...` `New primary database "rdscdb_b" is opening...` `Operation requires start up of instance "RDSCDB" on database "rdscdb_a"` `Starting instance "RDSCDB"...` `Connected to an idle instance.` `ORACLE instance started.` `Connected to "RDSCDB_A"` `Database mounted.` `Database opened.` `Connected to "RDSCDB_A"` `Switchover succeeded, new primary is "rdscdb_b"`	

Tarea	Descripción	Habilidades requeridas
Verifique la conexión de Oracle Data Guard.	Tras la transición, compruebe la conexión de Oracle Data Guard desde el nodo principal a `DGMGRL`. No CDB `DGMGRL> show configura tion;` `Configuration - rds_dg` `Protection Mode:` ` MaxAvailability` `Members:` `orcl_d - Primary` ` database` `orcl_a - Physical` ` standby database` `Fast-Start Failover:` ` Disabled` `Configuration Status:` `SUCCESS (status updated` ` 60 seconds ago)` `DGMGRL>` `DGMGRL> show configura tion lag;` `Configuration - rds_dg` `Protection Mode:` ` MaxAvailability` `Members:` `orcl_d - Primary` ` database` `orcl_a - Physical` ` standby database` `Transport Lag: 0` ` seconds (computed 0` ` seconds ago)` `Apply Lag: 0 seconds` ` (computed 0 seconds` ` ago)`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 44 seconds ago) DGMGRL>	
	CDB DGMGRL> show configura tion DGMGRL> show configura tion Configuration - rds_dg Protection Mode: MaxAvailability Members: rdscdb_b - Primary database rdscdb_a - Physical standby database Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 52 seconds ago) DGMGRL> DGMGRL> show configura tion lag Configuration - rds_dg Protection Mode: MaxAvailability Members: rdscdb_b - Primary database rdscdb_a - Physical standby database Transport Lag: 0 seconds	

Tarea	Descripción	Habilidades requeridas
	(computed 0 seconds ago) Apply Lag: 0 seconds (computed 0 seconds ago) Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 53 seconds ago) DGMGRL>	
Verifique el rol de instancia en la consola de Amazon RDS.	Tras realizar el cambio de rol, la consola de Amazon RDS muestra los nuevos roles en la sección Replicación de la pestaña Conectividad y seguridad, en Bases de datos. Es posible que el Estado de replicación tarde unos minutos en actualizarse de vacío a Replicando.	Administrador de base de datos

Configure la FSFO

Tarea	Descripción	Habilidades requeridas
Restablezca la transición.	Vuelva a establecer la transición en el nodo principal.	Administrador de base de datos
Instale e inicie el observador.	Un proceso de observación es un componente del cliente DGMGRL que, por lo general, se ejecuta en una máquina diferente a la de las bases de	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	datos principal y en espera. La instalación de ORACLE HOME para el observador puede ser una instalación de Oracle Client Administrator. También puede instalar Oracle Database Enterprise Edition o Personal Edition. Para obtener más información sobre la instalación del observador para su versión de base de datos, consulte Instalar e iniciar el observador. Para configurar la alta disponibilidad para el proceso de observación, puede hacer lo siguiente: • Habilite la recuperación automática de la instancia de EC2 en la instancia de EC2 que ejecuta el observador. Debe automatizar el proceso de inicio del observador como parte del inicio del sistema operativo. • Implemente un observador en la instancia de EC2 y configure un grupo de Amazon EC2 Auto Scaling de tamaño uno (1). En caso de que se produzca un error en la instancia de EC2, el grupo de escalado automático	

Tarea	Descripción	Habilidades requeridas
	activará automáticamente otra instancia de EC2. En la versión 2 de Oracle 12c y versiones posteriores, puede implementar hasta tres observadores. Uno es el observador principal, y el resto son observadores de respaldo. Cuando el observador principal falla, uno de los observadores de respaldo asume el rol de principal.	

Tarea	Descripción	Habilidades requeridas
Conéctese a DGMGRL desde el host del observador.	El host del observador está configurado con entradas `tnsnames.ora` para la conectividad de las bases de datos principal y en espera. Puede habilitar la FSFO con el modo de protección de máximo rendimiento siempre que la pérdida de datos esté dentro de la FastStart FailoverLagLimitconfiguración (valor en segundos). Sin embargo, debe utilizar el modo de protección de máxima disponibilidad para lograr una pérdida de datos cero (RPO=0). No CDB `DGMGRL> show configuration;` `Configuration - rds_dg` `Protection Mode: MaxAvailability` `Members:` `orcl_a - Primary database` `orcl_d - Physical standby database` `Fast-Start Failover: Disabled` `Configuration Status:` `SUCCESS (status updated 58 seconds ago)` `DGMGRL> show configuration lag` `Configuration - rds_dg`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Protection Mode: MaxAvailability Members: orcl_a - Primary database orcl_d - Physical standby database Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 0 seconds (computed 1 second ago) Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 5 seconds ago) DGMGRL> CDB -bash-4.2$ dgmgrl C##RDS_DATAGUARD@R DS_CUSTOM_RDSCDB_A DGMGRL for Linux: Release 19.0.0.0.0 - Production on Wed Jan 18 06:55:09 2023 Version 19.16.0.0.0 Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved. Welcome to DGMGRL, type "help" for informati on. Password: Connected to "RDSCDB_A " Connected as SYSDG.	

Tarea	Descripción	Habilidades requeridas
	`DGMGRL> show configura tion Configuration - rds_dg Protection Mode: MaxAvailability Members: rdscdb_a - Primary database rdscdb_b - Physical standby database Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 18 seconds ago) DGMGRL>`	

Tarea	Descripción	Habilidades requeridas
Modifique la base de datos en espera para que sea el objetivo de la conmutación por error.	Conéctese desde el nodo principal o desde el nodo de observador a una base de datos en espera. (Aunque su configuración puede tener varias bases de datos en espera, solo necesita conectarse a una en este momento). No CDB `DGMGRL> edit database orcl_a set property FastStartFailoverTarget='orcl_d';` `Property "faststartfailovertarget" updated` `DGMGRL> edit database orcl_d set property FastStartFailoverTarget='orcl_a';` `Property "faststartfailovertarget" updated` `DGMGRL> show database orcl_a FastStartFailoverTarget;` `FastStartFailoverTarget = 'orcl_d'` `DGMGRL> show database orcl_d FastStartFailoverTarget;` `FastStartFailoverTarget = 'orcl_a'` `DGMGRL>` CDB	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`DGMGRL> edit database orcl_a set property FastStartFailoverTarget='rdscdb_b';` `Object "orcl_a" was not found` `DGMGRL> edit database rdscdb_a set property FastStartFailoverTarget='rdscdb_b';` `Property "faststartfailovertarget" updated` `DGMGRL> edit database rdscdb_b set property FastStartFailoverTarget='rdscdb_a';` `Property "faststartfailovertarget" updated` `DGMGRL> show database rdscdb_a FastStartFailoverTarget;` `FastStartFailoverTarget = 'rdscdb_b'` `DGMGRL> show database rdscdb_b FastStartFailoverTarget;` `FastStartFailoverTarget = 'rdscdb_a'` `DGMGRL>`	

Tarea	Descripción	Habilidades requeridas
Configure la conexión FastStartFailoverThreshold a la DGMGRL.	El valor predeterminado es de 30 segundos en Oracle 19c. El valor mínimo es de 6 segundos. Un valor inferior puede acortar el objetivo de tiempo de recuperación (RTO) durante la conmutación por error. Un valor superior ayuda a reducir la posibilidad de que se produzcan errores transitorios de conmutación por error innecesarios en la base de datos principal. El marco de automatización de RDS Custom para Oracle supervisa el estado de la base de datos y lleva a cabo acciones correctivas cada pocos segundos. Por lo tanto, se recomienda establecer un valor superior FastStart FailoverThreshold a 10 segundos. En el siguiente ejemplo, se configura el valor de umbral en 35 segundos. No CBD o CDB `DGMGRL> edit configuration set property FastStartFailoverThreshold=35;` `Property "faststartfailoverthreshold" updated`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`DGMGRL> show configura tion FastStart FailoverThreshold; FastStartFailover Threshold = '35' DGMGRL>`	

Tarea	Descripción	Habilidades requeridas
Habilite la FSFO conectándose a DGMGRL desde el nodo principal o el nodo de observador.	Si la base de datos no tiene activada la base de datos Flashback, aparecerá el mensaje de advertencia `ORA-16827` . La base de datos retrospectiva opcional ayuda a restablecer automáticamente las bases de datos principales con errores a un punto en el tiempo anterior a la conmutación por error si la propiedad de FastStartFailoverAutoReinstateconfiguración está establecida en `TRUE` (que es la predeterminada). No CDB `DGMGRL> enable fast_start failover;` `Warning: ORA-16827: Flashback Database is disabled` `Enabled in Zero Data Loss Mode.` `DGMGRL>` `DGMGRL> show configuration` `Configuration - rds_dg` `Protection Mode: MaxAvailability` `Members:` `orcl_a - Primary database` `Warning: ORA-16819: fast-start failover observer not started`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	orcl_d - (*) Physical standby database Warning: ORA-16819: fast-start failover observer not started Fast-Start Failover: Enabled in Zero Data Loss Mode Configuration Status: WARNING (status updated 29 seconds ago) DGMGRL> CDB DGMGRL> enable fast_star t failover; Warning: ORA-16827: Flashback Database is disabled Enabled in Zero Data Loss Mode. DGMGRL> show configura tion; Configuration - rds_dg Protection Mode: MaxAvailability Members: rdscdb_a - Primary database Warning: ORA-16819 : fast-start failover observer not started rdscdb_b - (*) Physical standby database Fast-Start Failover: Enabled in Zero Data Loss Mode Configuration Status:	

Tarea	Descripción	Habilidades requeridas
	`WARNING (status updated 11 seconds ago)` `DGMGRL>`	

Tarea	Descripción	Habilidades requeridas
Inicie el observador para la supervisión de la FSFO y verifique el estado.	Puede iniciar el observador antes o después de activar la FSFO. Si la FSFO ya está habilitada, el observador comienza inmediatamente a supervisar el estado y las conexiones a las bases de datos principal y en espera. Si la FSFO no está habilitada, el observador no comienza a supervisar hasta que la FSFO esté habilitada. Al iniciar el observador, la configuración de base de datos principal se mostrará sin ningún mensaje de error, como demuestra el comando anterior `show configuration` . No CDB `DGMGRL> start observer;` `[W000 2022-12-01T06:16:51.271+00:00]` `FSFO target standby is orcl_d` `Observer 'ip-10-0-1-89' started` `[W000 2022-12-01T06:16:51.352+00:00]` `Observer trace level is set to USER` `DGMGRL> show configuration` `Configuration - rds_dg`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Protection Mode: MaxAvailability Members: orcl_a - Primary database orcl_d - (*) Physical standby database Fast-Start Failover: Enabled in Zero Data Loss Mode Configuration Status: SUCCESS (status updated 56 seconds ago) DGMGRL> DGMGRL> show observer Configuration - rds_dg Primary: orcl_a Active Target: orcl_d Observer "ip-10-0- 1-89" - Master Host Name: ip-10-0-1 -89 Last Ping to Primary: 1 second ago Last Ping to Target: 1 second ago DGMGRL> CDB DGMGRL> start observer; Succeeded in opening the observer file "/home/oracle/fsfo _ip-10-0-1-56.dat". [W000 2023-01-1 8T07:31:32.589+00:00] FSFO target standby is rdscdb_b	

Tarea	Descripción	Habilidades requeridas
	Observer 'ip-10-0-1-56' started The observer log file is '/home/oracle/observer_ip-10-0-1-56.log'. DGMGRL> show configuration Configuration - rds_dg Protection Mode: MaxAvailability Members: rdscdb_a - Primary database rdscdb_b - (*) Physical standby database Fast-Start Failover: Enabled in Zero Data Loss Mode Configuration Status: SUCCESS (status updated 12 seconds ago) DGMGRL> DGMGRL> show observer; Configuration - rds_dg Primary: rdscdb_a Active Target: rdscdb_b Observer "ip-10-0-1-56" - Master Host Name: ip-10-0-1-56 Last Ping to Primary: 1 second ago Last Ping to Target: 2 seconds ago DGMGRL>	

Tarea	Descripción	Habilidades requeridas
Verifique la conmutación por error.	En este escenario, puede realizar una prueba de conmutación por error deteniendo manualmente la instancia de EC2 principal. Antes de detener la instancia de EC2, ejecute el comando `tail` para supervisar el archivo de registro del observador en función de su configuración. Use `DGMGRL` para iniciar sesión en la base de datos en espera `orcl_d` con el usuario `RDS_DATAGUARD` y compruebe el estado de Oracle Data Guard. Debería mostrar que `orcl_d` es la nueva base de datos principal. Nota: en este escenario de prueba de conmutación por error, `orcl_d` es una base de datos no CDB. Antes de la conmutación por error, la base de datos Flashback se ha habilitado en `orcl_a`. Cuando la anterior base de datos principal vuelva a estar en línea y regrese al estado `MOUNT`, el observador la restablecerá en una nueva base de datos en espera. La base de datos restablec	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	ida actúa como destino de la FSFO para la nueva base de datos principal. Puede verificar los detalles en los registros del observador. `DGMGRL> show configura tion Configuration - rds_dg Protection Mode: MaxAvailability Members: orcl_d - Primary database Warning: ORA-16824 : multiple warnings, including fast-star t failover-related warnings, detected for the database orcl_a - (*) Physical standby database (disabled) ORA-16661: the standby database needs to be reinstated Fast-Start Failover: Enabled in Zero Data Loss Mode Configuration Status: WARNING (status updated 25 seconds ago) DGMGRL>`  A continuación se muestra un ejemplo de salida`observer. log` .	

Tarea	Descripción	Habilidades requeridas
	`$ tail -f /tmp/obse rver.log` `Unable to connect to database using rds_custom_orcl_a` `[W000 2023-01-1 8T07:50:32.589+00:00] Primary database cannot be reached.` `[W000 2023-01-1 8T07:50:32.589+00:00] Fast-Start Failover threshold has expired.` `[W000 2023-01-1 8T07:50:32.590+00:00] Try to connect to the standby.` `[W000 2023-01-1 8T07:50:32.590+00: 00] Making a last connection attempt to primary database before proceeding with Fast-Start Failover.` `[W000 2023-01-1 8T07:50:32.591+00:00] Check if the standby is ready for failover.` `[S002 2023-01-1 8T07:50:32.591+00:00] Fast-Start Failover started...` `2023-01-18T07:50 :32.591+00:00` `Initiating Fast-Star t Failover to database "orcl_d"...` `[S002 2023-01-1 8T07:50:32.592+00:00] Initiating Fast-start Failover.`	

Tarea	Descripción	Habilidades requeridas
	`Performing failover NOW, please wait... Failover succeeded, new primary is "orcl_d" 2023-01-18T07:55:32.101+00:00 [S002 2023-01-18T07:55:32.591+00:00] Fast-Start Failover finished... [W000 2023-01-18T07:55:32.591+00:00] Failover succeeded. Restart pinging. [W000 2023-01-18T07:55:32.603+00:00] Primary database has changed to orcl_d. [W000 2023-01-18T07:55:33.618+00:00] Try to connect to the primary. [W000 2023-01-18T07:55:33.622+00:00] Try to connect to the primary rds_custom_orcl_d. [W000 2023-01-18T07:55:33.634+00:00] The standby orcl_a needs to be reinstated [W000 2023-01-18T07:55:33.654+00:00] Try to connect to the new standby orcl_a. [W000 2023-01-18T07:55:33.654+00:00] Connection to the primary restored! [W000 2023-01-18T07:55:35.654+00:00] Disconnecting`	

Tarea	Descripción	Habilidades requeridas
	`from database rds_custo m_orcl_d. [W000 2023-01-1 8T07:55:57.701+00:00] Try to connect to the new standby orcl_a. ORA-12170: TNS:Connect timeout occurred`	

Configure la conectividad entre la aplicación Oracle Peoplesoft y la base de datos

Tarea	Descripción	Habilidades requeridas
Cree e inicie el servicio en la base de datos principal.	Puede evitar los cambios en la configuración de la aplicación durante la transición de rol con una entrada de TNS que contenga en la configuración los puntos de conexión de las bases de datos principal y en espera. Puede definir dos servicios de bases de datos basados en roles para admitir cargas de trabajo de lectura y escritura y de solo lectura. En el siguiente ejemplo, `orcl_rw` es el servicio de lectura/escritura activo en la base de datos principal. `orcl_ro` es el servicio de solo lectura, activo en la base de datos en espera que se ha abierto en modo de solo lectura.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`SQL> select name,open _mode from v$database; NAME OPEN_MODE --------- --------- ----------- ORCL READ WRITE SQL> exec dbms_serv ice.create_service ('orcl_rw','orcl_r w'); PL/SQL procedure successfully completed . SQL> exec dbms_serv ice.create_service ('orcl_ro','orcl_r o'); PL/SQL procedure successfully completed .`  `SQL> exec dbms_serv ice.start_service('orcl_rw'); PL/SQL procedure successfully completed . SQL>`	

Tarea	Descripción	Habilidades requeridas
Inicie el servicio en la base de datos en espera.	Para iniciar el servicio en la base de datos en espera de solo lectura, ejecute el siguiente código. `SQL> select name,open _mode from v$database; NAME OPEN_MODE --------- ---------- ----------- ORCL READ ONLY WITH  APPLY SQL> exec dbms_serv ice.start_service( 'orcl_ro'); PL/SQL procedure  successfully completed . SQL>`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Automatice el inicio del servicio cuando se reinicie la base de datos principal.	Para iniciar automáticamente el servicio en la base de datos principal cuando se reinicie, ejecute el siguiente código. `SQL> CREATE OR REPLACE TRIGGER TrgDgServices after startup on database DECLARE db_role VARCHAR(30); db_open_mode VARCHAR(30); BEGIN SELECT DATABASE_ROLE, OPEN_MODE INTO db_role, db_open_mode FROM V$DATABASE; IF db_role = 'PRIMARY' THEN DBMS_SERV 2 ICE.START_SERVICE('orcl_rw'); END IF; IF db_role = 'PHYSICAL STANDBY' AND db_open_mode LIKE 'READ ONLY%' THEN DBMS_SERVICE.START_SERVICE('orcl_ro'); END IF; END; / Trigger created. SQL>`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Configure una conexión entre las bases de datos de lectura/escritura y de solo lectura.	Puede usar el siguiente ejemplo de configuración de aplicación para la conexión de lectura/escritura y de solo lectura. `ORCL_RW = (DESCRIPTION = (CONNECT_TIMEOUT= 120)(RETRY_COUNT=20)(RETRY_DELAY=3)(TRANSPORT_CONNECT_TIMEOUT=3) (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST=devpsftdb.******.us-west-2.rds.amazonaws.com) (PORT=1521)) (ADDRESS = (PROTOCOL = TCP)(HOST=psftread.******.us-west-2.rds.amazonaws.com) (PORT=1521))) (CONNECT_DATA=(SERVICE_NAME = orcl_rw)))` `ORCL_RO = (DESCRIPTION = (CONNECT_TIMEOUT= 120)(RETRY_COUNT=20)(RETRY_DELAY=3)(TRANSPORT_CONNECT_TIMEOUT=3) (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST=devpsftdb.******.us-west-2`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`.rds.amazonaws.com) (PORT=1521)) (ADDRESS = (PROTOCOL = TCP)(HOST=psftread .******.us-west-2. rds.amazonaws.com) (PORT=1521)) ) (CONNECT_DATA=(SERVIC E_NAME = orcl_ro)) )`	

Recursos relacionados

- Habilitar la alta disponibilidad con Data Guard en Amazon RDS Custom para Oracle (guía técnica de AWS)
- Configuración de Amazon RDS como una PeopleSoft base de datos de Oracle (documento técnico de AWS)
- Guía de agente de Oracle Data Guard (documentación de referencia de Oracle)
- Oracle Data Guard Concepts and Administration(documentación de referencia de Oracle)
- Requisitos de configuración de FAN y FCF específicos de Oracle Data Guard (documentación de referencia de Oracle)

Patrones de migración de bases de datos según la carga

Temas

IBM

- Migrar una base de datos de Db2 de Amazon EC2 a Aurora compatible con MySQL mediante AWS DMS
- Migre Db2 para LUW a Amazon EC2 mediante envío de registros para reducir el tiempo de interrupción
- Migración de Db2 para LUW a Amazon EC2 con recuperación de desastres de alta disponibilidad
- Migrar de IBM Db2 en Amazon EC2 a compatible con Aurora PostgreSQL mediante AWS DMS y AWS SCT
- Migre de IBM WebSphere Application Server a Apache Tomcat en Amazon EC2
- Proteja y optimice el acceso de los usuarios a una base de datos de federación DB2 en AWS mediante contextos de confianza

Microsoft

- Acelere el descubrimiento y la migración de las cargas de trabajo de Microsoft a AWS
- Acceso a tablas en las instalaciones de Microsoft SQL Server desde Microsoft SQL Server en Amazon EC2 mediante servidores vinculados
- Evaluar el rendimiento de las consultas para migrar bases de datos de SQL Server a MongoDB Atlas en AWS
- Cambie las aplicaciones de Python y Perl para que admitan la migración de bases de datos de Microsoft SQL Server a una edición compatible con PostgreSQL de Amazon Aurora
- Configure el enrutamiento de solo lectura en un grupo de disponibilidad Always On en SQL Server en AWS
- Cree CloudFormation plantillas de AWS para las tareas de AWS DMS con Microsoft Excel y Python
- Exportación de una base de datos de Microsoft SQL Server a Amazon S3 mediante AWS DMS
- Exporte tablas de Amazon RDS para SQL Server a un bucket S3 mediante AWS DMS
- Incorporar y migrar instancias de Windows de EC2 a una cuenta de AWS Managed Services
- Migración de una cola de mensajes de Microsoft Azure Service Bus a Amazon SQS
- Migración de una base de datos de Microsoft SQL Server de Amazon EC2 a Amazon DocumentDB mediante AWS DMS
- Migración de una base de datos de Microsoft SQL Server a Aurora MySQL mediante AWS DMS y AWS SCT
- Migración de una aplicación .NET de Microsoft Azure App Service a AWS Elastic Beanstalk
- Migración de una base de datos de Microsoft SQL Server en las instalaciones a Amazon EC2
- Migración de una base de datos de Microsoft SQL Server en las instalaciones a Amazon RDS para SQL Server
- Migración de bases de datos en las instalaciones de Microsoft SQL Server a Amazon RDS para SQL Server mediante servidores vinculados
- Migre una base de datos de Microsoft SQL Server en las instalaciones a Amazon RDS para SQL Server mediante métodos nativos de copia de seguridad y restauración
- Migre una base de datos de Microsoft SQL Server en las instalaciones a Amazon Redshift mediante AWS DMS
- Migre una base de datos en las instalaciones de Microsoft SQL Server a Amazon Redshift mediante agentes de extracción de datos de AWS SCT

- ???
- Migre datos de Microsoft Azure Blob a Amazon S3 mediante Rclone
- Migrar SQL Server a AWS mediante grupos de disponibilidad distribuidos
- Migración de los certificados SSL de Windows a un equilibrador de carga de aplicación mediante ACM
- ???
- Envíe notificaciones para una instancia de base de datos de Amazon RDS para SQL Server mediante un servidor SMTP en las instalaciones y el Correo de base de datos
- Configure una infraestructura Multi-AZ para una FCI Always On de SQL Server mediante Amazon FSx

N/A

- Crear un proceso de aprobación para las solicitudes de firewall durante una migración para volver a alojar a AWS
- Cifrar una instancia de base de datos de Amazon RDS para PostgreSQL existente
- Costos de almacenamiento estimados para una tabla de Amazon DynamoDB
- Implemente recuperación de desastres entre regiones con AWS DMS y Amazon Aurora

Código abierto

- ???
- Crear usuarios y roles de aplicaciones en Aurora compatible con PostgreSQL
- Habilite conexiones cifradas para instancias de base de datos de PostgreSQL en Amazon RDS
- ???
- Migración de una base de datos MySQL en las instalaciones a Amazon EC2
- Migrar una base de datos MySQL en las instalaciones a Amazon RDS para MySQL
- Migrar de una base de datos de MySQL en las instalaciones a Aurora MySQL
- Migrar una base de datos PostgreSQL en las instalaciones a Aurora PostgreSQL
- Migre de IBM WebSphere Application Server a Apache Tomcat en Amazon EC2 con Auto Scaling
- Migre de Oracle 8i o 9i a Amazon RDS para Oracle con AWS DMS SharePlex
- Migre de Oracle GlassFish a AWS Elastic Beanstalk
- Migre de PostgreSQL en Amazon EC2 a Amazon RDS para PostgreSQL mediante pglogical
- Migración de aplicaciones Java locales en las instalaciones a AWS mediante AWS App2Container
- Migre bases de datos MySQL locales a Aurora MySQL mediante Percona, XtraBackup Amazon EFS y Amazon S3
- Migre tablas externas de Oracle a Amazon Aurora compatible con PostgreSQL
- Migre funciones y procedimientos de Oracle con más de 100 argumentos a PostgreSQL
- Migración de las cargas de trabajo de Redis a Redis Enterprise Cloud en AWS
- Supervisar Amazon Aurora en busca de instancias sin cifrado
- Reinicie el agente de replicación de AWS automáticamente sin deshabilitar SELinux después de reiniciar un servidor fuente de RHEL
- Programe trabajos para Amazon RDS para PostgreSQL y Aurora PostgreSQL mediante Lambda y Secrets Manager
- Configure la replicación de datos entre Amazon RDS para MySQL y MySQL en Amazon EC2 mediante GTID
- Transportar bases de datos PostgreSQL entre dos instancias de base de datos de Amazon RDS utilizando pg_transport

Oracle

- Agregue HA a Oracle PeopleSoft en Amazon RDS Custom mediante una réplica de lectura
- Configurar enlaces entre la base de datos de Oracle y Aurora compatible con PostgreSQL
- Convertir consultas JSON de Oracle en SQL de bases de datos PostgreSQL
- Convierta el tipo de datos VARCHAR2 (1) para Oracle en un tipo de datos booleano para Amazon Aurora PostgreSQL
- Emule Oracle DR mediante una base de datos global de Aurora compatible con PostgreSQL
- Emule cargas de trabajo de Oracle RAC mediante puntos de conexión personalizados en Aurora PostgreSQL
- Calcule el tamaño del motor de Amazon RDS para una base de datos de Oracle mediante informes de AWR
- Gestionar bloques anónimos en instrucciones SQL dinámicas en Aurora PostgreSQL
- Gestionar las sobrecargadas funciones de Oracle en Aurora PostgreSQL
- Migre gradualmente de Amazon RDS para Oracle a Amazon RDS para PostgreSQL con Oracle SQL Developer y AWS SCT
- ???
- Migrar las instancias de base de datos de Amazon RDS para Oracle a otras cuentas que usen AMS
- Migrar Amazon RDS para Oracle a Amazon RDS para PostgreSQL en modo SSL mediante AWS DMS
- Migre Amazon RDS para Oracle a Amazon RDS para PostgreSQL con AWS SCT y AWS DMS mediante AWS CLI y AWS CloudFormation
- ???
- Migre una instancia de base de datos de Amazon RDS para Oracle a otra VPC
- Migre una base de datos de Oracle en las instalaciones a Amazon EC2 mediante Oracle Data Pump
- Migre una base de datos Oracle local a Amazon OpenSearch Service mediante Logstash
- Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para MySQL con AWS DMS y AWS SCT
- Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle

- Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle mediante Oracle Data Pump
- Migrar una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle mediante Oracle Data Pump
- Migre una base de datos Oracle en las instalaciones a Amazon RDS para PostgreSQL mediante Oracle Bystander y AWS DMS
- Migre una base de datos de Oracle en las instalaciones a Amazon EC2
- Migrar una base de datos Oracle de Amazon EC2 a Amazon RDS para MariaDB mediante AWS DMS y AWS SCT
- Migración de una base de datos de Oracle de Amazon EC2 a Amazon RDS para Oracle mediante AWS DMS
- Migrar una base de datos de Oracle a Amazon DynamoDB mediante AWS DMS
- Migre una base de datos Oracle a Amazon RDS for Oracle mediante adaptadores de archivos planos de GoldenGate Oracle
- Migración de una base de datos de Oracle a Amazon Redshift con AWS DMS y AWS SCT
- Migrar una base de datos de Oracle a Aurora PostgreSQL con AWS DMS y AWS SCT
- Migre una EnterpriseOne base de datos de Oracle JD Edwards a AWS mediante Oracle Data Pump y AWS DMS
- Migre una tabla particionada de Oracle a PostgreSQL mediante AWS DMS
- Migre una PeopleSoft base de datos de Oracle a AWS mediante AWS DMS
- Migre datos de una base de datos Oracle en las instalaciones a Aurora PostgreSQL
- Migrar de Amazon RDS para Oracle a Amazon RDS para MySQL
- Migre de Oracle 8i o 9i a Amazon RDS para PostgreSQL mediante la vista materializada y AWS DMS
- Migre de Oracle 8i o 9i a Amazon RDS para PostgreSQL mediante AWS DMS SharePlex
- Migre de Oracle Database a Amazon RDS for PostgreSQL mediante Oracle GoldenGate
- ???
- Migración de Oracle a Amazon DocumentDB con AWS DMS
- Migre de Oracle WebLogic a Apache Tomcat (ToMEE) en Amazon ECS
- Migre índices basados en funciones de Oracle a PostgreSQL
- Migre aplicaciones heredadas de Oracle Pro*C a ECPG
- Migre valores CLOB de Oracle a filas individuales en PostgreSQL en AWS

- Migre los códigos de error de Oracle Database a una base de datos Amazon Aurora compatible con PostgreSQL
- Migre Oracle E-Business Suite a Amazon RDS Custom
- Migrar las funciones nativas de Oracle a PostgreSQL mediante extensiones
- Migrar las variables de enlace OUT de Oracle a una base de datos PostgreSQL
- Migre Oracle PeopleSoft a Amazon RDS Custom
- Migre la funcionalidad ROWIdentificador de Oracle a PostgreSQL en AWS
- Migre los paquetes pragma SERIALLY_REUTILIZABLE de Oracle a PostgreSQL
- Migre columnas generadas de forma virtual de Oracle a PostgreSQL
- Supervise GoldenGate los registros de Oracle mediante Amazon CloudWatch
- Redefina la plataforma de Oracle Database Enterprise Edition a Standard Edition 2 en Amazon RDS para Oracle
- Configure una arquitectura HA/DR para Oracle E-Business Suite en Amazon RDS Custom con una base de datos en espera activa
- Configure la funcionalidad UTL_FILE de Oracle en Aurora compatible con PostgreSQL
- Funciones de transición para una PeopleSoft aplicación de Oracle en Amazon RDS Custom for Oracle
- Validar los objetos de la base de datos después de migrar de Oracle a Amazon Aurora PostgreSQL

SAP

- Realice copias de seguridad automáticas de las bases de datos de SAP HANA mediante Systems Manager y EventBridge
- Migración de una base de datos de SAP ASE en las instalaciones a Amazon EC2
- Migración de SAP ASE a Amazon RDS para SQL Server utilizando AWS DMS
- Migre SAP ASE de Amazon EC2 a Amazon Aurora compatible con PostgreSQL mediante AWS SCT y AWS DMS
- ???
- Reduzca el tiempo de transición de la migración homogénea de SAP mediante el servicio de migración de aplicaciones
- Configurar la recuperación de desastres para SAP en IBM Db2 en AWS

Más patrones

- Acceder, consultar y unirse a las tablas de Amazon DynamoDB con Athena
- Agregue datos en Amazon DynamoDB para pronósticos de ML en Athena
- Permitir a las instancias de EC2 el acceso de escritura a los buckets de S3 en las cuentas de AMS
- Analice y visualice datos JSON anidados con Amazon Athena y Amazon QuickSight
- Autenticar Microsoft SQL Server en Amazon EC2 mediante AWS Directory Service
- Automatizar las copias de seguridad de las instancias de base de datos de Amazon RDS para PostgreSQL mediante AWS Batch
- Archivar automáticamente los elementos en Amazon S3 con DynamoDB TTL
- Genere automáticamente un modelo de PynamoDB y funciones CRUD para Amazon DynamoDB mediante una aplicación de Python
- Corrija automáticamente las instancias y los clústeres de bases de datos de Amazon RDS no cifrados
- ???
- Cree una arquitectura de acoplamiento flexible con microservicios mediante DevOps prácticas y AWS Cloud9
- Cambie las aplicaciones de Python y Perl para que admitan la migración de bases de datos de Microsoft SQL Server a una edición compatible con PostgreSQL de Amazon Aurora
- Configurar el acceso entre cuentas a Amazon DynamoDB
- Configurar enlaces entre la base de datos de Oracle y Aurora compatible con PostgreSQL
- Convierta y desempaquete datos EBCDIC a ASCII en AWS mediante Python
- Convierta la característica temporal NORMALIZE de Teradata en Amazon Redshift SQL
- Convierta la característica RESET WHEN de Teradata en Amazon Redshift SQL
- Convierta el tipo de datos VARCHAR2 (1) para Oracle en un tipo de datos booleano para Amazon Aurora PostgreSQL
- Crear usuarios y roles de aplicaciones en Aurora compatible con PostgreSQL
- Cree CloudFormation plantillas de AWS para las tareas de AWS DMS con Microsoft Excel y Python
- ???
- Implementar un clúster de Cassandra en Amazon EC2 con IP estáticas privadas para evitar el reequilibrio

- Desarrolle asistentes avanzados de IA generativa basados en chat mediante RAG y solicitudes ReAct
- Emule Oracle DR mediante una base de datos global de Aurora compatible con PostgreSQL
- Habilitar el cifrado transparente de datos en Amazon RDS para SQL Server
- Exportación de una base de datos de Microsoft SQL Server a Amazon S3 mediante AWS DMS
- Migre gradualmente de Amazon RDS para Oracle a Amazon RDS para PostgreSQL con Oracle SQL Developer y AWS SCT
- ???
- Administrar credenciales mediante AWS Secrets Manager
- Migrar una base de datos de Db2 de Amazon EC2 a Aurora compatible con MySQL mediante AWS DMS
- Migración de una base de datos de Microsoft SQL Server de Amazon EC2 a Amazon DocumentDB mediante AWS DMS
- Migración de una base de datos de Microsoft SQL Server a Aurora MySQL mediante AWS DMS y AWS SCT
- Migración de un entorno de MongoDB autoalojado a MongoDB Atlas en la nube de AWS
- Migración de una base de datos de Teradata a Amazon Redshift con los agentes de extracción de datos de AWS SCT
- Migrar Amazon RDS para Oracle a Amazon RDS para PostgreSQL en modo SSL mediante AWS DMS
- Migre Amazon RDS para Oracle a Amazon RDS para PostgreSQL con AWS SCT y AWS DMS mediante AWS CLI y AWS CloudFormation
- Migre una instancia de base de datos de Amazon RDS a otra VPC o cuenta
- ???
- Migre una instancia de base de datos de Amazon RDS para Oracle a otra VPC
- Migre un clúster de Amazon Redshift a una región de AWS en China
- ???
- Migración de una base de datos de Microsoft SQL Server en las instalaciones a Amazon EC2
- Migración de una base de datos de Microsoft SQL Server en las instalaciones a Amazon RDS para SQL Server
- Migración de bases de datos en las instalaciones de Microsoft SQL Server a Amazon RDS para SQL Server mediante servidores vinculados

- Migre una base de datos de Microsoft SQL Server en las instalaciones a Amazon RDS para SQL Server mediante métodos nativos de copia de seguridad y restauración
- Migre una base de datos de Microsoft SQL Server en las instalaciones a Amazon Redshift mediante AWS DMS
- Migre una base de datos en las instalaciones de Microsoft SQL Server a Amazon Redshift mediante agentes de extracción de datos de AWS SCT
- ???
- Migración de una base de datos MySQL en las instalaciones a Amazon EC2
- Migrar una base de datos MySQL en las instalaciones a Amazon RDS para MySQL
- Migrar de una base de datos de MySQL en las instalaciones a Aurora MySQL
- Migre una base de datos de Oracle en las instalaciones a Amazon EC2 mediante Oracle Data Pump
- Migre una base de datos Oracle local a Amazon OpenSearch Service mediante Logstash
- Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para MySQL con AWS DMS y AWS SCT
- Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle
- Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle mediante Oracle Data Pump
- Migrar una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle mediante Oracle Data Pump
- Migre una base de datos Oracle en las instalaciones a Amazon RDS para PostgreSQL mediante Oracle Bystander y AWS DMS
- Migre una base de datos de Oracle en las instalaciones a Amazon EC2
- Migrar una base de datos PostgreSQL en las instalaciones a Aurora PostgreSQL
- Migración de una base de datos de SAP ASE en las instalaciones a Amazon EC2
- Migre una base de datos ThoughtSpot Falcon local a Amazon Redshift
- Migración de una base de datos Vertica en las instalaciones a Amazon Redshift con los agentes de extracción de datos de AWS SCT
- Migrar una base de datos Oracle de Amazon EC2 a Amazon RDS para MariaDB mediante AWS DMS y AWS SCT
- Migración de una base de datos de Oracle de Amazon EC2 a Amazon RDS para Oracle mediante AWS DMS

- Migrar una base de datos de Oracle a Amazon DynamoDB mediante AWS DMS
- Migre una base de datos Oracle a Amazon RDS for Oracle mediante adaptadores de archivos planos de GoldenGate Oracle
- Migración de una base de datos de Oracle a Amazon Redshift con AWS DMS y AWS SCT
- Migrar una base de datos de Oracle a Aurora PostgreSQL con AWS DMS y AWS SCT
- Migre una EnterpriseOne base de datos de Oracle JD Edwards a AWS mediante Oracle Data Pump y AWS DMS
- Migre una tabla particionada de Oracle a PostgreSQL mediante AWS DMS
- Migre una PeopleSoft base de datos de Oracle a AWS mediante AWS DMS
- Migre datos de una base de datos Oracle en las instalaciones a Aurora PostgreSQL
- Migre datos a la nube de AWS mediante Starburst
- Migre Db2 para LUW a Amazon EC2 mediante envío de registros para reducir el tiempo de interrupción
- Migración de Db2 para LUW a Amazon EC2 con recuperación de desastres de alta disponibilidad
- Migrar de Amazon RDS para Oracle a Amazon RDS para MySQL
- ???
- Migrar de IBM Db2 en Amazon EC2 a compatible con Aurora PostgreSQL mediante AWS DMS y AWS SCT
- Migre de Oracle 8i o 9i a Amazon RDS para PostgreSQL mediante la vista materializada y AWS DMS
- Migre de Oracle 8i o 9i a Amazon RDS para PostgreSQL mediante AWS DMS SharePlex
- Migre de Oracle Database a Amazon RDS for PostgreSQL mediante Oracle GoldenGate
- ???
- Migración de Oracle a Amazon DocumentDB con AWS DMS
- Migre de PostgreSQL en Amazon EC2 a Amazon RDS para PostgreSQL mediante pglogical
- Migración de SAP ASE a Amazon RDS para SQL Server utilizando AWS DMS
- Migre índices basados en funciones de Oracle a PostgreSQL
- Migre aplicaciones heredadas de Oracle Pro*C a ECPG
- Migración de cargas de trabajo de Cloudera en las instalaciones a la plataforma de datos de Cloudera en AWS
- Migre bases de datos MySQL locales a Aurora MySQL mediante Percona, XtraBackup Amazon EFS y Amazon S3

- Migración de Oracle Business Intelligence 12c a la nube de AWS desde servidores en las instalaciones
- Migre valores CLOB de Oracle a filas individuales en PostgreSQL en AWS
- Migre los códigos de error de Oracle Database a una base de datos Amazon Aurora compatible con PostgreSQL
- Migre Oracle E-Business Suite a Amazon RDS Custom
- Migre tablas externas de Oracle a Amazon Aurora compatible con PostgreSQL
- Migrar las funciones nativas de Oracle a PostgreSQL mediante extensiones
- Migre Oracle PeopleSoft a Amazon RDS Custom
- Migre la funcionalidad ROWIdentificador de Oracle a PostgreSQL en AWS
- Migre los paquetes pragma SERIALLY_REUTILIZABLE de Oracle a PostgreSQL
- Migración de las cargas de trabajo de Redis a Redis Enterprise Cloud en AWS
- Migre SAP ASE de Amazon EC2 a Amazon Aurora compatible con PostgreSQL mediante AWS SCT y AWS DMS
- Migre columnas generadas de forma virtual de Oracle a PostgreSQL
- Supervise ElastiCache los clústeres de Amazon para comprobar el cifrado en reposo
- Supervise ElastiCache los clústeres para grupos de seguridad
- Reduzca el tiempo de transición de la migración homogénea de SAP mediante el servicio de migración de aplicaciones
- Rotar las credenciales de la base de datos sin reiniciar los contenedores
- Ejecute cargas de trabajo basadas en mensajes a escala con AWS Fargate
- Configure una PeopleSoft arquitectura de alta disponibilidad en AWS
- ???
- Configure la funcionalidad UTL_FILE de Oracle en Aurora compatible con PostgreSQL
- Transfiera datos de Db2 z/OS a gran escala a Amazon S3 en archivos CSV
- Transportar bases de datos PostgreSQL entre dos instancias de base de datos de Amazon RDS utilizando pg_transport
- Uso CloudEndure para la recuperación ante desastres de una base de datos local
- Validar los objetos de la base de datos después de migrar de Oracle a Amazon Aurora PostgreSQL
- Compruebe que los nuevos clústeres de Amazon Redshift se lanzan en una VPC

DevOps

Temas

- Automatice la evaluación de recursos de AWS
- Instalar sistemas SAP automáticamente mediante herramientas de código abierto
- Automatice la implementación de productos y la cartera de AWS Service Catalog mediante AWS CDK
- Automatice las copias de seguridad basadas en eventos desde CodeCommit Amazon S3 mediante CodeBuild and Events CloudWatch
- Automatice la implementación de conjuntos de pilas mediante AWS CodePipeline y AWS CodeBuild
- Adjunte automáticamente una política administrada de AWS para Systems Manager a los perfiles de instancia de EC2 mediante Cloud Custodian y AWS CDK
- Crear automáticamente canalizaciones de CI/CD y clústeres de Amazon ECS para microservicios mediante AWS CDK
- Cree una arquitectura de acoplamiento flexible con microservicios mediante DevOps prácticas y AWS Cloud9
- Cree e inserte imágenes de Docker en Amazon ECR mediante GitHub Actions y Terraform
- Cree y pruebe aplicaciones iOS con AWS CodeCommit CodePipeline, AWS y AWS Device Farm
- Consulte las aplicaciones o CloudFormation plantillas de CDK de AWS para conocer las prácticas recomendadas mediante los paquetes de reglas de cdk-nag
- Configurar el acceso entre cuentas a Amazon DynamoDB
- Configure autenticación TLS mutua para aplicaciones ejecutadas en Amazon EKS
- Crear un analizador de registros personalizado para Amazon ECS mediante un enrutador de registros Firelens
- Cree una canalización y una AMI con CodePipeline un HashiCorp empaquetador
- Cree una canalización e implemente actualizaciones de artefactos en instancias EC2 locales mediante CodePipeline
- Crear automáticamente canalizaciones de CI dinámicas para proyectos de Java y Python
- Despliega canarios de CloudWatch Synthetics con Terraform
- Implemente una canalización de CI/CD para microservicios de Java en Amazon ECS

- Utilice AWS CodeCommit y AWS CodePipeline para implementar una canalización de CI/CD en varias cuentas de AWS
- Implemente un firewall con AWS Network Firewall y AWS Transit Gateway
- Implemente un trabajo de AWS Glue con una canalización de CodePipeline CI/CD de AWS
- Implementar un clúster de Amazon EKS desde AWS Cloud9 mediante un perfil de instancia de EC2
- Implemente código en varias regiones de AWS mediante AWS CodePipeline CodeCommit, AWS y AWS CodeBuild
- Exportar los informes de AWS Backup de toda la organización en AWS Organizations como un archivo CSV
- Exportación de etiquetas para una lista de instancias de Amazon EC2 a un archivo CSV
- Genere una CloudFormation plantilla de AWS que contenga las reglas administradas por AWS Config mediante Troposphere
- Otorgue a las instancias de SageMaker notebook acceso temporal a un CodeCommit repositorio de otra cuenta de AWS
- Implemente una estrategia GitHub de ramificación de Flow para entornos de cuentas múltiples DevOps
- Implementa una estrategia de ramificación de Gitflow para entornos de múltiples cuentas DevOps
- Implemente una estrategia de ramificación troncal para entornos de cuentas múltiples DevOps
- Detecta automáticamente los cambios e inicia diferentes CodePipeline canalizaciones para un monorepo en CodeCommit
- Integre un repositorio de Bitbucket con AWS Amplify mediante AWS CloudFormation
- Lance un CodeBuild proyecto en todas las cuentas de AWS mediante Step Functions y una función de proxy Lambda
- Gestione las implementaciones azul/verde de microservicios en varias cuentas y regiones mediante los servicios de código de AWS y las claves multirregionales de AWS KMS
- Supervise los repositorios de Amazon ECR en busca de permisos comodín mediante AWS y AWS Config CloudFormation
- Realice acciones personalizadas a partir de CodeCommit eventos de AWS
- Publica CloudWatch las métricas de Amazon en un archivo CSV
- Ejecutar pruebas unitarias para trabajos ETL de Python en AWS Glue con el marco pytest
- Configure un repositorio de gráficos de Helm v3 en Amazon S3

- Configure una canalización de CI/CD mediante AWS y CodePipeline AWS CDK
- Configure el end-to-end cifrado para aplicaciones en Amazon EKS mediante cert-manager y Let's Encrypt
- Simplifique la implementación de aplicaciones multiusuario de Amazon EKS mediante Flux
- Suscriba varios puntos de conexión de correo electrónico a un tema de SNS mediante un recurso personalizado
- Use Serverspec para desarrollar código de infraestructura basado en pruebas
- Utilice repositorios de código fuente de Git de terceros en AWS CodePipeline
- Cree una canalización de CI/CD para validar las configuraciones de Terraform mediante AWS CodePipeline
- Más patrones

Automatice la evaluación de recursos de AWS

Creado por Naveen Suthar (AWS), Arun Bagal (AWS), Manish Garg (AWS) y Sandeep Gawande (AWS)

Repositorio de código: infrastructure-assessment-iac-automation	Entorno: PoC o piloto	Tecnologías: infraestructura DevOps; administración y gobierno; operaciones; sin servidor
Servicios de AWS: Amazon Athena; AWS CloudTrail; AWS Lambda; Amazon S3; Amazon QuickSight		

Resumen

Este patrón describe un enfoque automatizado para configurar las capacidades de evaluación de recursos mediante AWS Cloud Development Kit (AWS CDK). Usando este patrón, los equipos de operaciones recopilan los detalles de auditoría de los recursos de forma automatizada y ven los detalles de todos los recursos implementados en una cuenta de AWS en un único panel. Esto resulta útil en los siguientes casos de uso:

- Identificar las herramientas de infraestructura como código (IaC) y aislar los recursos creados por diferentes soluciones de IaC, como HashiCorp Terraform, AWS CloudFormation, AWS CDK y AWS Command Line Interface (AWS CLI)
- Obtener información de auditoría de recursos

Esta solución también ayuda al equipo directivo a obtener información sobre los recursos y las actividades de una cuenta de AWS desde un único panel.

Nota: Amazon QuickSight es un servicio de pago. Antes de ejecutarlo para analizar los datos y crear un panel de control, revisa los precios de Amazon QuickSight.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Roles y permisos de AWS Identity and Access Management (IAM) con acceso a recursos de aprovisionamiento
- Una QuickSight cuenta de Amazon creada con acceso a Amazon Simple Storage Service (Amazon S3) y Amazon Athena
- Se ha instalado la versión 2.55.1 o posterior de AWS CDK
- Se ha instalado la versión 3.9 o posterior de Python

Limitaciones

- Esta solución se implementa en una única cuenta de AWS.
- La solución no rastreará los eventos que ocurrieron antes de su implementación, a menos que AWS ya CloudTrail estuviera configurado y almacenando datos en un bucket de S3.

Versiones de producto

- CDK de AWS, versión 2.55.1 o posterior
- Python, versión 3.9 o posterior

Arquitectura

Pila de tecnología de destino

- Amazon Athena
- AWS CloudTrail
- AWS Glue
- AWS Lambda
- Amazon QuickSight
- Amazon S3

Arquitectura de destino

El código de AWS CDK implementará todos los recursos necesarios para configurar las capacidades de evaluación de recursos en una cuenta de AWS. En el siguiente diagrama se muestra el proceso de envío de CloudTrail registros a AWS Glue, Amazon Athena y. QuickSight

1. CloudTrail envía los registros a un depósito de S3 para su almacenamiento.
2. Una notificación de evento invoca una función de Lambda que procesa los registros y genera datos filtrados.
3. Los datos filtrados se almacenan en otro bucket de S3.
4. Se configura un rastreador de AWS Glue en los datos filtrados del bucket de S3 para crear un esquema en la tabla del catálogo de datos de AWS Glue.
5. Los datos filtrados están listos para que Amazon Athena los consulte.
6. Se accede a los datos consultados QuickSight para su visualización.

Automatizar y escalar

- Esta solución se puede escalar de una cuenta de AWS a varias cuentas de AWS si existe un registro que abarque a toda la organización en AWS CloudTrail Organizations. CloudTrail Al implementarla a nivel organizacional, también puede usar esta solución para obtener detalles de auditoría de recursos para todos los recursos necesarios.
- Este patrón emplea recursos sin servidor de AWS para implementar la solución.

Herramientas

Servicios de AWS

- Amazon Athena es un servicio de consultas interactivo que facilita el análisis de datos en Amazon S3 con SQL estándar.
- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura de la nube de AWS en código.
- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- AWS le CloudTrail ayuda a auditar la gobernanza, el cumplimiento y el riesgo operativo de su cuenta de AWS.

- AWS Glue es un servicio de extracción, transformación y carga (ETL) completamente administrado. Ayuda a clasificar, limpiar, enriquecer y mover datos de forma fiable entre almacenes de datos y flujos de datos. Este patrón emplea un rastreador de AWS Glue y una tabla del catálogo de datos de AWS Glue.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon QuickSight es un servicio de inteligencia empresarial (BI) a escala de nube que le ayuda a visualizar, analizar y elaborar informes sobre sus datos en un único panel de control.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Repositorio de código

El código de este patrón está disponible en el GitHub infrastructure-assessment-iac-automationrepositorio.

El repositorio de código contiene los siguientes archivos y carpetas:

- Carpeta `lib` – los archivos Python de constructo de AWS CDK usados para crear los recursos de AWS
- `src/lambda_code` – El código Python que se ejecuta en la función de Lambda
- `requirements.txt` – La lista de todas las dependencias de Python que se deben instalar
- `cdk.json` – El archivo de entrada que proporciona los valores necesarios para activar los recursos

Prácticas recomendadas

Configure la supervisión y las alertas para las funciones de Lambda de AWS. Para obtener más información, consulte Supervisión y solución de problemas de funciones de Lambda. Para obtener más información sobre las prácticas recomendadas generales en el uso de funciones de Lambda, consulte la documentación de AWS.

Epics

Configure su entorno

Tarea	Descripción	Habilidades requeridas
Clone el repositorio en su máquina local.	Para clonar el repositorio, ejecute el comando `git clone https://github.com/aws-samples/infrastructure-assessment-iac-automation.git` .	AWS DevOps, DevOps ingeniero
Configure el entorno virtual de Python e instale las dependencias necesarias.	Para configurar y activar el entorno virtual de Python, ejecute el siguiente comando. `cd infrastructure-assessment-iac-automation` `python3 -m venv .venv` `source .venv/bin/activate` Ejecute el comando `pip install -r requirements.txt` para configurar las dependencias necesarias.	AWS DevOps, DevOps ingeniero
Configure el entorno de AWS CDK y sintetice el código de AWS CDK.	1. Para configurar el entorno de AWS CDK en su cuenta de AWS, ejecute el comando `cdk bootstrap aws://ACCOUNT-NUMBER/REGION` . 2. Para convertir el código en una configuración	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	de CloudFormation pila de AWS, ejecute el comando`cdk synth`.	

Configuración de las credenciales de AWS en su máquina local

Tarea	Descripción	Habilidades requeridas
Exporte las variables de cuenta y región en las que se implementará la pila.	Para proporcionar las credenciales de AWS para AWS CDK mediante variables de entorno, ejecute los siguientes comandos. `export CDK_DEFAULT_ACCOUNT=<12 Digit AWS Account Number>` `export CDK_DEFAULT_REGION=<region>`	AWS DevOps, DevOps ingeniero
Configure el perfil de AWS CLI.	Para configurar el perfil de AWS CLI para la cuenta, siga las instrucciones de la documentación de AWS.	AWS DevOps, DevOps ingeniero

Configure e implemente la herramienta de evaluación de recursos

Tarea	Descripción	Habilidades requeridas
Implementar recursos en la cuenta.	Para implementar recursos en la cuenta de AWS mediante AWS CDK, haga lo siguiente: 1. En la raíz del repositorio clonado, en el archivo	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`cdk.json`, introduzca entradas para los siguientes parámetros: • `s3_context` • `ct_context` • `kms_context` • `lambda_context` • `glue_context` • `qs_context` Estos valores definen la nomenclatura y la configuración de los recursos. Los valores predeterminados están establecidos, y se pueden cambiar si es necesario. Nota: Para evitar que aparezca un error que indique que el bucket de S3 ya existe, asegúrese de proporcionar nombres exclusivos para `s3_context` en las secciones `ct` y `output`. 2. Ejecute el `cdk deploy` comando para implementar los recursos. El `cdk deploy` comando crea un CloudTrail recurso para registrar eventos y guardar el archivo de	

Tarea	Descripción	Habilidades requeridas
	registro en el depósito S3 de entrada. La función de Lambda procesa los archivos de registros de la ruta. Los resultados filtrados se almacenan en el depósito S3 de salida y están listos para que Amazon Athena y Amazon los consuman. QuickSight	

Tarea	Descripción	Habilidades requeridas
Ejecute el rastreador de AWS Glue y cree la tabla del catálogo de datos.	El rastreador de AWS Glue se usa para mantener el esquema de datos dinámico. La solución crea y actualiza las particiones en la tabla del catálogo de datos de AWS Glue, ejecutando el rastreador periódicamente según lo definido en el programador de rastreo de AWS Glue. Una vez que los datos estén disponibles en el bucket de S3 de salida, siga estos pasos para ejecutar el rastreador de AWS Glue y crear el esquema de la tabla del catálogo de datos para realizar las pruebas: 1. Inicie sesión en la consola de administración de AWS y vaya a la consola de AWS Glue. 2. En el panel de navegación, en Catálogo de datos, seleccione rastreador. 3. Seleccione el rastreador `iac-tool-qa-resource-iac-json-crawler` . 4. Ejecute el rastreador. 5. Una vez que el rastreador se ejecuta correctamente, crea una tabla de Catálogo de datos de AWS Glue.	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	AWS QuickSight utilizará la tabla para visualizar los datos. Nota: El código de AWS CDK configura el rastreador de AWS Glue para que se ejecute en un momento determinado, pero también puede ejecutarlo bajo demanda.	
Implemente la QuickSight construcción.	1. Para implementar la QuickSight construcción, descomente el código intermedio `#QuickSight setup - start` y interno`#QuickSight setup – ends` . `resource_iac_tool_stack.py` 2. Tras eliminar los comentarios, ejecuta el `cdk deploy` comando para crear `QuickSight DataSource` y `QuickSight DataSet` en la QuickSight cuenta.	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Crea el QuickSight panel de control.	Para crear el QuickSight panel y el análisis de ejemplo, haga lo siguiente: 1. Navegue a la QuickSigh t consola y seleccione la región de AWS en la que se implementan los recursos. 2. En el panel de navegación, elija Conjuntos de datos y valide que se `ct-operat ions-iac-ds` haya creado un conjunto de datos denominado en el QuickSight conjunto de datos de Amazon. Si no ve el conjunto de datos, vuelva a implementar la construcción. QuickSight 3. Seleccione el conjunto de datos `ct-operations-iac-ds` y elija USAR EN ANÁLISIS. 4. Seleccione la hoja predeterminada. 5. Seleccione las columnas correspondientes de la lista de campos de la izquierda. 6. Tras seleccionar las columnas necesarias, seleccione el tipo de visualización adecuado para los datos.	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Para obtener más información, consulte Iniciar un análisis en Amazon QuickSight y Tipos visuales en Amazon QuickSight.	

Limpie todos los recursos de AWS de la solución

Tarea	Descripción	Habilidades requeridas
Elimine los recursos de AWS.	1. Para eliminar los recursos de AWS implementados por la solución, ejecute el comando `cdk destroy`. 2. Elimine todos los objetos de los dos buckets de S3 y, a continuación, elimine los buckets. Para obtener más información, consulte Eliminación de un bucket.	AWS DevOps, DevOps ingeniero

Configure funciones adicionales además de la automatización de la herramienta de evaluación de recursos de AWS

Tarea	Descripción	Habilidades requeridas
Supervise y limpie los recursos creados manualmente.	(Opcional) Si su organización tiene requisitos de conformidad para crear recursos con las herramientas de IaC, puede satisfacerlos automatizando las herramientas de evaluació	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	n de recursos de AWS para obtener los recursos aprovisionados manualmente. También puede usar la herramienta para importar los recursos a una herramienta de IaC o volver a crearlos. Realice las siguientes tareas de alto nivel para supervisar los recursos aprovisionados de manera manual: 1. Implemente la automatización de la herramienta de evaluación de recursos de AWS. 2. Configure una función de Lambda para consultar las tablas de Athena a diario, buscar los datos relevantes sobre los recursos aprovisionados manualmente y exportarlos a un archivo de valores separados por comas (CSV). 3. Una vez ejecutada la función de Lambda, puede enviar una notificación con los datos necesarios a las respectivas partes interesadas. 4. El archivo .csv se puede almacenar en el bucket	

Tarea	Descripción	Habilidades requeridas
	de S3 para prolongar su retención. 5. En función de la informaci ón del archivo .csv, elimine los recursos creados manualmente o impórtelo s a una solución IaC existente.	

Solución de problemas

Problema	Solución
AWS CDK devuelve errores.	Para obtener ayuda con los errores de AWS CDK, consulte Solución de problemas comunes de AWS CDK.

Recursos relacionados

- Creación de funciones de Lambda con Python
- Introducción a AWS CDK
- Utilización de AWS CDK en Python
- Creando un CloudTrail registro
- Empieza con Amazon QuickSight

Información adicional

Cuentas múltiples

Para configurar la credencial de AWS CLI para múltiples cuentas, use los perfiles de AWS. Para obtener más información, consulte la sección Configurar varios perfiles en Configurar AWS CLI.

Comandos de AWS CDK

Cuando trabaje con AWS CDK, recuerde los siguientes comandos útiles:

- Muestra todas las pilas de la aplicación

```
cdk ls
```

- Emite la plantilla de AWS CloudFormation sintetizada

```
cdk synth
```

- Implementa la pila en la cuenta y región de AWS predeterminadas

```
cdk deploy
```

- Compara la pila implementada con el estado actual

```
cdk diff
```

- Abre la documentación de AWS CDK

```
cdk docs
```

Instalar sistemas SAP automáticamente mediante herramientas de código abierto

Creado por Guilherme Sesterheim (AWS)

Repositorio de código: repositorio principal	Entorno: producción	Tecnologías: DevOps
Carga de trabajo: SAP	Servicios de AWS: Amazon EC2; Amazon S3	

Resumen

Este patrón muestra cómo automatizar la instalación de sistemas SAP mediante el uso de herramientas de código abierto para crear los recursos siguientes:

- Una base de datos SAP S/4HANA 1909
- Una instancia de SAP ABAP Central Services (ASCS)
- Una instancia de servidor principal de aplicaciones (PAS) de SAP

HashiCorp Terraform crea la infraestructura del sistema SAP y Ansible configura el sistema operativo (SO) e instala las aplicaciones SAP. Jenkins ejecuta la instalación.

Con esta configuración, la instalación de sistemas SAP se convierte en un proceso repetible, lo que puede ayudar a aumentar la eficiencia y la calidad de la implementación.

Nota: El código de ejemplo que se proporciona en este patrón funciona tanto para sistemas de alta disponibilidad (HA) como para sistemas que no lo son.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un bucket de Amazon Simple Storage Service (Amazon S3) que contenga todos sus archivos multimedia de SAP

- Una entidad principal de Identity and Access Management (IAM) de AWS con una clave de acceso y una clave secreta y con los siguientes permisos:
  - Permisos de solo lectura: Amazon Route 53, AWS Key Management Service (AWS KMS)
  - Permisos de lectura y escritura: Amazon S3, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic File System (Amazon EFS), IAM, Amazon, Amazon DynamoDB CloudWatch
- Una zona alojada privada de Route 53
- Una suscripción a Red Hat Enterprise Linux para SAP con Imagen de máquina de Amazon (AMI) de alta disponibilidad y Update Services 8.2 en Amazon Marketplace
- Una clave gestionada de cliente de AWS KMS
- Un par de claves Secure Shell (SSH)
- Un grupo de seguridad de Amazon EC2 que permita la conexión SSH en el puerto 22 desde el nombre de host donde se instala Jenkins (lo más probable es que el nombre de host sea localhost)
- Vagrant by instalado y configurado HashiCorp
- VirtualBoxinstalado y configurado por Oracle
- Familiaridad con Git, Terraform, Ansible y Jenkins

Limitaciones

- Solamente SAP S/4HANA 1909 se ha probado completamente para este escenario específico. El código de Ansible de ejemplo de este patrón requiere modificaciones si utiliza otra versión de SAP HANA.
- El procedimiento de ejemplo de este patrón funciona para los sistemas operativos Mac y Linux. Algunos de los comandos solo se pueden ejecutar en terminales basados en Unix. Sin embargo, puede lograr un resultado similar utilizando diferentes comandos y un sistema operativo Windows.

Versiones de producto

- SAP S/4HANA 1909
- Red Hat Enterprise Linux (RHEL) versión 8.2 o posterior

Arquitectura

El diagrama siguiente muestra un ejemplo de flujo de trabajo que utiliza herramientas de código abierto para automatizar la instalación de sistemas SAP en una cuenta de AWS:

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Jenkins orquesta la instalación del sistema SAP mediante la ejecución del código de Terraform y Ansible.
2. El código de Terraform crea la infraestructura del sistema SAP.
3. El código de Ansible configura el sistema operativo e instala las aplicaciones SAP.
4. En una instancia de Amazon EC2 se instalan una base de datos SAP S/4HANA 1909, una instancia de ASCS y una instancia de PAS que incluyen todos los requisitos previos definidos.

Nota: El ejemplo de configuración de este patrón crea automáticamente un bucket de Amazon S3 en su cuenta AWS para almacenar el archivo de estado de Terraform.

Pila de tecnología

- Terraform
- Ansible
- Jenkins
- Una base de datos SAP S/4HANA 1909
- Una instancia de SAP ASCS
- Una instancia de SAP PAS
- Amazon EC2

Herramientas

Servicios de AWS

- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Key Management Service (AWS KMS) le ayuda a crear y controlar claves criptográficas para proteger sus datos.

- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esta red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Otras herramientas

- HashiCorp Terraform es una aplicación de interfaz de línea de comandos que le ayuda a usar el código para aprovisionar y administrar la infraestructura y los recursos de la nube.
- Ansible es una herramienta de código abierto de configuración como código (CaC) que ayuda a automatizar las aplicaciones, las configuraciones y la infraestructura de TI.
- Jenkins es un servidor de código abierto de automatización que permite a los desarrolladores crear, probar e implementar su software.

Código

El código de este patrón está disponible en el repositorio -jenkins-ansible. GitHub aws-install-sap-with

Epics

Configurar los requisitos previos

Tarea	Descripción	Habilidades requeridas
Añada sus archivos multimedia SAP a un bucket de Amazon S3.	Cree un bucket de Amazon S3 que contenga todos sus archivos multimedia SAP. Importante: Asegúrese de seguir la jerarquía de carpetas de AWS Launch Wizard para S/4HANA en la documentación de Launch Wizard.	Administrador de la nube
Instalar. VirtualBox	Instalación y configuración VirtualBoxpor parte de Oracle.	DevOps ingeniero
Instalar Vagrant.	Instale y configure Vagrant mediante. HashiCorp	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Configurar su cuenta de AWS.	1. Compruebe que tiene una entidad principal de IAM con una clave de acceso y una clave secreta, y que tiene los permisos siguientes: • Permisos de solo lectura: Amazon Route 53, AWS Key Management Service (AWS KMS) • Permisos de lectura y escritura: Amazon S3, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic File System (Amazon EFS), IAM, Amazon, Amazon DynamoDB CloudWatch 2. Guarde la clave de acceso y la clave secreta de la entidad principal de IAM para consultarlas más adelante. 3. Cree una zona alojada privada de Route 53, si aún no la tiene. Guarde el nombre de la zona (por ejemplo, sapteam.net) para consultarlo más adelante. 4. Suscríbase a Red Hat Enterprise Linux para SAP con AMI de alta disponibilidad y Update Services 8.2	AWS general

Tarea	Descripción	Habilidades requeridas
	en Amazon Marketplace. Guarde el ID de AMI (por ejemplo, ami-0000000) para consultarlo más adelante. 5. Cree una clave gestionada de cliente de AWS KMS. Guarde el nombre de recurso de Amazon (ARN) de la clave de cifrado para consultarlo más adelante. Nota: A continuación se muestra un ejemplo de ARN de clave gestionada de cliente de AWS KMS: arn:aws:kms:us-east-1:123412341234:key/uuid 6. Cree un par de claves SSH. Guarde el nombre del par de claves y el archivo .pem para consultarlos más adelante. 7. Cree un grupo de seguridad de Amazon EC2 que permita la conexión SSH en el puerto 22 desde el nombre de host donde se instala Jenkins. Guarde el ID del grupo de seguridad para consultarlo más adelante.	

Tarea	Descripción	Habilidades requeridas
	Nota: Lo más probable es que el nombre de host sea localhost.	

Crear y ejecutar su instalación de SAP

Tarea	Descripción	Habilidades requeridas
Clona el repositorio de código desde. GitHub	Clona el repositorio aws-install-sap-with-jenkins-ansible en. GitHub	DevOps ingeniero
Inicie el servicio de Jenkins.	Abra la terminal de Linux. A continuación, navegue hasta la carpeta local que contiene la carpeta del repositorio de código clonado y ejecute el comando siguiente: `sudo vagrant up` Nota: Jenkins tarda unos 20 minutos en iniciarse. El comando devuelve el mensaje Service is up and running (El servicio está funcionando) cuando el funcionamiento es correcto.	DevOps ingeniero
Abra Jenkins en un navegador web e inicie sesión.	1. En un navegador web, escriba http://localhost:5555. Se abrirá Jenkins. 2. Inicie sesión en Jenkins usando admin como	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	nombre de usuario y my_secret_pass_from_vault como contraseña.	

Tarea	Descripción	Habilidades requeridas
Configure los parámetros de instalación de su sistema SAP.	1. En Jenkins, seleccione Manage Jenkins (Administrar Jenkins). A continuación, seleccione Manage Credentials (Administrar credenciales). Se muestra una lista de variables de credenciales que puede configurar. 2. Configure todas las variables de credenciales siguientes: • Para AWS_ACCOUNT_CREDENTIALS, escriba el ID de clave de acceso y el ID de clave de acceso secreta de su entidad principal de IAM. • Para AMI_ID, escriba el ID de AMI de Red Hat Enterprise Linux para SAP con el ID de AMI del AMI alta disponibilidad y Update Services 8.2. • Para KMS_KEY_ARN, escriba el ARN de la clave gestionada de cliente de AWS KMS. • Para SSH_KEYPAIR_NAME, escriba el nombre del par de claves	Administrador de sistemas de AWS, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	SSH, sin el tipo de archivo .pem. • Para SSH_KEYPAIR_FILE, escriba el nombre completo del archivo .pem del par de claves (por ejemplo, mykeypair.pem). Asegúrese de cargar también el archivo .pem de los pares de claves en Jenkins. • Para S3_ROOT_FOLDER_INSTALL_FILES, introduzca el nombre del depósito de Amazon S3 y de la carpeta, si procede, (por ejemplo, s3:///S4H1909) que contiene los archivos multimedia de SAP. my-media-bucket • Para PRIVATE_DNS_ZONE_NAME, escriba el nombre de su zona alojada privada de Route 53 (por ejemplo, myprivatecompanyurl.net). • Para VPC_ID, escriba el ID de VPC (por ejemplo, vpc-12345) de la VPC de Amazon en la que va a crear los recursos de SAP. • Para SUBNET_IDS, escriba dos ID de subred públicas si trabaja en un entorno de prueba (para	

Tarea	Descripción	Habilidades requeridas
	futuras capacidades de alta disponibilidad). Si trabaja en un entorno de producción, se recomienda utilizar dos subredes privadas con un host bastión. • Para SECURITY_ GROUP_ID, escriba el ID del grupo de seguridad de Amazon EC2 que permite la conexión SSH en el puerto 22 desde el nombre de host en el que instaló Jenkins. Nota: Puede configura r los demás parámetros no obligatorios según sea necesario, en función de su caso de uso. Así, por ejemplo, puede cambiar el ID del sistema SAP (SID) de las instancias, la contraseña predeterminada, los nombres y las etiquetas del sistema SAP. Todas las variables obligatorias muestran Required (Obligatoria) al principio de sus nombres.	

Tarea	Descripción	Habilidades requeridas
Ejecute la instalación de su sistema SAP.	1. En Jenkins, seleccione Jenkins Home. A continuación, seleccione 3 instancias de SAP Hana+ASCS+PAS. 2. Seleccione Spin up and install (Poner en marcha e instalar). A continuación, seleccione Main (Principal). 3. Seleccione Build now (Crear ahora). Para obtener información sobre los pasos del proceso, consulte la sección Understanding the pipeline steps (Comprender los pasos del proceso) de Automating SAP installation with open-source tools (Automatizar la instalación de SAP con herramientas de código abierto) en el blog de AWS. Nota: Si se produce un error, mueva el cursor sobre el cuadro de error rojo que aparece y seleccione Logs (Registros). Aparecen los registros del paso del proceso en el que se produjo el error. La mayoría de los errores se producen debido a una configuración de parámetros incorrecta.	DevOps ingeniero, administrador de sistemas de AWS

Recursos relacionados

- DevOps para SAP: instalación de SAP: de 2 meses a 2 horas (videoteca de DevOps Enterprise Summit)

Automatice la implementación de productos y la cartera de AWS Service Catalog mediante AWS CDK

Creado por Sandeep Gawande (AWS), RAJNEESH TYAGI (AWS) y Viyoma Sachdeva (AWS)

Repositorio de código: aws-cdk-servicecatalog-automation	Entorno: PoC o piloto	Tecnologías: infraestructura DevOps, gestión y gobierno
Carga de trabajo: código abierto	Servicios de AWS: AWS Service Catalog; AWS CDK	

Resumen

AWS Service Catalog le ayuda a administrar de forma centralizada los catálogos de servicios de TI o productos aprobados para su uso en el entorno de AWS de su organización. La cartera es una colección de productos que, además, contiene información de configuración. Con AWS Service Catalog, puede crear una cartera de productos personalizada para cada tipo de usuario de su organización y conceder acceso a la cartera de productos apropiada. Después, esos usuarios pueden implementar rápidamente cualquier producto que necesiten de la cartera.

Si tiene una infraestructura de red compleja, como arquitecturas en múltiples regiones y cuentas, se recomienda crear y administrar las carteras de Service Catalog en una única cuenta centralizada. Este patrón describe cómo usar AWS Cloud Development Kit (AWS CDK) para automatizar la creación de carteras de Service Catalog en una cuenta central, conceder a los usuarios finales acceso a ellas y, opcionalmente, aprovisionar productos en una o más cuentas de AWS de destino. Esta ready-to-use solución crea las carteras de Service Catalog en la cuenta de origen. También, de forma opcional, aprovisiona los productos en las cuentas de destino mediante AWS CloudFormation stacks y le ayuda a TagOptions configurarlos:

- AWS CloudFormation StackSets: puede utilizarlos StackSets para lanzar productos de Service Catalog en varias regiones y cuentas de AWS. La implementación de esta solución le permite aprovisionar productos automáticamente. Para obtener más información, consulte Uso de AWS CloudFormation StackSets (documentación de Service Catalog) y StackSets conceptos (CloudFormation documentación).
- TagOption biblioteca: puede administrar las etiquetas de los productos aprovisionados mediante la TagOption biblioteca. A TagOptiones un par clave-valor administrado en AWS Service Catalog.

No es una etiqueta de AWS, pero sirve como plantilla para crear una etiqueta de AWS basada en TagOption. Para obtener más información, consulte la TagOption biblioteca (documentación de Service Catalog).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa que quiera usar como cuenta de supervisión para administrar carteras de Service Catalog.
- Si usa esta solución para aprovisionar productos en una o más cuentas de destino, la cuenta de destino debe existir ya y estar activa.
- Permisos de AWS Identity and Access Management (IAM) para acceder a AWS Service Catalog CloudFormation, AWS y AWS IAM.

Versiones de producto

- AWS CDK versión 2.27.0

Arquitectura

Pila de tecnología de destino

- Carteras de Service Catalog en una cuenta de AWS centralizada
- Productos de Service Catalog implementados en la cuenta de destino

Arquitectura de destino

1. En la cuenta de cartera (u origen), debe actualizar el archivo config.json con la información de la cuenta de AWS, la región de AWS, el rol de IAM, la cartera y el producto para su caso de uso.
2. Implemente la aplicación AWS CDK.
3. La aplicación AWS CDK asume el rol de IAM de implementación y crea las carteras y los productos de Service Catalog definidos en el archivo config.json.

Si ha configurado StackSets la implementación de productos en una cuenta de destino, el proceso continúa. Si no lo configuraste StackSets para aprovisionar ningún producto, el proceso se ha completado.

4. La aplicación AWS CDK asume la función de StackSet administrador e implementa el conjunto de CloudFormation pilas de AWS que definió en el archivo config.json.
5. En la cuenta de destino, StackSets asume la función de StackSet ejecución y aprovisiona los productos.

Herramientas

Servicios de AWS

- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura de la nube de AWS en código.
- El Kit de herramientas de AWS CDK es un kit de desarrollo en la nube de línea de comandos que le ayuda a interactuar con su aplicación AWS CDK.
- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Service Catalog le ayuda a administrar de forma centralizada los catálogos de servicios de TI aprobados para AWS. Los usuarios finales pueden implementar rápidamente solo los servicios de TI aprobados que necesitan, de acuerdo con las limitaciones establecidas por su organización.

Repositorio de código

El código de este patrón está disponible en GitHub, en el aws-cdk-servicecatalog-automationrepositorio. El repositorio de código contiene los siguientes archivos y carpetas:

- cdk-sevicecatalog-app— Esta carpeta contiene la aplicación AWS CDK para esta solución.
- config: esta carpeta contiene el archivo config.json y la CloudFormation plantilla para implementar los productos de la cartera de Service Catalog.
- config/config.json: este archivo contiene toda la información de configuración. Actualice este archivo para personalizar esta solución según su caso de uso.

- config/templates: esta carpeta contiene las CloudFormation plantillas de los productos de Service Center.
- setup.sh: este script implementa la solución.
- uninstall.sh: este script elimina la pila y todos los recursos de AWS creados al implementar esta solución.

Para usar el código de muestra, siga las instrucciones en sección Epics.

Prácticas recomendadas

- Los roles de IAM usados para implementar esta solución deben cumplir con el principio de privilegio mínimo (documentación de IAM).
- Respete las Prácticas recomendadas para desarrollar aplicaciones en la nube con AWS CDK (publicación del blog de AWS).
- Siga las prácticas CloudFormation recomendadas de AWS (CloudFormation documentación).

Epics

Configure su entorno

Tarea	Descripción	Habilidades requeridas
Instale el kit de herramientas de AWS CDK.	Asegúrese de tener instalado el kit de herramientas de AWS CDK. Ejecute el siguiente comando para confirmar si está instalado y verifique la versión. `cdk --version` Si el kit de herramientas de AWS CDK no está instalado, ejecute el siguiente comando para instalarlo.	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`npm install -g aws-cdk@2.27.0` Si la versión del kit de herramientas de AWS CDK es anterior a la 2.27.0, ejecute el siguiente comando para actualizarla a la versión 2.27.0. `npm install -g aws-cdk@2.27.0 --force`	

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Escriba el siguiente comando. En Clonar el repositorio, en la sección Información adicional, puede copiar el comando completo que contiene la URL del repositorio. Esto clona el aws-cdk-servicecatalog-automationrepositorio desde GitHub. `git clone <repository-URL>.git` Se creará la carpeta `cd aws-cdk-servicecatalog-automation` en el directorio de destino. Ejecute el siguiente comando para navegar a esta carpeta. `cd aws-cdk-servicecatalog-automation`	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Configure las credenciales de AWS.	Introduzca los comandos siguientes. Se exportan las siguientes variables, que definen la cuenta y la región de AWS en las que se va a implementar la pila. `export CDK_DEFAU LT_ACCOUNT=<12-digit AWS account number>` `export CDK_DEFAU LT_REGION=<AWS Region>` Las credenciales de AWS para AWS CDK se proporcio nan a través de variables de entorno.	AWS DevOps, DevOps ingeniero
Configurar permisos de roles de IAM para usuarios finales.	Si va a usar roles de IAM para conceder acceso a la cartera y a los productos que contiene, estos roles deben tener permisos para que los asuma la entidad principal servicecatalog.amazonaws.com. Para obtener instrucciones sobre cómo conceder estos permisos, consulte Habilitar acceso de confianza con Service Catalog (document ación de AWS Organizations).	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Configure las funciones de IAM requeridas por StackSets.	Si va StackSets a aprovisionar automáticamente los productos en las cuentas de destino, debe configurar las funciones de IAM que administran y ejecutan el conjunto apilado. 1. En la cuenta de origen, confirme que ya existe `AWSCloudFormationStackSetAdministrationRole` . En la cuenta de destino, confirme que ya existe `AWSCloudFormationStackSetExecutionRole` . Si estos roles ya existen, puede pasar a la siguiente épica. 2. Siga las instrucciones de Conceder permisos autogestionados (documentación de IAM) para crear el rol de administración de conjunto de pilas en la cuenta de cartera y crear el rol de ejecución en cada cuenta de destino.	AWS DevOps, DevOps ingeniero

Personalice e implemente la solución

Tarea	Descripción	Habilidades requeridas
Crea las CloudFormation plantillas.	En la `config/templates` carpeta, crea CloudForm ation plantillas para cualquier producto que desees incluir en tus carteras. Para obtener más información, consulte Trabajar con CloudFormation plantillas de AWS (CloudFor mation documentación).	Desarrollador de aplicacio nes, AWS DevOps, DevOps ingeniero
Personalice el archivo de configuración.	En la carpeta `config`, abra el archivo config.json y defina los parámetros según correspon da a su caso de uso. Los siguientes parámetros son obligatorios a menos que se indique lo contrario: • En la sección `portfolio s` , defina los siguientes parámetros para crear una o más carteras de Service Catalog: • `portfolioName` : El nombre de la cartera. • `providerName` : El nombre de la persona, equipo u organización que administra la cartera. • `description` : Descripción breve de la cartera.	Desarrollador de aplicacio nes, DevOps ingeniero, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	• `roles`: (Opcional) Nombres de rol de IAM que deban tener acceso a esta cartera. Los usuarios con este rol pueden acceder a los productos de esta cartera. • `users`: (Opcional) Nombres de todos los usuarios de IAM que deban tener acceso a esta cartera y sus productos. • `groups`: (Opcional) Nombres de cualquier grupo de usuarios de IAM que deban tener acceso a esta cartera y sus productos. Advertencia: los usuarios de IAM tienen credenciales de larga data, lo que supone un riesgo para la seguridad . Para ayudar a mitigar este riesgo, le recomendamos que brinde a estos usuarios únicamente los permisos que necesitan para realizar la tarea y que los elimine cuando ya no los necesiten. Importante: `roles`, `users` y `groups` son todos parámetros opcionales, pero	

Tarea	Descripción	Habilidades requeridas
	si no define uno de ellos, nadie podrá ver la cartera de productos en la consola de Service Catalog. Defina al menos uno de estos parámetros. Para obtener más información, consulte Conceder permisos a los usuarios finales de Service Catalog (documentación de Service Catalog). • (Opcional) En la `tagOption` sección, defina TagOptions para los productos: • `key`— Nombre de la TagOption clave • `value`— Valores de cadena permitidos para TagOption Para obtener más información, consulte la TagOption biblioteca (documentación de Service Catalog). • En la sección `products`, defina los siguientes parámetros para los productos: • `portfolioName` – Nombre de la cartera a la que se agregará el producto. Puede especificar solo una cartera.	

Tarea	Descripción	Habilidades requeridas
	• `productName` : El nombre del producto. • `owner`: El propietario del producto. • `productVersionName` : Nombre de la versión del producto en un valor de cadena, por ejemplo `v1`. • `templatePath` — La ruta del archivo de la CloudFormation plantilla del producto. • `deployWithStackSets` — (Opcional) Especifique una o más cuentas y regiones en las que desee StackSets aprovisionar automáticamente los productos de las carteras. Si usa esta opción de implementación, es obligatorio introducir todos los parámetros de esta sección: • `accounts`: Las cuentas de destino. • `regions`: Las regiones de destino. • `stackSetAdministrationRoleName` —	

Tarea	Descripción	Habilidades requeridas
	El nombre de la función de IAM utilizada para administrar la StackSets configuración. No cambie este valor. El rol debe tener este nombre exacto. • `stackSetExecutionRoleName` : El nombre del rol de IAM en la cuenta de destino que implementa las instancias de la pila. No cambie este valor. El rol debe tener este nombre exacto. Para ver un ejemplo de un archivo de configuración completo, consulte el Ejemplo de archivo de configuración en la sección Información adicional.	
Implemente la solución.	Escriba el siguiente comando. Esto implementa la aplicación AWS CDK y aprovisiona las carteras y productos de Service Catalog, tal y como se especifica en el archivo config.json. `sh +x setup.sh`	Desarrollador de aplicaciones, DevOps ingeniero, AWS DevOps

Tarea	Descripción	Habilidades requeridas
Comprobar la implementación.	Compruebe que la implementación se ha realizado correctamente de la siguiente manera: 1. Inicie sesión en la consola de administración de AWS con credenciales que puedan acceder a una o más de las carteras que definió en el archivo de configuración. 2. Abra la consola de Service Catalog en https://console.aws.amazon.com/servicecatalog/. 3. En el panel de navegación, en Aprovisionamiento, elija Productos. Compruebe que ve una lista de los productos que especificó para la cartera. 4. Siga las instrucciones de Lanzamiento de un producto (documentación de Service Catalog) para lanzar uno de los productos disponibles. Confirme que las versiones y etiquetas de los productos disponibles coincidan con los valores que proporcionó en el archivo de configuración.	AWS general

Tarea	Descripción	Habilidades requeridas
	5. Si opta por aprovisionar automáticamente los productos en una o más cuentas de destino mediante el uso StackSets, haga lo siguiente: a. Inicie sesión con credenciales que le otorguen permisos para ver los productos aprovisionados en una de las cuentas de destino. b. En la consola de Service Catalog, en el panel de navegación, en Aprovisionamiento, seleccione Productos aprovisionados. c. Confirme que los productos esperados aparecen en la lista.	

Tarea	Descripción	Habilidades requeridas
(Opcional) Actualice las carteras y los productos.	Si desea usar esta solución para actualizar las carteras o los productos, o para aprovisionar nuevos productos: 1. Realice los cambios necesarios en el archivo config.json. 2. Añada o modifique CloudFormation las plantillas que necesite en la `config/template` carpeta. 3. Implementar la solución. Por ejemplo, puede añadir carteras adicionales o aprovisionar más recursos. La aplicación AWS CDK implementará solo los cambios. Si no hay cambios en las carteras o los productos implementados anteriormente, la reimplementación no les afectará.	Desarrollador de aplicaciones, DevOps ingeniero, AWS general

Elimine la solución

Tarea	Descripción	Habilidades requeridas
(Opcional) Elimine los recursos de AWS implementados por esta solución.	Si desea eliminar un producto aprovisionado, siga las instrucciones de Eliminar	AWS DevOps, DevOps ingeniero, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	productos aprovisionados (documentación de Service Catalog). Si desea eliminar todos los recursos creados por esta solución, ejecute el siguiente comando. `sh uninstall.sh`	

Recursos relacionados

- Biblioteca de constructos de AWS Service Catalog (referencia de API de AWS)
- StackSets conceptos (CloudFormation documentación)
- AWS Service Catalog (marketing de AWS)
- Uso de Service Catalog con AWS CDK (taller de AWS)

Información adicional

Información adicional

Clone el repositorio

Introduzca el siguiente comando desde el que desea clonar el repositorio GitHub.

```
git clone https://github.com/aws-samples/aws-cdk-servicecatalog-automation.git
```

Ejemplo de archivo de configuración

El siguiente es un archivo de muestra config.json con valores de ejemplo.

```
{
    "portfolios": [
        {
            "displayName": "EC2 Product Portfolio",
```

```
            "providerName": "User1",
            "description": "Test1",
            "roles": [
                "<Names of IAM roles that can access the products>"
            ],
            "users": [
                "<Names of IAM users who can access the products>"
            ],
            "groups": [
                "<Names of IAM user groups that can access the products>"
            ]
        },
        {
            "displayName": "Autoscaling Product Portfolio",
            "providerName": "User2",
            "description": "Test2",
            "roles": [
                "<Name of IAM role>"
            ]
        }
    ],
    "tagOption": [
        {
            "key": "Group",
            "value": [
                "finance",
                "engineering",
                "marketing",
                "research"
            ]
        },
        {
            "key": "CostCenter",
            "value": [
                "01",
                "02",
                "03",
                "04"
            ]
        },
        {
            "key": "Environment",
            "value": [
                "dev",
```

```
                "prod",
                "stage"
            ]
        }
    ],
    "products": [
        {
            "portfolioName": "EC2 Product Profile",
            "productName": "Ec2",
            "owner": "owner1",
            "productVersionName": "v1",
            "templatePath": "../../config/templates/template1.json"
        },
        {
            "portfolioName": "Autoscaling Product Profile",
            "productName": "autoscaling",
            "owner": "owner1",
            "productVersionName": "v1",
            "templatePath": "../../config/templates/template2.json",
            "deployWithStackSets": {
                "accounts": [
                    "012345678901",
                ],
                "regions": [
                    "us-west-2"
                ],
                "stackSetAdministrationRoleName":
 "AWSCloudFormationStackSetAdministrationRole",
                "stackSetExecutionRoleName": "AWSCloudFormationStackSetExecutionRole"
            }
        }
    ]
}
```

Automatice las copias de seguridad basadas en eventos desde CodeCommit Amazon S3 mediante CodeBuild and Events CloudWatch

Documento creado por Kirankumar Chandrashekar (AWS)

Entorno: producción	Tecnologías: DevOps almacenamiento y respaldo	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon S3; Amazon CloudWatch; AWS CodeBuild; AWS CodeCommit		

Resumen

En la nube de Amazon Web Services (AWS), puede utilizar AWS CodeCommit para alojar repositorios seguros basados en Git. CodeCommit es un servicio de control de código fuente totalmente gestionado. Sin embargo, si un CodeCommit repositorio se elimina accidentalmente, su contenido también se elimina y no se puede restaurar.

Este patrón describe cómo realizar automáticamente una copia de seguridad de un CodeCommit repositorio en un bucket de Amazon Simple Storage Service (Amazon S3) después de realizar un cambio en el repositorio. Si el CodeCommit repositorio se elimina posteriormente, esta estrategia de copia de seguridad le ofrece una opción point-in-time de recuperación.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Un CodeCommit repositorio existente, con el acceso de los usuarios configurado de acuerdo con sus requisitos. Para obtener más información, consulte Configuración de AWS CodeCommit en la CodeCommit documentación.
- Un bucket de S3 para cargar las CodeCommit copias de seguridad.

Limitaciones

- Este patrón hace copias de seguridad automáticas de todos sus CodeCommit repositorios. Si quieres hacer copias de seguridad de CodeCommit repositorios individuales, debes modificar la regla de Amazon CloudWatch Events.

Arquitectura

En el siguiente diagrama, se ilustra el flujo de trabajo de este patrón.

El flujo de trabajo consta de los pasos siguientes:

1. El código se envía a un CodeCommit repositorio.
2. El CodeCommit repositorio notifica a CloudWatch Events cualquier cambio en el repositorio (por ejemplo, un `git push` comando).
3. CloudWatch Events invoca a AWS CodeBuild y le envía la información del CodeCommit repositorio.
4. CodeBuild clona todo el CodeCommit repositorio y lo empaqueta en un archivo.zip.
5. CodeBuild carga el archivo.zip en un bucket de S3.

Pila de tecnología

- CloudWatch Eventos
- CodeBuild
- CodeCommit
- Amazon S3

Herramientas

- Amazon CloudWatch Events — CloudWatch Events ofrece una transmisión casi en tiempo real de los eventos del sistema que describen los cambios en los recursos de AWS.

- AWS CodeBuild: CodeBuild es un servicio de integración continua totalmente gestionado que compila el código fuente, ejecuta pruebas y produce paquetes de software listos para su implementación.

- AWS CodeCommit: CodeCommit es un servicio de control de código fuente totalmente gestionado que aloja repositorios seguros basados en Git.
- AWS Identity and Access Management (IAM): IAM es un servicio web que le ayuda a controlar de forma segura el acceso a los recursos de AWS.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet.

Epics

Crea un proyecto CodeBuild

Tarea	Descripción	Habilidades requeridas
Crea un rol CodeBuild de servicio.	Inicie sesión en la consola de administración de AWS y abra la consola de IAM. Elija Roles y después Create Role (Crear rol). Cree un rol de servicio CodeBuild para clonar el CodeCommit repositorio, cargar archivos al bucket de S3 y enviar los registros a Amazon CloudWatch. Para obtener más informaci ón, consulte Crear un rol CodeBuild de servicio en la CodeBuild documentación.	Administrador de la nube
Cree un CodeBuild proyecto.	En la CodeBuild consola, selecciona Crear CodeBuild proyecto. Cree un CodeBuild proyecto mediante la	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	`buildspec.yml` plantilla de la sección Información adicional. Para obtener ayuda con esta historia, consulte Crear un proyecto de compilación en la CodeBuild documentación.	

Cree y configure la regla de CloudWatch eventos

Tarea	Descripción	Habilidades requeridas
Cree un rol de IAM para los CloudWatch eventos.	En la consola de IAM, elija Funciones y cree una función de IAM para los eventos. CloudWatch Para obtener más información al respecto, consulte la función de IAM de CloudWatch eventos en la documentación de IAM. Importante: Debe añadir `codebuild:StartBuild` permisos al rol de IAM para eventos. CloudWatch	Administrador de la nube
Cree una regla de CloudWatch eventos.	1. En la CloudWatch consola, selecciona Eventos y, a continuación, elige Reglas. Elija Crear regla y utilice la regla CloudWatch Eventos de la sección Información adicional. Esto crea una regla que detecta los cambios de eventos (por	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	ejemplo, `git push` o `git commit` los comandos) en sus CodeCommit repositorios. Para obtener más información, consulte Crear una regla de CloudWatch eventos para una CodeCommit fuente en la CodePipeline documentación de AWS. 2. Elija Destinos (Targets), elija Topic (Tema) y, a continuación, elija Configure input (Configurar entrada). Elija Input transformer (Transformador de entrada) y utilice la ruta de entrada y la plantilla de entrada de la sección Información adicional. Esto garantiza que los detalles CodeCommit del repositorio se analicen y se envíen como variables de entorno al CodeBuild proyecto. Para obtener más información, consulta el tutorial sobre el transformador de entrada en la CloudWatch documentación. 3. Elija Configure details (Configurar detalles), e ingrese un nombre y una descripción para la regla.	

Tarea	Descripción	Habilidades requeridas
	Elija Create rule (Crear regla). Importante: Esta regla de CloudWatch eventos describe los cambios en todos tus CodeCommit repositorios. Debes modificar la regla de CloudWatch eventos si quieres hacer copias de seguridad de CodeCommit repositorios individuales o usar depósitos de S3 independientes para las copias de seguridad de los distintos repositorios.	

Recursos relacionados

Crear un proyecto CodeBuild

- Crea un rol CodeBuild de servicio
- Crea un CodeBuild proyecto
- Permisos obligatorios para comandos del cliente Git

Crear y configurar una regla de CloudWatch eventos

- Cree una regla de CloudWatch eventos para una CodeCommit fuente
- Utilizar el transformador de entrada para personalizar qué se transfiere al destino de eventos
- Cree una regla de CloudWatch eventos que se inicie en un evento
- Cree un rol de CloudWatch IAM de eventos

Información adicional

CodeBuild plantilla buildspec.yml

```
version: 0.2
phases:
  install:
    commands:
      - pip install git-remote-codecommit
  build:
    commands:
       - env
       - git clone -b $REFERENCE_NAME codecommit::$REPO_REGION://$REPOSITORY_NAME
       - dt=$(date '+%d-%m-%Y-%H:%M:%S');
       - echo "$dt"
       - zip -yr $dt-$REPOSITORY_NAME-backup.zip ./
       - aws s3 cp $dt-$REPOSITORY_NAME-backup.zip s3:// #substitute a valid S3 Bucket
 Name here
```

CloudWatch Regla de eventos

```
{
  "source": [
    "aws.codecommit"
  ],
  "detail-type": [
    "CodeCommit Repository State Change"
  ],
  "detail": {
    "event": [
      "referenceCreated",
      "referenceUpdated"
    ]
  }
}
```

Ejemplo de transformador de entrada para el objetivo de la regla de CloudWatch eventos

Ruta de entrada:

```
{"referenceType":"$.detail.referenceType","region":"$.region","repositoryName":"$.detail.reposi
```

Plantilla de entrada (rellene los valores según corresponda):

```
{
    "environmentVariablesOverride": [
        {
            "name": "REFERENCE_NAME",
            "value": ""
        },
        {
            "name": "REFERENCE_TYPE",
            "value": ""
        },
        {
            "name": "REPOSITORY_NAME",
            "value": ""
        },
        {
            "name": "REPO_REGION",
            "value": ""
        },
        {
            "name": "ACCOUNT_ID",
            "value": ""
        }
    ]
}
```

Automatice la implementación de conjuntos de pilas mediante AWS CodePipeline y AWS CodeBuild

Creado por Thiyagarajan Mani (AWS), Mihir Borkar (AWS) y Raghu Gowda (AWS)

Repositorio de código: automated-code-pipeline-stackset -deployment	Entorno: producción	Tecnologías: DevOps desarrollo y pruebas de software
Servicios de AWS: AWS CodeBuild CodeCommit; AWS CodePipeline; AWS Organizations; AWS CloudFormation		

Resumen

En sus procesos de integración continua y entrega continua (CI/CD), es posible que desee implementar aplicaciones automáticamente en todas sus cuentas de AWS existentes y en las cuentas nuevas que añada a su organización en AWS Organizations. Al diseñar una solución de CI/CD para este requisito, la capacidad de administrador de conjuntos de pilas delegado de AWS CloudFormation resulta útil porque habilita una capa de seguridad al restringir el acceso a la cuenta de administración. Sin embargo, AWS CodePipeline utiliza el modelo de permisos gestionados por el servicio para implementar aplicaciones en varias cuentas y regiones. Debe usar la cuenta de administración de AWS Organizations para realizar la implementación con conjuntos de pilas, ya CodePipeline que AWS no admite la función de administrador delegado de conjuntos de pilas.

Este patrón describe cómo puede evitar esta limitación. El patrón utiliza AWS CodeBuild y un script personalizado para automatizar la implementación de conjuntos de pilas con AWS CodePipeline. Automatiza las siguientes actividades de implementación de aplicaciones:

- Implementación de una aplicación como conjuntos de pilas en unidades organizativas (UO) existentes
- Ampliación de la implementación de una aplicación a UO y regiones adicionales
- Eliminación de una aplicación implementada de todas o determinadas UO o regiones

Requisitos previos y limitaciones

Requisitos previos

Antes de seguir los pasos de este patrón:

- Cree organizaciones en su cuenta de administración de AWS Organizations. Para obtener instrucciones, consulte la documentación de AWS Organizations.
- Habilite el acceso confiable entre AWS Organizations y utilice CloudFormation los permisos administrados por el servicio. Para obtener instrucciones, consulte Habilitar el acceso de confianza con AWS Organizations en la CloudFormation documentación.

Limitaciones

El código que se suministra con este patrón tiene las siguientes limitaciones:

- Puede implementar solo una CloudFormation plantilla para una aplicación; actualmente, no se admite el despliegue de varias plantillas.
- La personalización de la implementación actual requiere DevOps experiencia.
- Este patrón no utiliza claves AWS Key Management System (AWS KMS). Sin embargo, puede habilitar esta funcionalidad reconfigurando la CloudFormation plantilla incluida en este patrón.

Arquitectura

Esta arquitectura para la canalización de la implementación de CI/CD gestiona lo siguiente:

- Restringe el acceso directo a la cuenta de administración al delegar la responsabilidad de implementación del conjunto de pilas a una cuenta de CI/CD dedicada como administradora del conjunto de pilas para las implementaciones de aplicaciones.
- Utiliza el modelo de permisos administrados por servicios para implementar la aplicación automáticamente cada vez que se crea una nueva cuenta y se asigna a una UO.
- Garantiza la coherencia de las versiones de las aplicaciones en todas las cuentas del entorno.
- Utiliza varias etapas de aprobación en el repositorio y la canalización para proporcionar capas adicionales de seguridad y control a la aplicación implementada.

- Supera la limitación actual que suponía utilizar un script de CodePipeline despliegue personalizado para implementar o CodeBuild eliminar automáticamente conjuntos de pilas e instancias de pila. Para ver un ejemplo del control de flujo y la jerarquía de las llamadas a las API implementadas por el script personalizado, consulte la sección de Información adicional.
- Crea conjuntos de pilas individuales para los entornos de desarrollo, prueba y producción. Además, puede crear conjuntos de pilas que combinen varias UO y regiones en cada etapa. Por ejemplo, puede combinar UO de entorno aislado y de desarrollo en una etapa de implementación de desarrollo.
- Admite la implementación de aplicaciones en, o la exclusión de, un subconjunto de cuentas o una lista de unidades organizativas.

Automatizar y escalar

Puede usar el código que se proporciona con este patrón para crear un CodeCommit repositorio de AWS y una canalización de código para su aplicación. A continuación, puede implementarlos como conjuntos de pilas en varias cuentas en la unidad organizativa. El código también automatiza componentes como los temas de Amazon Simple Notification Service (Amazon SNS) para notificar a los aprobadores, los roles de AWS Identity and Access Management (IAM) requeridos y la política de control de servicio (SCP) que se aplicará en la cuenta de administración.

Herramientas

Servicios de AWS

- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- AWS CodeBuild es un servicio de compilación totalmente gestionado que le ayuda a compilar código fuente, ejecutar pruebas unitarias y producir artefactos listos para su implementación.
- AWS CodeCommit es un servicio de control de versiones que le ayuda a almacenar y gestionar repositorios de Git de forma privada, sin necesidad de gestionar su propio sistema de control de código fuente.
- AWS CodeDeploy automatiza las implementaciones en Amazon Elastic Compute Cloud (Amazon EC2) o en instancias locales, funciones de AWS Lambda o servicios de Amazon Elastic Container Service (Amazon ECS).

- AWS le CodePipeline ayuda a modelar y configurar rápidamente las diferentes etapas de una versión de software y a automatizar los pasos necesarios para publicar cambios de software de forma continua.
- AWS Organizations es un servicio de administración de cuentas que le permite agrupar varias cuentas de AWS en una organización que usted crea y administra de manera centralizada.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub automated-code-pipeline-stackset-deployment. Para ver la estructura de carpetas y otros detalles, consulte el archivo readme del repositorio.

Prácticas recomendadas

Este patrón restringe el acceso directo a la cuenta de administración al implementar la aplicación en la UO. Agregar varias etapas de aprobación al proceso de canalización y repositorio ayuda a proporcionar seguridad y gobierno adicionales a las aplicaciones y los componentes que se implementan mediante este enfoque.

Epics

Configurar cuentas en AWS Organizations

Tarea	Descripción	Habilidades requeridas
Habilitar todas las caracterí sticas en la cuenta de administración.	Habilitar todas las caracterí sticas de la cuenta de administración de su organización siguiendo las instrucciones de la documenta ción de AWS Organizations.	Administrador de AWS, administrador de plataformas
Crear una cuenta CI/CD.	En AWS Organizations, en su organización, crear una	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	cuenta de CI/CD dedicada y asignar a un equipo la propiedad y el control del acceso a la cuenta.	
Agregar un administrador delegado.	En la cuenta de administración, registrar la cuenta de CI/CD que creó en el paso anterior como administrador delegado del conjunto de pilas. Para obtener instrucciones, consulte la CloudFormation documentación de AWS.	Administrador de AWS, administrador de plataformas

Crear un repositorio de aplicaciones y una canalización de CI/CD

Tarea	Descripción	Habilidades requeridas
Clone el repositorio de código.	1. Clone el repositorio de código proporcionado con este patrón en su computadora: `git clone https://github.com/aws-samples/automated-code-pipeline-stackset-deployment.git` 2. Revisar el archivo readme para entender la estructura de directorios y otros detalles.	AWS DevOps
Cree temas de SNS.	Puede usar la `sns-template.yaml` plantilla que se	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	proporciona en el GitHub repositorio para crear temas de SNS y configurar las suscripciones para las solicitudes de aprobación. 1. En la consola de AWS, inicie sesión en la cuenta de CI/CD. 2. Abre la CloudFormation consola en https://console.aws.amazon.com/cloudformation. 3. Cree una pila nueva con nuevos recursos (opción estándar). 4. En Especificar plantilla, elija Cargar un archivo de plantilla, Elegir archivo y, a continuación, seleccione el `sns-template.yaml` archivo de la `templates` carpeta del GitHub repositorio clonado. Elija Next (Siguiente). 5. Proporcione un nombre significativo para la pila de aplicaciones. 6. Especifique un prefijo para los recursos. 7. Seleccione Next (Siguiente), Next (Siguiente) y Submit (Enviar).	

Tarea	Descripción	Habilidades requeridas
	8. Cuando la pila se haya creado correctamente, seleccione la pestaña Outputs (Salidas) y anote los nombres de recursos de Amazon (ARN) de los temas de SNS para las solicitudes de incorporación de datos, el entorno de pruebas y el entorno de producción. Utilizará esta información en los pasos siguientes.	

Tarea	Descripción	Habilidades requeridas
Crear roles de IAM para los componentes de CI/CD.	Puede utilizar la `cicd-role-template.yaml` plantilla que se proporciona en el GitHub repositorio para crear las funciones y políticas de IAM requeridas por los componentes de la CI/CD. 1. En la consola de AWS, inicie sesión en la cuenta de CI/CD. 2. Abra la CloudFormation consola en https://console.aws.amazon.com/cloudformation. 3. Cree una pila nueva con nuevos recursos (opción estándar). 4. En Especificar plantilla, elija Cargar un archivo de plantilla, Elegir archivo y, a continuación, seleccione el `cicd-role-template.yaml` archivo de la `templates` carpeta del GitHub repositorio clonado. Elija Next (Siguiente). 5. Proporcione un nombre significativo para la pila de aplicaciones. 6. Introduzca los valores de los siguientes parámetros: • El ARN para la política de límite de permisos.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	Puede obtener este ARN en la sección Detalles de la política de su política de límites de permisos en la consola de IAM. • El ARN del tema de aprobación de producción SNS que anotó anteriormente. • El ARN del tema de aprobación de la prueba SNS que anotó anteriormente. • Un prefijo para los recursos creados por la plantilla. 7. Seleccione Next (Siguiente), Next (Siguiente) y Submit (Enviar). 8. Cuando la pila se haya creado correctamente, seleccione la pestaña Outputs (Salidas) y anote los ARN de los roles de IAM que se crearon. Utilizará esta información en los pasos siguientes.	

Tarea	Descripción	Habilidades requeridas
Cree un CodeCommit repositorio y una canalización de código para su aplicación.	Puedes usar la `cicd-pipeline-template.yaml` plantilla que se proporciona en el GitHub repositorio para crear un CodeCommit repositorio y una canalización de código para tu aplicación. 1. En la consola de AWS, inicie sesión en la cuenta de CI/CD. 2. Abre la CloudFormation consola en https://console.aws.amazon.com/cloudformation. 3. Cree una pila nueva con nuevos recursos (opción estándar). 4. En Especificar plantilla, elija Cargar un archivo de plantilla, Elegir archivo y, a continuación, seleccione el `cicd-pipeline-template.yaml` archivo de la `templates` carpeta del GitHub repositorio clonado. Elija Next (Siguiente). 5. Proporcione un nombre significativo para la pila de aplicaciones. 6. Introduzca los valores de los siguientes parámetros: • AppRepositoryName— El nombre del CodeCommit	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	repositorio que se creará para la aplicación. • AppRepositoryDescription— Una breve descripción del CodeCommit repositorio que se creará para la aplicación. • ApplicationName— El nombre de la aplicación. Esta cadena se utiliza como nombre del CodeCommit repositorio y como prefijo de la canalización de CI/CD. • CloudWatchEventRoleARN: el ARN del rol de CloudWatch evento de la tarea anterior. • CodeBuildProjectRoleARN: el ARN del rol del CodeBuild proyecto de la tarea anterior. • CodePipelineRoleARN: el ARN del CodePipeline rol de la tarea anterior. • DeploymentConfigBucket— El nombre del bucket de Amazon Simple Storage Service (Amazon S3) donde se almacenarán los archivos de configuración de	

Tarea	Descripción	Habilidades requeridas
	despliegue y el archivo.zip del script. • DeploymentConfigKey— La ruta y el nombre del archivo.zip (clave Amazon S3). • PRApprovalSNSARN: el ARN del tema de SNS para las notificaciones de solicitudes de extracción. • ProdApprovalSNSARN: el ARN del tema SNS para las aprobaciones de producción. • TESTApprovalSNSARN: el ARN del tema de SNS para las aprobaciones de pruebas. • TemplateBucket— El nombre del depósito de S3 de la cuenta de CI/CD donde se almacenará la plantilla de creación de canalizaciones de CI/CD. 7. Seleccione Next (Siguiente), Next (Siguiente) y Submit (Enviar). 8. Cuando la pila se completa correctamente, se crea un CodeCommit repositorio con el nombre especificado y una estructura de directorios predeterminada,	

Tarea	Descripción	Habilidades requeridas
	archivos de configuración de despliegue, scripts y una canalización de código para el repositorio.	

Implementación de un conjunto de pilas

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio de la aplicación.	La plantilla de canalización de CI/CD que utilizó anteriorm ente crea un repositorio de aplicaciones y una canalizac ión de código de muestra. Para clonar y verificar el repositorio: 1. Inicie sesión en la cuenta de CI/CD. 2. Busque el repositorio de la aplicación y la canalizac ión de CI/CD que creó en la epopeya anterior. 3. Copie la URL del repositorio y use el comando git clone para clonar el repositorio en su máquina local. 4. Compruebe que la estructur a del directorio y los archivos coincidan con lo siguiente: `root` `|- deploy_configs`	Desarrollador de aplicaciones, ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	<pre>| |- deployment_config.json |- parameters | |- template-parameter-dev.json | |- template-parameter-test.json | |- template-parameter-prod.json |- templates | |- template.yml |- buildspec.yml</pre> donde la `deploy_configs` carpeta contiene el archivo de configuración de despliegue y las `parameters` carpetas `templates` y incluyen los archivos predeterminados que sustituirá por sus propios archivos de CloudFormation plantillas y parámetros. Importante: No personalice la estructura de carpetas. 5. Cree una rama de características.	

Tarea	Descripción	Habilidades requeridas
Agregar artefactos de aplicaciones.	Actualice el repositorio de aplicaciones mediante una CloudFormation plantilla. Nota: Esta solución admite el despliegue de una sola CloudFormation plantilla. 1. Cree una CloudFormation plantilla para implementar los cambios en el código de la aplicación y asígnele un nombre`<application-name>.yaml` . 2. Sustituya el `template.yml` archivo de la `templates` carpeta del repositorio de aplicaciones por la CloudFormation plantilla que creó en el paso 1. 3. Prepare los archivos de parámetros para cada entorno (desarrollo, pruebas y producción). 4. Asigne un nombre a los archivos de parámetros con el formato `<cloudformation-template-name>-parameter-<environment-name>.json` . 5. Sustituya los archivos de parámetros predeterm	Desarrollador de aplicaciones, ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	inados de la carpeta `parameters` por los archivos del paso 4.	

Tarea	Descripción	Habilidades requeridas
Actualizar el archivo de configuración de implement ación.	Actualice el archivo `deployment_config.json` : 1. En el repositorio de aplicaciones, navegue hasta la carpeta `deploy_configs` . 2. Abra el archivo `deployment_config.json` : `{ "deployment_action": "<deploy/delete>", "stack_set_name": "<stack set name>", "stack_set_desciption": "<stack set description>", "deployment_targets": { "dev": { "org_units": ["list of OUs"], "regions": ["list of regions"], "filter_accounts": ["list of accounts"],`	Desarrollador de aplicaciones, ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	"filter_type": "<DIFFERENCE/INTERSECTION/UNION>" }, "test": { "org_units": ["list of OUs"], "regions": ["list of regions"], "filter_accounts": ["list of accounts"], "filter_type": "<DIFFERENCE/INTERSECTION/UNION>" }, "prod": { "org_units": ["list of OUs"], "regions": ["list of regions"],	

Tarea	Descripción	Habilidades requeridas
	<pre>"filter_accounts": ["list of accounts"], "filter_type": "<DIFFERENCE/INTERSECTION/UNION>" } }, "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"], "auto_deployement": "<True/False>", "retain_stacks_on_account_removal": "<True/False>", "region_deployment_concurrency": "<SEQUENTIAL/PARALLEL>" }</pre> 3. Actualice los valores de acción de implementación, el nombre del conjunto de pilas, la descripción del conjunto de pilas y los objetivos de implement ación. Por ejemplo, puede configurar `deploymen`	

Tarea	Descripción	Habilidades requeridas
	`t_action` como `delete` para que elimine el conjunto de pilas completo y sus instancias de pila asociadas . Se utiliza `deploy` para crear un conjunto de pilas nuevo, actualizar un conjunto de pilas existente o añadir o eliminar instancia s de pila para unidades organizativas o regiones adicionales. Para obtener más ejemplos, consulte la sección Additional informati on (Información adicional). Este patrón crea conjuntos de pilas individuales para cada entorno añadiendo el nombre del entorno al nombre del conjunto de pilas que se proporciona en el archivo de configuración de implement ación.	

Tarea	Descripción	Habilidades requeridas
Confirme los cambios e implemente el conjunto de pilas.	Confirme los cambios que especificó en la plantilla de la aplicación y fusione e implemente el conjunto de pilas en varios entornos paso a paso: 1. Guarde todos sus archivos y confirme los cambios en la rama de caracterí sticas de su repositorio de aplicaciones local. 2. Inserte la rama de caracterí sticas en el repositorio remoto. 3. Cree una solicitud de extracción para combinar los cambios en la rama principal. Cuando la solicitud de extracción haya sido aprobada y los cambios se hayan fusionado con la rama principal, se iniciará la canalización de CI/CD. 4. Cuando la etapa de desarrollo y despliegue se haya completado correctam ente, consulte la pestaña Administrado por el servicio de la CloudFormation consola. StackSets	Desarrollador de aplicaciones, ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	Verá un nuevo conjunto de pilas con el sufijo `dev`. 5. Compruebe los CodeBuild registros de la etapa de despliegue de desarroll o para ver si hay algún problema. 6. Implemente el conjunto de pilas en los entornos de prueba y producción solicitando a sus responsab les de aprobación que aprueben las implement aciones de esas etapas y repitiendo los pasos 5 y 6. Los conjuntos de pilas para los entornos de prueba y producción tienen los sufijos `test` y `prod`.	

Solución de problemas

Problema	Solución
La implementación falla y muestra la excepción : Cambie el nombre del archivo de parámetros de la plantilla a <application name>-parameter-<evn>.json; no se permiten los nombres predeterminados	Los archivos CloudFormation de parámetro s de la plantilla deben seguir la convención de nomenclatura especificada. Actualice los nombres de archivo de parámetros e inténtelo de nuevo.

Problema	Solución
La implementación falla y muestra la excepción : Cambie el nombre de la CloudFormation plantilla a .yml; las plantillas predeterm inadas.yml o template.yaml no están permitidas <application name>	El nombre de la plantilla debe seguir la convención de nomenclatura especificada. CloudFormation Actualice el nombre del archivo e inténtelo de nuevo.
La implementación falla y muestra la excepción : No se ha encontrado CloudFormation una plantilla válida ni su archivo de parámetros para el entorno {environment name}	Compruebe las convenciones de nomenclatura de archivos de la CloudFormation plantilla y su archivo de parámetros para el entorno especific ado.
La implementación falla y muestra la excepción : Acción de implementación no válida proporcio nada en el archivo de configuración de implementación. Las opciones válidas son «implementar» y «eliminar».	Usted especificó un valor no válido para el parámetro `deployment_action` en el archivo de configuración de implementación. El parámetro tiene dos valores válidos: `deploy` y`delete`. Utilice `deploy` para crear y actualiza r los conjuntos de pilas y sus instancias de pila asociadas. Utilice `delete` solo cuando desee eliminar el conjunto de pilas completo y las instancias de pila asociadas.

Recursos relacionados

- GitHub automated-code-pipeline-stackset-repositorio de despliegue
- Habilitar todas las características en su organización (documentación de AWS Organizations)
- Registrar un administrador delegado (CloudFormation documentación de AWS)
- Objetivos a nivel de cuenta para conjuntos de pilas administrados por servicios (documentación de AWS CloudFormation)

Información adicional

Diagrama de flujo

El siguiente diagrama de flujo muestra el control de flujo y la jerarquía de las llamadas a la API implementadas por el script personalizado para automatizar la implementación de conjuntos de pilas.

Archivos de configuración de implementación de muestra

Crear un nuevo conjunto de pila

El siguiente archivo de configuración de implementación crea un nuevo conjunto de pilas llamado `sample-stack-set` en la región de AWS `us-east-1` en tres unidades organizativas.

```
{
     "deployment_action": "deploy",
     "stack_set_name": "sample-stack-set",
     "stack_set_desciption": "this is a sample stack set",
    "deployment_targets": {
                            "dev": {
                                        "org_units": ["dev-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                            "test": {
                                        "org_units": ["test-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                            "prod": {
                                        "org_units": ["prod-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    }
                          },
     "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
     "auto_deployement": "True",
     "retain_stacks_on_account_removal": "True",
     "region_deployment_concurrency": "PARALLEL"
```

```
 }
```

Implementación de un conjunto de pilas existente en otra UO

Si implementa la configuración que se muestra en el ejemplo anterior y desea implementar el conjunto de pilas en una UO adicional llamada `dev-org-unit-2` en el entorno de desarrollo, el archivo de configuración de implementación podría tener el siguiente aspecto.

```
{
     "deployment_action": "deploy",
     "stack_set_name": "sample-stack-set",
     "stack_set_desciption": "this is a sample stack set",
    "deployment_targets": {
                              "dev": {
                                          "org_units": ["dev-org-unit-1", "dev-org-
unit-2"],
                                          "regions": ["us-east-1"],
                                          "filter_accounts": [],
                                          "filter_type": ""
                                      },
                              "test": {
                                          "org_units": ["test-org-unit-1"],
                                          "regions": ["us-east-1"],
                                          "filter_accounts": [],
                                          "filter_type": ""
                                      },
                              "prod": {
                                          "org_units": ["prod-org-unit-1"],
                                          "regions": ["us-east-1"],
                                          "filter_accounts": [],
                                          "filter_type": ""
                                      }
                           },
     "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
     "auto_deployement": "True",
     "retain_stacks_on_account_removal": "True",
     "region_deployment_concurrency": "PARALLEL"
 }
```

Implementación de un conjunto de pilas existente en otra región de AWS

Si implementa la configuración que se muestra en el ejemplo anterior y desea implementar el conjunto de pilas en una región de AWS adicional (`us-east-2`) en el entorno de desarrollo de dos

UO (`dev-org-unit-1` y `dev-org-unit-2`), el archivo de configuración de implementación podría tener el siguiente aspecto.

Nota: Los recursos de la CloudFormation plantilla deben ser válidos y específicos de la región.

```
{
     "deployment_action": "deploy",
     "stack_set_name": "sample-stack-set",
     "stack_set_desciption": "this is a sample stack set",
    "deployment_targets": {
                             "dev": {
                                        "org_units": ["dev-org-unit-1", "dev-org-
unit-2"],
                                        "regions": ["us-east-1", "us-east-2"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                             "test": {
                                        "org_units": ["test-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                             "prod": {
                                        "org_units": ["prod-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    }
                           },
     "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
     "auto_deployement": "True",
     "retain_stacks_on_account_removal": "True",
     "region_deployment_concurrency": "PARALLEL"
 }
```

Eliminar una instancia de pila de una UO o una región de AWS

Supongamos que se ha implementado la configuración de implementación que se muestra en el ejemplo anterior. El siguiente archivo de configuración elimina las instancias de pila de ambas regiones de la UO`dev-org-unit-2`.

```
{
```

```
     "deployment_action": "deploy",
     "stack_set_name": "sample-stack-set",
     "stack_set_desciption": "this is a sample stack set",
    "deployment_targets": {
                            "dev": {
                                        "org_units": ["dev-org-unit-1"],
                                        "regions": ["us-east-1", "us-east-2"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                            "test": {
                                        "org_units": ["test-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                            "prod": {
                                        "org_units": ["prod-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    }
                           },
     "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
     "auto_deployement": "True",
     "retain_stacks_on_account_removal": "True",
     "region_deployment_concurrency": "PARALLEL"
 }
```

El siguiente archivo de configuración elimina la instancia de pila de la región de AWS `us-east-1` para ambas UO del entorno de desarrollo.

```
{
     "deployment_action": "deploy",
     "stack_set_name": "sample-stack-set",
     "stack_set_desciption": "this is a sample stack set",
    "deployment_targets": {
                            "dev": {
                                        "org_units": ["dev-org-unit-1", "dev-org-
unit-2"],
                                        "regions": ["us-east-2"],
                                        "filter_accounts": [],
```

```
                                        "filter_type": ""
                                    },
                                "test": {
                                        "org_units": ["test-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                                "prod": {
                                        "org_units": ["prod-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    }
                            },
    "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
    "auto_deployement": "True",
    "retain_stacks_on_account_removal": "True",
    "region_deployment_concurrency": "PARALLEL"
 }
```

Eliminar todo el conjunto de pilas

El siguiente archivo de configuración de implementación elimina el conjunto de pilas completo y todas sus instancias de pila asociadas.

```
{
     "deployment_action": “delete”,
     "stack_set_name": "sample-stack-set",
     "stack_set_desciption": "this is a sample stack set",
    "deployment_targets": {
                                "dev": {
                                        "org_units": ["dev-org-unit-1", "dev-org-
unit-2"],
                                        "regions": ["us-east-2"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                                "test": {
                                        "org_units": ["test-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
```

```
                                },
                            "prod": {
                                    "org_units": ["prod-org-unit-1"],
                                    "regions": ["us-east-1"],
                                    "filter_accounts": [],
                                    "filter_type": ""
                                }
                        },
    "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
    "auto_deployement": "True",
    "retain_stacks_on_account_removal": "True",
    "region_deployment_concurrency": "PARALLEL"
}
```

Excluir una cuenta de la implementación

El siguiente archivo de configuración de implementación excluye de la implementación la cuenta `111122223333`, que forma parte de la UO `dev-org-unit-1`.

```
{
    "deployment_action": "deploy",
    "stack_set_name": "sample-stack-set",
    "stack_set_desciption": "this is a sample stack set",
   "deployment_targets": {
                            "dev": {
                                    "org_units": ["dev-org-unit-1"],
                                    "regions": ["us-east-1"],
                                    "filter_accounts": ["111122223333"],
                                    "filter_type": "DIFFERENCE"
                                },
                            "test": {
                                    "org_units": ["test-org-unit-1"],
                                    "regions": ["us-east-1"],
                                    "filter_accounts": [],
                                    "filter_type": ""
                                },
                            "prod": {
                                    "org_units": ["prod-org-unit-1"],
                                    "regions": ["us-east-1"],
                                    "filter_accounts": [],
                                    "filter_type": ""
                                }
                        },
```

```
    "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
    "auto_deployement": "True",
    "retain_stacks_on_account_removal": "True",
    "region_deployment_concurrency": "PARALLEL"
}
```

Implementación de la aplicación en un subconjunto de cuentas de una UO

El siguiente archivo de configuración de implementación implementa la aplicación solo en tres cuentas (111122223333, 444455556666 y 777788889999) de la UO `dev-org-unit-1`.

```
{
    "deployment_action": "deploy",
    "stack_set_name": "sample-stack-set",
    "stack_set_desciption": "this is a sample stack set",
   "deployment_targets": {
                            "dev": {
                                        "org_units": ["dev-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": ["111122223333",
"444455556666", "777788889999"],
                                        "filter_type": "INTERSECTION"
                                    },
                            "test": {
                                        "org_units": ["test-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                            "prod": {
                                        "org_units": ["prod-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    }
                          },
    "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
    "auto_deployement": "True",
    "retain_stacks_on_account_removal": "True",
    "region_deployment_concurrency": "PARALLEL"
}
```

Adjunte automáticamente una política administrada de AWS para Systems Manager a los perfiles de instancia de EC2 mediante Cloud Custodian y AWS CDK

Creado por Ali Asfour (AWS) y Aaron Lennon (AWS)

Entorno: PoC o piloto	Tecnologías: desarrollo y pruebas de software DevOps; gestión y gobierno; seguridad , identidad y cumplimiento; infraestructura	Carga de trabajo: código abierto
Servicios de AWS: Amazon SNS; Amazon SQS; CodeBuild AWS; AWS; CodePipeline AWS Systems Manager; AWS CodeCommit		

Resumen

Puede integrar instancias de Amazon Elastic Compute Cloud (Amazon EC2) con AWS Systems Manager para automatizar las tareas operativas y proporcionar más visibilidad y control. Para integrarse con Systems Manager, las instancias EC2 deben tener instalado AWS Systems Manager Agent (SSM Agent) y una política de `AmazonSSMManagedInstanceCore` AWS Identity and Access Management (IAM) adjunta a sus perfiles de instancia.

Sin embargo, si quiere asegurarse de que todos los perfiles de instancias de EC2 incorporan la política `AmazonSSMManagedInstanceCore`, puede enfrentarse a dificultades al actualizar las nuevas instancias de EC2 que no tienen perfiles de instancia o las instancias de EC2 que tienen un perfil de instancia pero no tienen la política `AmazonSSMManagedInstanceCore`. También puede resultar difícil añadir esta política en varias cuentas de Amazon Web Services (AWS) y regiones de AWS.

Este patrón ayuda a resolver estos desafíos mediante la implementación de tres políticas de Cloud Custodian en sus cuentas de AWS:

- La primera política de Cloud Custodian comprueba las instancias de EC2 existentes que tienen un perfil de instancia pero que no cuentan con la política `AmazonSSMManagedInstanceCore`. A continuación, se adjunta la política `AmazonSSMManagedInstanceCore`.
- La segunda política de Cloud Custodian comprueba las instancias de EC2 existentes sin un perfil de instancia y añade un perfil de instancia predeterminado que tiene la política `AmazonSSMManagedInstanceCore` adjunta.
- La tercera política de Cloud Custodian crea funciones de AWS Lambda en sus cuentas para supervisar la creación de instancias y perfiles de instancias de EC2. Esto garantiza que la política `AmazonSSMManagedInstanceCore` se adjunte automáticamente cuando se cree una instancia de EC2.

Este patrón utiliza DevOps las herramientas de AWS para lograr una implementación continua y a escala de las políticas de Cloud Custodian en un entorno de varias cuentas, sin aprovisionar un entorno informático independiente.

Requisitos previos y limitaciones

Requisitos previos

- Dos o más cuentas de AWS activas. Una cuenta es la cuenta de seguridad y las demás son cuentas de miembros.
- Permisos para aprovisionar recursos de AWS en la cuenta de seguridad. Este patrón utiliza permisos de administrador, pero usted debe conceder los permisos de acuerdo con los requisitos y las políticas de su organización.
- Capacidad para asumir un rol de IAM desde la cuenta de seguridad hasta las cuentas de los miembros y crear los roles de IAM necesarios. Para obtener más información al respecto, consulte Delegar el acceso entre cuentas de AWS utilizando roles de IAM en la documentación de IAM.
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada. Para realizar pruebas, puede configurar la AWS CLI mediante el comando `aws configure` o configurando variables de entorno. Importante: esto no se recomienda para entornos de producción y recomendamos que a esta cuenta solo se le conceda el acceso con privilegios mínimos. Para obtener más información al respecto, consulte Conceder privilegios mínimos en la documentación de IAM.
- El archivo `devops-cdk-cloudcustodian.zip` (adjunto), descargado en su equipo local.
- Familiaridad con Python.

- Las herramientas necesarias (Node.js, AWS Cloud Development Kit (AWS CDK) y Git), instaladas y configuradas. Puede usar el archivo `install-prerequisites.sh` incluido en el archivo `devops-cdk-cloudcustodian.zip` para instalar estas herramientas. Asegúrese de ejecutar este archivo con privilegios de administrador.

Limitaciones

- Si bien este patrón se puede utilizar en un entorno de producción, asegúrese de que todos los roles y las políticas de IAM cumplan con los requisitos y las políticas de su organización.

Versiones de paquetes

- Cloud Custodian, versión 0.9 o posterior
- TypeScript versión 3.9.7 o posterior
- Node.js versión 14.15.4 y posteriores
- `npm` versión 7.6.1 o posterior
- AWS CDK, versión 1.96.0 o posterior

Arquitectura

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Las políticas de Cloud Custodian se envían a un CodeCommit repositorio de AWS en la cuenta de seguridad. Una regla de Amazon CloudWatch Events inicia automáticamente la CodePipeline canalización de AWS.
2. La canalización obtiene el código más reciente CodeCommit y lo envía a la parte de integración continua de la canalización de integración continua y entrega continua (CI/CD) gestionada por AWS. CodeBuild
3. CodeBuild realiza todas las DevSecOps acciones, incluida la validación de la sintaxis de las políticas de Cloud Custodian, y ejecuta estas políticas en `--dryrun` modo automático para comprobar qué recursos están identificados.
4. Si no hay errores, la siguiente tarea avisa al administrador para que revise los cambios y apruebe la implementación en las cuentas de los miembros.

Pila de tecnología

- AWS CDK
- CodeBuild
- CodeCommit
- CodePipeline
- IAM
- Cloud Custodian

Automatizar y escalar

El módulo AWS CDK Pipelines proporciona una canalización de CI/CD que se utiliza CodePipeline para organizar la creación y las pruebas del código fuente CodeBuild, además de la implementación de recursos de AWS con pilas de AWS. CloudFormation Puede usar este patrón para todas las cuentas de miembros y regiones de su organización. También puede ampliar la pila `Roles creation` para implementar otros roles de IAM en sus cuentas de miembros.

Herramientas

- El AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software para definir la infraestructura de nube en el código y aprovisionarla a través de AWS. CloudFormation
- La Interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su shell de línea de comandos.
- AWS CodeBuild es un servicio de compilación en la nube totalmente gestionado.
- AWS CodeCommit es un servicio de control de versiones que puede utilizar para almacenar y gestionar activos de forma privada.
- AWS CodePipeline es un servicio de entrega continua que puede utilizar para modelar, visualizar y automatizar los pasos necesarios para lanzar el software.
- AWS Identity and Access Management (IAM) es un servicio web que le ayuda a controlar de forma segura el acceso a los recursos de AWS.
- Cloud Custodian es una herramienta que unifica las decenas de herramientas y scripts que la mayoría de las organizaciones utilizan para administrar sus cuentas de nube pública en una sola herramienta de código abierto.

- Node.js es un JavaScript motor de ejecución basado en el JavaScript motor V8 de Google Chrome.

Código

Para obtener una lista detallada de los módulos, las funciones de la cuenta, los archivos y los comandos de implementación que se utilizan en este patrón, consulte el archivo `README` en el archivo `devops-cdk-cloudcustodian.zip` (adjunto).

Epics

Configure la canalización con AWS CDK

Tarea	Descripción	Habilidades requeridas
Configura el CodeCommit repositorio.	1. Arranque el archivo `devops-cdk-cloudcustodian.zip` (adjunto) en el directorio de trabajo en su equipo local. 2. Inicie sesión en la consola de administración de AWS de su cuenta de seguridad, abra la CodeCommit consola y, a continuación, cree un `devops-cdk-cloudcustodian` repositorio nuevo. 3. Diríjase al directorio del proyecto y configure el CodeCommit repositorio como origen, confirme los cambios y, a continuación, envíelos a la rama de origen ejecutando los siguientes comandos:	Desarrollador

Tarea	Descripción	Habilidades requeridas
	• `cd devops-cdk-cloudcustodian` • `git init --initial-branch=main` • `git add . git commit -m 'initial commit'` • `git remote add origin https://git-codecommit.us-east-1.amazonaws.com/v1/devops-cdk-cloudcustodian` • `git push origin main` Para obtener más información al respecto, consulte Creación de un CodeCommit repositorio en la CodeCommit documentación de AWS.	
Instalar las herramientas necesarias.	Utilice el archivo `install-prerequisites.sh` para instalar todas las herramientas necesarias en Amazon Linux. Esto no incluye la AWS CLI porque viene preinstalada. Para obtener más información al respecto, consulte la sección Requisitos previos de Introducción a AWS CDK en la documentación de AWS CDK.	Desarrollador

Tarea	Descripción	Habilidades requeridas
Instalar los paquetes de AWS CDK obligatorios.	1. Configure su entorno virtual ejecutando el siguiente comando en la CLI de AWS: `$ python3 -m venv .env` 2. Active su entorno virtual ejecutando el siguiente comando: `$ source .env/bin/activate` 3. Después de activar el entorno virtual, instale las dependencias necesarias mediante la ejecución del siguiente comando: `$ pip install -r requirements.txt` 4. Para añadir dependencias adicionales (por ejemplo, otras bibliotecas de AWS CDK), agréguelas al archivo `requirements.txt` y ejecute el siguiente comando: `pip install -r requirements.txt` AWD CDK requiere los siguientes paquetes y se incluyen en el archivo `requirements.txt` : • `aws-cdk.aws-cloudwatch`	Desarrollador

Tarea	Descripción	Habilidades requeridas
	• `aws-cdk.aws-codebuild` • `aws-cdk.aws-codecommit` • `aws-cdk.aws-codedeploy` • `aws-cdk.aws-codepipeline` • `aws-cdk.aws-codepipeline-actions` • `aws-cdk.aws-events` • `aws-cdk.aws-events-targets` • `aws-cdk.aws-iam` • `aws-cdk.aws-logs` • `aws-cdk.aws-s3` • `aws-cdk.aws-sns` • `aws-cdk.aws-sns-subscriptions` • `aws-cdk.aws-sqs` • `aws-cdk.core`	

Configuración de su entorno.

Tarea	Descripción	Habilidades requeridas
Actualice las variables requeridas.	Abra el `vars.py` archivo en la carpeta raíz del CodeCommit repositorio y actualice las siguientes variables:	Desarrollador

Tarea	Descripción	Habilidades requeridas
	• Actualice `var_deploy_region = 'us-east-1'` con la región de AWS en la que desea implementar la canalización. • Actualízalo `var_codecommit_repo_name = "cdk-cloudcustodian"` con el nombre de tu CodeCommit repositorio. • Actualiza `var_codecommit_branch_name = "main"` con el nombre de la CodeCommit sucursal. • Actualice `var_adminEmail=notifyadmin@email.com'` con la dirección de correo electrónico del administrador que aprueba los cambios. • Actualice `var_slackWebHookUrl = https://hooks.slack.com/services/T000000000/B00000000/XXXXXXXXXXXXXXXXXXXXXXXX` con el webhook de Slack que se utiliza para enviar notificaciones a Cloud Custodian cuando se realizan cambios. • Actualice `var_orgId = 'o-yyyyyyyyyy'` con el ID de su organización.	

Tarea	Descripción	Habilidades requeridas
	• Actualice `security_account = '123456789011'` con el ID de cuenta de AWS para la cuenta en la que se implementa la canalización. • Actualice `member_accounts = ['111111111111','111111111112','111111111113']` con las cuentas de los miembros en las que desee iniciar la pila de AWS CDK e implementar los roles de IAM necesarios. • Configure `cdk_bootstrap_member_accounts = True` como `True` si desea que la canalización inicie automáticamente AWS CDK en sus cuentas de miembros. Si se configura como `True`, esto también requiere el nombre de un rol de IAM existente en las cuentas de los miembros que se pueda asumir desde la cuenta de seguridad. Este rol de IAM también debe tener los permisos necesarios para arrancar AWS CDK. • Actualice `cdk_bootstrap_role =`	

Tarea	Descripción	Habilidades requeridas
	`'AWSControlTowerExecution'` con el rol de IAM existente en las cuentas de los miembros que se pueden asumir desde la cuenta de seguridad. Este rol también debe tener permiso para arrancar AWS CDK. Nota: Esto sólo se aplica si `cdk_bootstrap_member_accounts` está configurado en `True` .	

Tarea	Descripción	Habilidades requeridas
Actualice el archivo account.yml con la información de la cuenta del miembro.	Para ejecutar la herramienta Cloud Custodian de c7n-org en varias cuentas, debe colocar el archivo de configuración `accounts.yml` en la raíz del repositorio. A continuación, se muestra un ejemplo de archivo de configuración de Cloud Custodian para AWS. `accounts:` `- account_id: '123123123123'` `  name: account-1` `  regions:` `  - us-east-1` `  - us-west-2` `  role: arn:aws:iam::123123123123:role/CloudCustodian` `  vars:` `  charge_code: xyz` `  tags:` `  - type:prod` `  - division:some division` `  - partition:us` `  - scope:pci`	Desarrollador

Arrancar las cuentas de AWS

Tarea	Descripción	Habilidades requeridas
Arranque la cuenta de seguridad.	Arranque `deploy_account` con la aplicación `cloudcust`	Desarrollador

Tarea	Descripción	Habilidades requeridas
	`odian_stack` ejecutando el siguiente comando: `cdk bootstrap -a 'python3 cloudcustodian/cloudcustodian_stack.py`	
Opción 1: arrancar automáticamente las cuentas de los miembros.	Si la variable `cdk_bootstrap_member_accounts` está establecida en `True` en el archivo `vars.py`, la canalización arranca automáticamente las cuentas especificadas en la variable `member_accounts` . Si es necesario, puede actualizar `*cdk_bootstrap_role*` con un rol de IAM que pueda asumir desde la cuenta de seguridad y que tenga los permisos necesarios para arrancar la AWS CDK. La canalización arranca automáticamente las cuentas nuevas que se agreguen a la variable `member_accounts` para poder implementar los roles necesarios.	Desarrollador

Tarea	Descripción	Habilidades requeridas
Opción 2: Inicie manualmente el proceso de arranque de las cuentas de los miembros.	Aunque no se recomiend a utilizar este enfoque, puede establecer el valor de `cdk_bootstrap_memb er_accounts` y `False`, y realizar este paso manualmen te ejecutando el siguiente comando: `$ cdk bootstrap -a 'python3 cloudcust odian/member_accou nt_roles_stack.py' \ --trust {security _account_id} \ --context assume-ro le-credentials:wri teIamRoleName={rol e_name} \ --context assume-ro le-credentials:rea dIamRoleName={role _name} \ --mode=ForWriting \ --context bootstrap =true \ --cloudformation- execution-policies arn:aws:iam::aws:p olicy/Administrato rAccess`	Desarrollador

Tarea	Descripción	Habilidades requeridas
	Importante: asegúrese de actualizar los valores `{security_account_id}` y `{role_name}` con el nombre de un rol de IAM que pueda asumir desde la cuenta de seguridad y que tenga los permisos necesarios para iniciar el proceso de arranque de AWS CDK. También puede utilizar otros enfoques para impulsar las cuentas de los miembros, por ejemplo, con AWS CloudFormation. Para obtener más información al respecto, consulte Proceso de arranque en la documentación de AWS CDK.	

Implemente la pila de AWD CDK.

Tarea	Descripción	Habilidades requeridas
Cree los roles de IAM en las cuentas de los miembros.	Ejecute el siguiente comando para implementar la pila `member_account_roles_stack` y crear los roles de IAM en las cuentas de miembros: `cdk deploy --all -a 'python3 cloudcustodian/member_accou`	Desarrollador

Tarea	Descripción	Habilidades requeridas
	`nt_roles_stack.py' --require-approval never`	
Implemente la pila de canalizaciones de Cloud Custodian.	Ejecute el siguiente comando para crear la canalización `cloudcustodian_stack.py` de Cloud Custodian que se implementa en la cuenta de seguridad: `cdk deploy -a 'python3 cloudcustodian/cloudcustodian_stack.py'`	Desarrollador

Recursos relacionados

- Introducción a los AWS CDK

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Crear automáticamente canalizaciones de CI/CD y clústeres de Amazon ECS para microservicios mediante AWS CDK

Creado por Varsha Raju (AWS)

Entorno: PoC o piloto	Tecnologías: contenedores y microservicios DevOps; Modernización; Infraestructura	Servicios de AWS: AWS CodeBuild; AWS CodeCommit CodePipeline; Amazon ECS; AWS CDK

Resumen

Este patrón describe cómo crear automáticamente las canalizaciones de integración y entrega continuas (CI/CD) y la infraestructura subyacente para crear e implementar microservicios en Amazon Elastic Container Service (Amazon ECS). Puede utilizar este enfoque si quiere configurar canalizaciones de proof-of-concept CI/CD para mostrar a su organización los beneficios de la CI/CD, los microservicios y. DevOps También puede utilizar este enfoque para crear canalizaciones iniciales de CI/CD que, a continuación, podrá personalizar o cambiar según los requisitos de su organización.

El enfoque del patrón crea un entorno de producción y un entorno de no producción, cada uno con una nube privada virtual (VPC) y un clúster de Amazon ECS configurado para ejecutarse en dos zonas de disponibilidad. Todos sus microservicios comparten estos entornos y, a continuación, usted crea una canalización de CI/CD para cada microservicio. Estas canalizaciones de CI/CD extraen los cambios de un repositorio de origen en AWS CodeCommit, los crean automáticamente y, a continuación, los implementan en sus entornos de producción y no producción. Cuando una canalización completa correctamente todas sus etapas, puede usar las URL para acceder al microservicio en los entornos de producción y no producción.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta activa de Amazon Web Services (AWS).
- Un bucket de Amazon Simple Storage Service (Amazon S3) existente que contiene el archivo `starter-code.zip` (adjunto).

- AWS Cloud Development Kit (AWS CDK), instalado y configurado en su cuenta. Para obtener más información al respecto, consulte Introducción a AWS CDK en la documentación de AWS CDK.
- Python 3 y `pip`, instalado y configurado. Para obtener más información, consulte la documentación de Python.
- Familiaridad con AWS CDK CodeBuild, CodePipeline AWS, CodeCommit Amazon Elastic Container Registry (Amazon ECR), Amazon ECS y AWS Fargate.
- Conocimientos de Docker.
- Comprensión de la CI/CD y. DevOps

Limitaciones

- Se aplican límites generales a las cuentas de AWS. Para obtener más información al respecto, consulte AWS Service Quotas en la documentación de referencia general de AWS.

Versiones de producto

- El código se probó usando Node.js versión 16.13.0 y AWS CDK versión 1.132.0.

Arquitectura

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un desarrollador de aplicaciones envía el código a un CodeCommit repositorio.
2. Se inicia una canalización.
3. CodeBuild compila y envía la imagen de Docker a un repositorio de Amazon ECR
4. CodePipeline implementa una nueva imagen en un servicio Fargate existente en un clúster de Amazon ECS que no es de producción.
5. Amazon ECS extrae la imagen del repositorio de Amazon ECR y la coloca en un servicio Fargate de no producción.
6. Las pruebas se realizan mediante una URL de no producción.
7. El administrador de versiones aprueba la implementación de producción.
8. CodePipeline implementa la nueva imagen en un servicio Fargate existente en un clúster de Amazon ECS de producción

9. Amazon ECS extrae la imagen del repositorio de Amazon ECR y la coloca en el servicio Fargate de producción.
10. Los usuarios de producción acceden a su característica mediante una URL de producción.

Pila de tecnología

- AWS CDK
- CodeBuild
- CodeCommit
- CodePipeline
- Amazon ECR
- Amazon ECS
- Amazon VPC

Automatizar y escalar

Puede utilizar el enfoque de este patrón para crear canalizaciones para microservicios implementados en una pila de AWS CloudFormation compartida. La automatización puede crear más de un clúster de Amazon ECS en cada VPC y también crear canalizaciones para los microservicios implementados en un clúster de Amazon ECS compartido. Sin embargo, esto requiere que proporcione nueva información sobre los recursos como entradas a la pila de canalizaciones.

Herramientas

- AWS CDK: el AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software para definir la infraestructura de nube en el código y aprovisionarla a través de AWS. CloudFormation
- AWS CodeBuild: AWS CodeBuild es un servicio de compilación en la nube totalmente gestionado. CodeBuild compila su código fuente, ejecuta pruebas unitarias y produce artefactos listos para su implementación.
- AWS CodeCommit: AWS CodeCommit es un servicio de control de versiones que le permite almacenar y gestionar de forma privada los repositorios de Git en la nube de AWS. CodeCommit elimina la necesidad de administrar su propio sistema de control de código fuente o de preocuparse por escalar su infraestructura.

- AWS CodePipeline: AWS CodePipeline es un servicio de entrega continua que puede utilizar para modelar, visualizar y automatizar los pasos necesarios para lanzar su software. Puede modelar y configurar rápidamente las diferentes etapas de un proceso de lanzamiento de software. CodePipeline automatiza los pasos necesarios para publicar los cambios de software de forma continua.
- Amazon ECS: Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores altamente escalable y rápido que se utiliza para ejecutar, detener y administrar contenedores en un clúster. Las tareas y los servicios se pueden ejecutar en una infraestructura sin servidor administrada por AWS Fargate. Alternativamente, para obtener más control sobre su infraestructura, puede ejecutar sus tareas y servicios en un clúster de instancias de Amazon Elastic Compute Cloud (Amazon EC2) que administre.
- Docker: Docker ayuda a los desarrolladores a empaquetar, enviar y ejecutar cualquier aplicación como un contenedor ligero, portátil y autosuficiente.

Código

El código de este patrón está disponible en los archivos `cicdstarter.zip` y `starter-code.zip` (adjuntos).

Epics

Configure su entorno

Tarea	Descripción	Habilidades requeridas
Configure el directorio de trabajo de AWS CDK.	1. Cree un directorio denominado `cicdproject` en su máquina local. 2. Descargue el archivo `cicdstarter.zip` (adjunto) al directorio `cicdproject` y descomprímalo. Esto crea una carpeta denominada `cicdstarter`.	AWS DevOps, infraestructura en la nube

Tarea	Descripción	Habilidades requeridas
	3. Ejecute el comando `cd <user-home>/cicdproject/cicdstarter` . 4. Configure el entorno virtual de Python ejecutando el comando `python3 -m venv .venv`. 5. Ejecute el comando `source ./.venv/bin/activate` . 6. Configure su entorno de AWS ejecutando el comando `aws configure` o utilizando las siguientes variables de entorno: • `AWS_ACCESS_KEY_ID` • `AWS_SECRET_ACCESS_KEY` • `AWS_DEFAULT_REGION`	

Crear la infraestructura compartida

Tarea	Descripción	Habilidades requeridas
Cree la infraestructura compartida.	1. En su directorio de trabajo, ejecute el comando `cd cicdvpcecs` . 2. Ejecute el comando `pip3 install -r requirements.txt` para instalar todas las dependencias de Python necesarias.	AWS DevOps, infraestructura en la nube

Tarea	Descripción	Habilidades requeridas
	3. Ejecute el `cdk bootstrap command` para configurar el entorno de AWS para AWS CDK. 4. Ejecute el comando `cdk synth --context aws_account=<aws_account_ID> --context aws_region=<aws-region>` . 5. Ejecute el comando `cdk deploy --context aws_account=<aws_account_ID> --context aws_region=<aws-region>` . 6. La CloudFormation pila de AWS crea la siguiente infraestructura: • Una VPC de no producción denominada `cicd-vpc-ecs/cicd-vpc-nonprod` • Una VPC de producción denominada `cicd-vpc-ecs/cicd-vpc-prod` • Un clúster de Amazon ECS de no producción denominado `cicd-ecs-nonprod` • Un clúster de Amazon ECS de producción	

Tarea	Descripción	Habilidades requeridas
	denominado `cicd-ecs-prod`	
Supervise la CloudFormation pila de AWS.	1. Inicie sesión en la consola de administración de AWS, abra la CloudFormation consola de AWS y, a continuación, elija la `cicd-vpc-ecs` pila de la lista. 2. En el panel de detalles de la pila, seleccione la pestaña Eventos y supervise el progreso de la creación de la pila.	AWS DevOps, infraestructura en la nube

Tarea	Descripción	Habilidades requeridas
Pruebe la CloudFormation pila de AWS.	1. Una vez creada la CloudFormation pila de `cicd-vpc-ecs` AWS, asegúrese de que se hayan creado las `cicd-vpc-ecs/cicd-vpc-prod` VPC `cicd-vpc-ecs/cicd-vpc-nonprod` y. 2. Asegúrese de que se creen los clústeres de Amazon ECS `cicd-ecs-nonprod` y `cicd-ecs-prod` . Importante: Asegúrese de registrar los ID de las dos VPC y los ID de los grupos de seguridad de los grupos de seguridad predeterminados en ambas VPC.	AWS DevOps, infraestructura en la nube

Crear una canalización de CI/CD para un microservicio

Tarea	Descripción	Habilidades requeridas
Cree la infraestructura para el microservicio.	1. Asigne un nombre a su microservicio. Por ejemplo, este patrón utiliza `myservice1` como nombre del microservicio. 2. En su directorio de trabajo, ejecute el comando `cd`	AWS DevOps, infraestructura en la nube

Tarea	Descripción	Habilidades requeridas
	`<working-directory>/cdkpipeline` . 3. Ejecute el comando `pip3 install -r requirements.txt` . 4. Ejecute el comando `cdk synth` completo que está disponible en la sección de Información adicional de este patrón. 5. Ejecute el comando `cdk deploy` completo que está disponible en la sección de Información adicional de este patrón. Nota: También puede proporcionar los valores de ambos comandos mediante el archivo `cdk.json` del directorio.	
Supervise la CloudFormation pila de AWS.	Abra la CloudFormation consola de AWS y supervise el progreso de la `myservice1-cicd-stack` pila. Finalmente, el estado cambia a `CREATE_COMPLETE` .	AWS DevOps, infraestructura en la nube

Tarea	Descripción	Habilidades requeridas
Pruebe la CloudFormation pila de AWS.	1. En la CodeCommit consola de AWS, compruebe que `myservice1` existe un repositorio con el nombre y que contiene el código de inicio. 2. En la CodeBuild consola de AWS, compruebe que `myservice1` existe un proyecto de compilación denominado. 3. En la consola de Amazon ECR, verifique que existe un repositorio de Amazon ECR denominado `myservice1` . 4. En la consola de Amazon ECS, verifique que exista un servicio de Fargate denominado `myservice1` en un clúster de Amazon ECS tanto de no producción como de producción. 5. En la consola de Amazon Elastic Compute Cloud (Amazon EC2), verifique que se hayan creado los equilibradores de carga de aplicaciones de no producción y de producción. Registre los nombres DNS de los ALB.	

Tarea	Descripción	Habilidades requeridas
	6. En la CodePipeline consola de AWS, compruebe que `myservice1` existe una canalización con el nombre. Debe tener las etapas `Source`, `Build`, `Deploy-NonProd` y `Deploy-Prod`. La canalización también debe tener un estado `in progress`. 7. Supervise la canalización hasta que se completen todas las etapas. 8. Apruébela manualmente para la producción. 9. En una ventana del navegador, introduzca los nombres DNS de los ALB. 10. La aplicación debería mostrar `Hello World` en las URL de no producción y de producción.	

Tarea	Descripción	Habilidades requeridas
Use la canalización.	1. Abra el CodeCommit repositorio que creó anteriormente y abra el `index.js` archivo. 2. Sustituya `Hello World` por `Hello CI/CD`. 3. Guarde y confirme los cambios en la rama principal. 4. Verifique que la canalización se inicie y que el cambio pase por las etapas `Build`, `Deploy-NonProd` y `Deploy-Prod` . 5. Apruebe la producción manualmente. 6. Ahora las URL tanto de producción como de no producción deberían mostrar `Hello CICD`.	AWS DevOps, infraestructura en la nube
Repita esta épica para cada microservicio.	Repita las tareas de esta épica para crear una canalización de CI/CD para cada uno de sus microservicios.	AWS DevOps, infraestructura en la nube

Recursos relacionados

- Uso de Python con AWS CDK
- Referencia sobre Python de AWS CDK
- Creación de un servicio de AWS Fargate con AWS CDK

Información adicional

Comando de la **`cdk synth`**

```
cdk synth --context aws_account=<aws_account_number> --context
 aws_region=<aws_region> --context vpc_nonprod_id=<id_of_non_production
 VPC> --context vpc_prod_id=<id_of_production_VPC> --context
 ecssg_nonprod_id=< default_security_group_id_of_non-production_VPC>
 --context ecssg_prod_id=<default_security_group_id_of_production_VPC>
 --context code_commit_s3_bucket_for_code=<S3 bucket name> --context
 code_commit_s3_object_key_for_code=<Object_key_of_starter_code> --context
 microservice_name=<name_of_microservice>
```

`cdk deploy` command

```
cdk deploy --context aws_account=<aws_account_number> --context
 aws_region=<aws_region> --context vpc_nonprod_id=<id_of_non_production_VPC>
 --context vpc_prod_id=<id_of_production_VPC> --context ecssg_nonprod_id=<
 default_security_group_id_of_non-production_VPC> --context
 ecssg_prod_id=<default_security_group_id_of_production_VPC> --
context code_commit_s3_bucket_for_code=<S3 bucket name> --context
 code_commit_s3_object_key_for_code=<Object_key_of_starter_code> --context
 microservice_name=<name_of_microservice>
```

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Cree una arquitectura de acoplamiento flexible con microservicios mediante DevOps prácticas y AWS Cloud9

Creado por Alexandre Nardi (AWS)

Entorno: PoC o piloto	Tecnologías: sin servidor DevOps; aplicaciones web y móviles; bases de datos	Servicios de AWS: AWS Cloud9; CloudFormation AWS; Amazon DynamoDB CodePipeline; AWS CodeCommit

Resumen

Este patrón demuestra cómo desarrollar una aplicación web típica en una arquitectura sin servidor, para los desarrolladores y líderes de desarrollo que están empezando a probar sus DevOps prácticas en Amazon Web Services (AWS). Crea una aplicación de ejemplo con un escaparate y un backend para buscar y comprar libros, y proporciona un microservicio que se puede desarrollar de forma independiente. El patrón utiliza AWS Cloud9 como entorno de desarrollo, una base de datos de Amazon DynamoDB como almacén de datos y servicios de AWS como AWS y CodeBuild AWS para la funcionalidad de integración continua CodePipeline y despliegue continuo (CI/CD).

El patrón le guía a través de las siguientes actividades de desarrollo:

- Creación de un entorno de desarrollo estándar de AWS Cloud9
- Uso de CloudFormation plantillas de AWS para crear una aplicación web y un microservicio para libros
- Uso de AWS Cloud9 para modificar la interfaz, confirmar cambios y probar cambios
- Creación y prueba de un proceso de CI/CD en el microservicio
- Automatización de las pruebas unitarias

El código de este patrón se proporciona en GitHub el repositorio de AWS DevOps End-End-End-End Workshop.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Archivos del taller DevOps integral de AWS descargados a su ordenador

Importante: al crear esta aplicación de demostración en su cuenta de AWS, se crearán y consumirán recursos de AWS. Usted es responsable de asumir el costo de los servicios y recursos de AWS utilizados para crear y ejecutar la aplicación. Cuando termine su trabajo, asegúrese de eliminar todos los recursos para evitar cargos continuados. Para obtener instrucciones de limpieza, consulte la sección Epics.

Limitaciones

Este tutorial se proporciona únicamente con fines de demostración y desarrollo. Para usarlo en un entorno de producción, consulte las Prácticas recomendadas de seguridad en la documentación de AWS Identity and Access Management (IAM) y realice los cambios necesarios en roles de IAM, Amazon DynamoDB y otros servicios empleados. La aplicación web se deriva de la aplicación de demostración de AWS Bookstore; para obtener información adicional, consulte la sección Limitaciones conocidas del archivo README.

Arquitectura

La arquitectura de la aplicación de tienda de libros se ilustra en la sección Arquitectura del archivo README de la aplicación de demostración de AWS Bookstore.

Desde el punto de vista de la implementación, la aplicación de demostración Bookstore utiliza una sola CloudFormation plantilla para implementar todos los servicios y objetos en una sola pila. Este patrón introduce algunos cambios para demostrar cómo un desarrollador o equipo podría trabajar en un producto específico (Books) y actualizarlo de forma independiente del resto de la aplicación. Por este motivo, el código de este patrón separa las funciones de AWS Lambda y los objetos relacionados del microservicio Books en una segunda CloudFormation plantilla, que crea una pila de libros. Esta estructura permite ver cómo se actualiza el microservicio mediante prácticas de CI/CD. En el siguiente diagrama, el borde discontinuo identifica el microservicio Books.

Herramientas

Herramientas

- Marco Jest para realizar pruebas JavaScript
- Python 3.9

Código

El código fuente y las plantillas de este patrón están disponibles en el GitHub repositorio de AWS DevOps End-End-End-End Workshop. Antes de seguir los pasos de la sección Épica, descargue todos los archivos del repositorio a su computadora.

Nota: La sección Épica proporciona los pasos generales de este tutorial para brindarle información sobre el proceso. Para completar cada paso, consulte el archivo README en el repositorio de AWS DevOps End-End-End-End Workshop para obtener instrucciones detalladas.

El repositorio de AWS DevOps End-End-End Workshop amplía el repositorio de aplicaciones de demostración de AWS Bookstore y utiliza una versión modificada del código de arranque de AWS Cloud9 para crear el IDE de AWS Cloud9.

Prácticas recomendadas

El uso de la aplicación Bookstore es sencillo. Estas son algunas de las prácticas recomendadas:

- Al instalar la aplicación, puede usar el nombre de proyecto que prefiera o dejar el nombre predeterminado (`demobookstore`) para mayor comodidad.
- Una vez que la aplicación esté en funcionamiento, se recomienda cerrar la base de datos de Amazon Neptune si desea continuar con las pruebas un día más, ya que la instancia de la base de datos podría generar cargos adicionales. Sin embargo, tenga en cuenta que la base de datos se iniciará automáticamente transcurridos siete días.
- Para obtener información sobre el código, consulte la documentación del repositorio de la aplicación de demostración AWS Bookstore. Describe cada microservicio y tabla.
- Para obtener más información sobre las mejores prácticas, consulte Algunos desafíos si tiene tiempo... sección del archivo README del repositorio de AWS DevOps End-End-End-End Workshop. Le recomendamos que revise esta información para profundizar en las características adicionales de seguridad y practicar la disociación de servicios.

Epics

Descargar el código fuente

Tarea	Descripción	Habilidades requeridas
Descargue el código fuente de GitHub.	El código fuente y las plantillas de este patrón están disponibles en GitHub el repositorio de AWS DevOps End-End-End-End Workshop. Antes de seguir los pasos de la sección Epics, descargue todos los archivos del repositorio a su computadora. Nota: La sección Épica proporciona los pasos generales de este tutorial para brindarle información sobre el proceso. Para completar cada paso, consulte el archivo README en el repositorio de AWS DevOps End-End-End-End Workshop para obtener instrucciones detalladas. El repositorio de AWS DevOps End-End-End Workshop amplía el repositorio de aplicaciones de demostración de AWS Bookstore y utiliza una versión modificada del código de arranque de AWS Cloud9 para crear el IDE de AWS Cloud9.	Desarrollador de aplicaciones

Cree la aplicación web Bookstore y el microservicio Books

Tarea	Descripción	Habilidades requeridas
Cree las funciones de Lambda y frontend para la aplicación Bookstore.	1. Inicie sesión en la CloudFormation consola e implemente la `DemoBookstoreMainTemplate.yml` plantilla para crear la DemoBookStoreStack pila. Esto crea las funciones de frontend y Lambda que están fuera del microservicio Books. 2. En la pestaña Resultados de la pila, anota la URL del sitio web debajo de la WebApplicationetiqueta.	Desarrollador
Cree el microservicio Books.	En la CloudFormation consola, despliega la `DemoBookstoreBooksServiceTemplate.yml` plantilla para crear la DemoBooksServiceStack pila.	Desarrollador
Pruebe su aplicación.	Utilice la URL del sitio web de la DemoBookStoreStack pila para acceder a la aplicación Bookstore.	Desarrollador

Use el entorno de Cloud9 para mantener su aplicación

Tarea	Descripción	Habilidades requeridas
Cree un IDE de AWS Cloud9.	En la CloudFormation consola, implemente la `C9EnvironmentTemplate.yml` plantilla para crear un entorno AWS Cloud9.	Desarrollador, jefe de desarrollo
Cree CodeCommit repositorios.	1. Inicie sesión en la CodeCommit consola de AWS y compruebe que dispone de un `demobookstore-WebAssets` repositorio que contenga el código de la aplicación front-end. 2. Cree un repositorio para el microservicio Books llamado `demobookstore-BooksService` . 3. Clone los dos repositorios en AWS Cloud9 (`demobookstore-WebAssets` y `demobookstore-BooksService`) mediante el comando `git clone`.	Desarrollador
Cambie el código en la interfaz y compruebe el proceso.	1. Use AWS Cloud9 para realizar algunos cambios en el código de la página web. Esto actualizará el repositorio `demobookstore-WebAssets` .	Desarrollador

Tarea	Descripción	Habilidades requeridas
	2. En la CodePipeline consola de AWS, compruebe que DemoBookStore-Assets-Pipeline esté en ejecución. 3. Pruebe su aplicación web actualizándola desde el navegador (Ctrl+F5 en Firefox).	

Implemente un proceso de CI/CD para el microservicio Books

Tarea	Descripción	Habilidades requeridas
Agregue los archivos YAML para la compilación y actualización del servicio.	1. En AWS Cloud9, cargue los archivos `buildspec.yml` y `DemoBookstoreBooksServiceUpdateTemplate.yml` . • `buildspec.yml` tiene instrucciones de compilación, y también incluye instrucciones de pruebas para llevar a cabo pruebas automatizadas. Se comentan en este punto y se usarán más adelante. • `DemoBookstoreBooksServiceUpdateTemplate.yml` es una versión actualizada de `DemoBookstoreBooksServiceTe`	Desarrollador

Tarea	Descripción	Habilidades requeridas
	`mplate.yml` , que se usará en la fase de implementación del proceso. 2. Confirme y envíe los archivos.	
Cree un bucket de S3 para el proceso de compilación.	Para crear un bucket de S3, siga las instrucciones de la documentación de Amazon S3. • El nombre del bucket tiene que ser único de forma global; por ejemplo, `demobookstore-books-service-pipeline-bucket-<YYYYMMDDHHMM>` . • Desmarque la casilla Bloquear todo el acceso público y seleccione Acepto…	Desarrollador
Utilice IAM para crear un rol para la implementación. CloudFormation	Cree un rol `demobookstore-CloudFormation-role` y adjunte la política `AdministratorAccess` . En la siguiente épica, puede volver a configurar este rol con los permisos mínimos.	Desarrollador

Tarea	Descripción	Habilidades requeridas
Cree un nuevo proceso para automatizar la creación e implementación del microservicio Books.	Cree una canalización (por ejemplo, demobookstore-BooksService -Pipeline) con las etapas de confirmación, compilación e implementación, tal y como se describe en el archivo README.	Desarrollador
Pruebe su microservicio en AWS Cloud9.	Realiza un cambio en la ListBooksfunción y observa cómo funciona la canalización.	Desarrollador
Automatice la prueba unitaria de la ListBooks función Lambda.	En el IDE de AWS Cloud9, habilite la compilación para ejecutar pruebas unitarias y compruebe los resultados de las pruebas. Consulte el archivo README para obtener instrucciones.	Desarrollador

(Opcional) Implemente funciones adicionales

Tarea	Descripción	Habilidades requeridas
Haga que su solución sea segura.	Configure `demobookstore-CloudFormation-role` con los permisos mínimos y compruebe también los demás roles utilizados.	Desarrollador
Elimine las dependencias en las CloudFormation plantillas.	El método para intercambiar información entre la plantilla `DemoBookstoreMainTemplate.yml` y la plantilla `DemoBookstoreBooks`	Desarrollador

Tarea	Descripción	Habilidades requeridas
	`ServiceTemplate.yml` se basa en salidas e importaciones. Pasar valores entre estas dos plantillas añade dependencias. Para eliminar las dependencias, considere la posibilidad de usar el Almacén de parámetros de AWS Systems Manager.	
Cree un microservicio Cart.	Use el microservicio Books como ejemplo para sacar de la plantilla `DemoBookstoreMainTemplate.yml` las funciones relacionadas con el carrito de compras y crear un microservicio de carrito llamado Cart.	Desarrollador

Limpieza

Tarea	Descripción	Habilidades requeridas
Elimine los buckets de S3.	En la consola de Amazon S3, elimine los siguientes buckets asociados a la aplicación web de muestra: • Se han creado dos buckets para la aplicación de demostración de AWS Bookstore. Los nombres de los buckets comienzan con el nombre de pila que proporcionó para	Desarrollador

Tarea	Descripción	Habilidades requeridas
	AWS CloudFormation cuando creó la interfaz; por ejemplo,. DemoBookStoreStack • <YYYYMMDDHHMM>Un bucket para la canalización de compilación; por ejemplo, demobookstore-books-service-pipeline-bucket -.	
Elimine las pilas.	En la CloudFormation consola, elimina las pilas asociadas a la aplicación web de muestra: • DemoBooksServiceStack • DemoBookStoreStack La eliminación puede tardar más de 90 minutos. Si la eliminación no se realiza correctamente, realice el proceso de nuevo y elimine también los recursos manuales (por ejemplo, la VPC o las interfaces de red) en función de las notificaciones recibidas.	Desarrollador

Tarea	Descripción	Habilidades requeridas
Elimine los roles de IAM.	En la consola de IAM, elimine los siguientes roles: • `demobookstore-Cloudformation-role` • `demobookstore-BooksService-BuildProject-service-role` Para obtener step-by-step instrucciones, consulte la documentación de IAM.	Desarrollador

Recursos relacionados

- Aplicación de demostración de AWS Bookstore
- Ejemplo de arranque de AWS Cloud9
- Creación de una pila en la CloudFormation consola de AWS (CloudFormation documentación de AWS)
- Creación de un bucket (documentación de Amazon S3)

Información adicional

Para obtener step-by-step instrucciones detalladas, consulte el archivo README en el GitHub repositorio de AWS DevOps End-End-End-End Workshop.

Sobre la actualización de mayo de 2023: este patrón se ha actualizado para usar versiones más recientes de Node y Python. Hemos actualizado muchos de los paquetes del código fuente, y hemos eliminado Glyphicon, que ya no es gratuito. También hemos eliminado todas las dependencias del repositorio de aplicación de demostración de AWS Bookstore, por lo que ahora los dos repositorios pueden evolucionar de forma independiente.

Cree e inserte imágenes de Docker en Amazon ECR mediante GitHub Actions y Terraform

Creado por Ruchika Modi (AWS)

Repositorio de código: docker-ecr-actions-workflow	Entorno: producción	Tecnologías: DevOps contenedores y microservicios; infraestructura
Carga de trabajo: todas las demás cargas de trabajo	Servicios de AWS: Amazon ECR	

Resumen

Este patrón explica cómo puede crear GitHub flujos de trabajo reutilizables para crear su Dockerfile y enviar la imagen resultante a Amazon Elastic Container Registry (Amazon ECR). El patrón automatiza el proceso de creación de sus Dockerfiles mediante Terraform y Actions. GitHub Esto minimiza la posibilidad de errores humanos y reduce considerablemente el tiempo de implementación.

Una GitHub acción de envío a la rama principal del GitHub repositorio inicia el despliegue de los recursos. El flujo de trabajo crea un repositorio Amazon ECR único en función de la combinación de la GitHub organización y el nombre del repositorio. A continuación, envía la imagen de Dockerfile al repositorio de Amazon ECR.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una cuenta activa. GitHub
- Un GitHub repositorio.
- Instalación y configuración de Terraform, versión 1 o posterior.
- Un bucket de Amazon Simple Storage Service (Amazon S3) para el backend de Terraform.

- Una tabla de Amazon DynamoDB para el bloqueo y la coherencia del estado de Terraform. La tabla debe tener una clave de partición denominada `LockID` con un tipo de. `String` Si esto no está configurado, se deshabilitará el bloqueo por estado.
- Un rol de AWS Identity and Access Management (IAM) que tiene permisos para configurar el backend de Amazon S3 para Terraform. Para obtener instrucciones de configuración, consulte la documentación de Terraform.

Limitaciones

Este código reutilizable se ha probado solo con GitHub Actions.

Arquitectura

Pila de tecnología de destino

- Repositorio Amazon ECR
- GitHub Acciones
- Terraform

Arquitectura de destino

En el siguiente diagrama se ilustra lo siguiente:

1. Un usuario añade plantillas de Dockerfile y Terraform al repositorio. GitHub

2. Estas adiciones inician un GitHub flujo de trabajo de acciones.

3. El flujo de trabajo comprueba si existe un repositorio de Amazon ECR. De lo contrario, crea el repositorio en función de la GitHub organización y el nombre del repositorio.

4. El flujo de trabajo crea el Dockerfile y envía la imagen al repositorio de Amazon ECR.

Herramientas

Servicios de Amazon

- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de contenedores gestionado que es seguro, escalable y fiable.

Otras herramientas

- GitHub Actions está integrado en la GitHub plataforma para ayudarlo a crear, compartir y ejecutar flujos de trabajo en sus GitHub repositorios. Puedes usar GitHub Actions para automatizar tareas como crear, probar e implementar tu código.
- Terraform es una herramienta de código abierto de infraestructura como código (IaC) HashiCorp que le ayuda a crear y administrar infraestructuras locales y en la nube.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub Docker ECR Actions Workflow.

- Al crear GitHub acciones, los archivos de flujo de trabajo de Docker se guardan en la `/.github/workflows/` carpeta de este repositorio. El flujo de trabajo de esta solución se encuentra en el archivo workflow.yaml.
- La `e2e-test` carpeta proporciona un ejemplo de Dockerfile para consultarlo y probarlo.

Prácticas recomendadas

- Para conocer las mejores prácticas para escribir Dockerfiles, consulta la documentación de Docker.
- Utilice un punto de enlace de VPC para Amazon ECR. Los puntos de enlace de VPC funcionan con AWS PrivateLink, una tecnología que le permite acceder de forma privada a las API de Amazon ECR a través de direcciones IP privadas. Para las tareas de Amazon ECS que utilizan el tipo de lanzamiento Fargate, el punto de enlace de VPC permite que la tarea extraiga imágenes privadas de Amazon ECR sin asignar una dirección IP pública a la tarea.

Epics

Configure el proveedor y el repositorio del OIDC GitHub

Tarea	Descripción	Habilidades requeridas
Configure OpenID Connect.	Cree un proveedor de OpenID Connect (OIDC). Utilizará el proveedor en la política	Administrador de AWS DevOps, AWS general

Tarea	Descripción	Habilidades requeridas
	de confianza para el rol de IAM utilizado en esta acción. Para obtener instrucciones, consulte Configuración de OpenID Connect en Amazon Web Services en la GitHub documentación.	
Clona el GitHub repositorio.	Clona el repositorio de GitHub Docker ECR Actions Workflow en tu carpeta local: `$git clone https://github.com/aws-samples/docker-ecr-actions-workflow`	DevOps ingeniero

Personalice el flujo de trabajo GitHub reutilizable e implemente la imagen de Docker

Tarea	Descripción	Habilidades requeridas
Personalice el evento que inicia el flujo de trabajo de Docker.	El flujo de trabajo de esta solución está en workflow.yaml. Este script está configurado actualmente para implementar recursos cuando recibe el evento. `workflow_dispatch` Puede personalizar esta configuración cambiando el evento a otro flujo de trabajo principal `workflow_call` y llamando al flujo de trabajo desde él.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Personalice el flujo de trabajo.	El archivo workflow.yaml está configurado para crear un flujo de trabajo dinámico y reutilizable. GitHub Puedes editar este archivo para personalizar la configuración predeterminada, o puedes pasar los valores de entrada desde la consola de GitHub Actions si utilizas el `workflow_dispatch` evento para iniciar la implementación manualmente. • Asegúrese de especificar el ID de cuenta de AWS y la región de destino correctos. • Cree una política de ciclo de vida de Amazon ECR (consulte la política de ejemplo) y actualice la ruta predeterminada (`e2e-test/policy.json`) en consecuencia. • El archivo de flujo de trabajo requiere dos funciones de IAM como entrada: • Un rol de IAM que tiene permisos para configurar el backend de Amazon S3 para Terraform (consulte la sección Requisitos previos). Puede actualizar el nombre del rol	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	predeterminado en. `workload-assumable-role yaml`archivar en consecuencia. • Un rol de IAM que tiene permisos de acceso GitHub. Esta función también se utiliza en la política de Amazon ECR para restringir las operaciones de Amazon ECR. Para obtener más información, consulte el archivo data.tf.	
Implemente las plantillas de Terraform.	El flujo de trabajo implementa automáticamente las plantilla s de Terraform que crean el repositorio de Amazon ECR, en función del GitHub evento que haya configurado. Estas plantillas están disponibles como `.tf` archivos en la raíz del repositorio de Github.	AWS DevOps, DevOps ingeniero

Solución de problemas

Problema	Solución
Problemas o errores al configurar Amazon S3 y DynamoDB como el backend remoto de Terraform.	Siga las instrucciones de la documentación de Terraform para configurar los permisos necesarios en los recursos de Amazon S3 y DynamoDB para la configuración del backend remoto.

Problema	Solución
No se pudo ejecutar ni iniciar el flujo de trabajo con el evento. `workflow_dispatch`	El flujo de trabajo que está configurado para implementarse desde el `workflow_dispatch` evento solo funcionará si también está configurado en la rama principal.

Recursos relacionados

- Reutilizar los flujos de trabajo (GitHub documentación)
- Activación de un flujo de trabajo (documentación) GitHub

Cree y pruebe aplicaciones iOS con AWS CodeCommit CodePipeline, AWS y AWS Device Farm

Creado por Abdullahi Olaoye (AWS)

Tipo R: N/D	Fuente: procesos locales DevOps	Destino: canalización de CI/CD para el desarrollo de aplicaciones iOS en AWS
Creado por: AWS	Entorno: PoC o piloto	Tecnologías: aplicaciones web y móviles; DevOps
Servicios de AWS: AWS CodeCommit CodePipeline; AWS Device Farm		

Resumen

Este patrón describe los pasos para crear una canalización de integración y entrega continuas (CI/CD) que utilice AWS CodePipeline para crear y probar aplicaciones iOS en dispositivos reales de AWS. El patrón utiliza AWS CodeCommit para almacenar el código de la aplicación, la herramienta de código abierto de Jenkins para crear la aplicación iOS y AWS Device Farm para probar la aplicación creada en dispositivos reales. Estas tres fases se organizan juntas en una canalización mediante AWS CodePipeline.

Este patrón se basa en la publicación Creación y prueba de aplicaciones iOS y iPadOS con AWS DevOps y servicios móviles en el DevOps blog de AWS. Para obtener instrucciones más detalladas, consulte la entrada del blog.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una cuenta de desarrollador de Apple
- Servidor de compilación (macOS)

- Xcode versión 11.3 (instalada y configurada en el servidor de compilación)
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada en la estación de trabajo
- Conocimientos básicos de Git

Limitaciones

- El servidor de compilación de aplicaciones debe ejecutar macOS.
- El servidor de compilación debe tener una dirección IP pública, por lo que CodePipeline puede conectarse a ella de forma remota para iniciar las compilaciones.

Arquitectura

Pila de tecnología de origen

- Un proceso de creación de aplicaciones iOS en las instalaciones que implica el uso de un simulador o una prueba manual en dispositivos físicos

Pila de tecnología de destino

- Un CodeCommit repositorio de AWS para almacenar el código fuente de las aplicaciones
- Un servidor Jenkins para compilar aplicaciones con Xcode
- Un conjunto de dispositivos de AWS Device Farm para probar aplicaciones en dispositivos reales

Arquitectura de destino

Cuando un usuario confirma cambios en el repositorio fuente, la canalización (AWS CodePipeline) recupera el código del repositorio fuente, inicia una compilación de Jenkins y pasa el código de la aplicación a Jenkins. Tras la compilación, la canalización recupera el artefacto de compilación e inicia un trabajo de AWS Device Farm para probar la aplicación en un grupo de dispositivos.

Herramientas

- AWS CodePipeline es un servicio de entrega continua totalmente gestionado que le ayuda a automatizar sus procesos de lanzamiento para obtener actualizaciones rápidas y fiables de

las aplicaciones y la infraestructura. CodePipeline automatiza las fases de creación, prueba e implementación del proceso de lanzamiento cada vez que se produce un cambio de código, en función del modelo de lanzamiento que defina.

- AWS CodeCommit es un servicio de control de código fuente totalmente gestionado que aloja repositorios seguros basados en Git. Facilita a los equipos la colaboración en el código en un ecosistema seguro y altamente escalable. CodeCommit elimina la necesidad de operar su propio sistema de control de código fuente o preocuparse por escalar su infraestructura.
- AWS Device Farm es un servicio de pruebas de aplicaciones que le permite mejorar la calidad de sus aplicaciones web y móviles probándolas en una amplia gama de navegadores de escritorio y dispositivos móviles reales, sin tener que aprovisionar ni administrar ninguna infraestructura de pruebas.
- Jenkins es un servidor de código abierto de automatización que permite a los desarrolladores crear, probar e implementar su software.

Epics

Configure el entorno de compilación

Tarea	Descripción	Habilidades requeridas
Instalar Jenkins en el servidor de compilación que ejecuta macOS.	Jenkins se utilizará para crear la aplicación, por lo que debe instalarla antes de nada en el servidor de compilación. Para obtener instrucciones detalladas para esta y otras tareas posteriores, consulte la entrada del blog de AWS sobre cómo crear y probar aplicaciones iOS y iPadOS con AWS DevOps y servicios móviles y otros recursos en la sección Recursos relacionados al final de este patrón.	DevOps

Tarea	Descripción	Habilidades requeridas
Configure Jenkins.	Siga las instrucciones en pantalla para configurar Jenkins.	DevOps
Instale el CodePipeline complemento de AWS para Jenkins.	Este complemento debe estar instalado en el servidor de Jenkins para que Jenkins interactúe con el servicio de AWS CodePipeline .	DevOps
Cree un proyecto de estilo libre de Jenkins.	En Jenkins, cree un proyecto de estilo libre. Configure el proyecto para especificar los activadores y otras opciones de configuración de compilación.	DevOps

Configure AWS Device Farm

Tarea	Descripción	Habilidades requeridas
Cree un proyecto de Device Farm.	Abra la consola de AWS Device Farm. Cree un proyecto y un grupo de dispositivos para realizar pruebas. Consulte esta entrada de blog para obtener instrucciones.	Desarrollador

Configure el repositorio de origen

Tarea	Descripción	Habilidades requeridas
Cree un CodeCommit repositorio.	Cree un repositorio donde se almacenará el código fuente.	DevOps
Confirme el código de la aplicación en el repositorio.	Conéctese al CodeCommit repositorio que creó. Inserte el código desde el equipo local en el repositorio.	DevOps

Configure la canalización

Tarea	Descripción	Habilidades requeridas
Cree una canalización en AWS CodePipeline.	Abra la CodePipeline consola de AWS y cree una canalización. La canalización orquesta todas las fases del proceso de CI/CD. Para obtener instrucciones, consulte la entrada del blog de AWS sobre cómo crear y probar aplicaciones iOS y iPadOS con AWS DevOps y servicios móviles.	DevOps
Añada una etapa de prueba a la canalización.	Para añadir una etapa de prueba e integrarla con AWS Device Farm, edite la canalización.	DevOps
Inicie la canalización.	Para iniciar la canalización y el proceso de CI/CD, seleccione Release change.	DevOps

Vea los resultados de las pruebas de la aplicación

Tarea	Descripción	Habilidades requeridas
Revisar los resultados de la prueba.	En la consola de AWS Device Farm, seleccione el proyecto que creó y revise los resultados de las pruebas. La consola mostrará los detalles de cada prueba.	Desarrollador

Recursos relacionados

S: tep-by-step instrucciones para este patrón

- Creación y prueba de aplicaciones para iOS y iPadOS con AWS DevOps y servicios móviles (entrada del DevOps blog de AWS)

Configure AWS Device Farm

- Consola AWS Device Farm

Configure el repositorio de origen

- Crear un CodeCommit repositorio de AWS
- Conéctese a un CodeCommit repositorio de AWS

Configure la canalización

- CodePipeline Consola AWS

Recursos adicionales

- CodePipeline Documentación de AWS
- CodeCommit Documentación de AWS
- Documentación de AWS Device Farm

- Documentación de Jenkins
- Instalación de Jenkins en macOS
- CodePipeline Complemento de AWS para Jenkins
- Instalación de Xcode
- Instalación y configuración de AWS CLI
- Documentación de Git

Consulte las aplicaciones o CloudFormation plantillas de CDK de AWS para conocer las prácticas recomendadas mediante los paquetes de reglas de cdk-nag

Creado por Arun Donti

Entorno: producción	Tecnologías: seguridad DevOps, identidad, conformidad	Carga de trabajo: código abierto
Servicios de AWS: AWS CDK		

Resumen

Este patrón explica cómo puede utilizar la utilidad cdk-nag para comprobar las prácticas recomendadas de las aplicaciones del AWS Cloud Development Kit (AWS CDK) mediante una combinación de paquetes de reglas. cdk-nag es un proyecto de código abierto que se inspiró en cfn_nag. Implementa reglas en paquetes de evaluación como Biblioteca de soluciones de AWS, Ley de Portabilidad y Responsabilidad de Seguros Médicos de EE. UU (HIPAA) y Instituto Nacional de Estándares y Tecnología 800-53 mediante AWS CDK Aspects. Puede comprobar las prácticas recomendadas de sus aplicaciones de CDK de AWS utilizando las reglas de estos paquetes, detectar y corregir el código en función de las prácticas recomendadas y suprimir las reglas que no desee utilizar en sus evaluaciones.

También puede usar cdk-nag para comprobar sus CloudFormation plantillas de AWS mediante el módulo cloudformation-include.

Para obtener información sobre todos los paquetes disponibles, consulte la sección Reglas del repositorio cdk-nag. Hay paquetes de evaluación disponibles para:

- Biblioteca de soluciones de AWS
- Seguridad HIPAA
- NIST 800-53 rev. 4
- NIST 800-53 rev. 5
- La norma de seguridad de datos del sector de pagos con tarjeta (PCI DSS), versión 3.2.1

Requisitos previos y limitaciones

Requisitos previos

- Una aplicación que usa AWS CDK

Herramientas

- AWS CDK: Cloud Development Kit (AWS CDK) es un marco de desarrollo de software para definir la infraestructura de nube en el código y aprovisionarla a través de AWS. CloudFormation
- AWS CloudFormation: AWS le CloudFormation ayuda a modelar y configurar sus recursos de AWS, a aprovisionarlos de forma rápida y coherente y a gestionarlos durante todo su ciclo de vida. Facilita poder usar una plantilla para describir los recursos y sus dependencias, y lanzarlos y configurarlos juntos como una pila, en lugar de administrarlos de forma individual. Puede administrar y aprovisionar pilas en varias cuentas y regiones de AWS.

Epics

Integre cdk-nag con su aplicación CDK de AWS

Tarea	Descripción	Habilidades requeridas
Más información sobre cdk-nag.	Navegue hasta el GitHub repositorio cdk-nag y lea la documentación.	Desarrollador de aplicaciones
Instale el paquete cdk-nag en su aplicación CDK de AWS.	Para usar cdk-nag en su aplicación CDK de AWS, primero debe instalarla. cdk-nag está disponible para su descarga desde PyPI, npm y Apache Maven. NuGet Para obtener la información más reciente sobre las versiones disponibles y las ubicacion	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	es de descarga, consulte el archivo Léame del repositorio.	
NagPacksElige tu.	cdk-nag tiene diferentes paquetes de reglas llamados. NagPacks Cada uno NagPack contiene reglas que se ajustan a un estándar específico. Por ejemplo, las soluciones de AWS NagPack contienen las mejores prácticas generales y el NIST 800-53 rev 5 NagPack puede ayudar a garantizar la conformidad. Puede aplicar varios paquetes NagPacks a su aplicación y añadir y eliminar paquetes según sea necesario. Para obtener una lista de los paquetes disponibl es, consulte el archivo Léame del GitHub repositorio. Para obtener información sobre las reglas individuales de cada paquete, consulta la sección Reglas del GitHub repositorio.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Integre cdk-nag en su aplicación CDK de AWS.	Puede integrar cdk-nag en su aplicación a nivel de toda la aplicación o integrarlo en etapas o pilas individuales de su aplicación. Por ejemplo, para integrar las soluciones de AWS y la seguridad de la HIPAA NagPacks en una aplicación CDK v2 de AWS a nivel de toda la TypeScript aplicación, puede utilizar el siguiente código: `import { App, Aspects } from 'aws-cdk-lib';` `import { CdkTestStack } from '../lib/cdk-test-stack';` `import { AwsSolutionsChecks, HIPAASecurityChecks } from 'cdk-nag';` `const app = new App();` `new CdkTestStack(app, 'CdkNagDemo');` `// Simple rule informational messages` `Aspects.of(app).add(new AwsSolutionsChecks());` `// Additional explanations on the purpose of triggered rules` `Aspects.of(app).add(new HIPAASecurityChecks({ verbose: true }));`	Desarrollador de aplicaciones

Recursos relacionados

- Repositorio de código cdk-nag
- cdk-nag en Construct Hub

Configurar el acceso entre cuentas a Amazon DynamoDB

Creado por Shashi Dalmia (AWS) y Jay Enjamoori (AWS)

Entorno: producción	Tecnologías: bases de datos DevOps; seguridad, identidad y cumplimiento	Servicios de AWS: Amazon DynamoDB; AWS Identity and Access Management; AWS Lambda

Resumen

Este patrón explica los pasos para configurar el acceso entre cuentas a Amazon DynamoDB. Los servicios de Amazon Web Services (AWS) pueden acceder a las tablas de DynamoDB que se encuentran en la misma cuenta de AWS si el servicio tiene los permisos de AWS Identity and Access Management (IAM) adecuados configurados en la base de datos. Sin embargo, el acceso desde una cuenta de AWS diferente requiere configurar los permisos de IAM y establecer una relación de confianza entre las dos cuentas.

Este patrón proporciona pasos y código de muestra para demostrar cómo puede configurar las funciones de Lambda de AWS en una cuenta para leer y escribir en una tabla DynamoDB de otra cuenta.

Requisitos previos y limitaciones

- Dos cuentas de AWS activas. Este patrón hace referencia a estas cuentas como Cuenta A y Cuenta B.
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada para acceder a la cuenta A y crear la base de datos de DynamoDB. Los demás pasos de este patrón proporcionan instrucciones para usar las consolas IAM, DynamoDB y Lambda. Si planea usar AWS CLI en su lugar, configúrela para acceder a ambas cuentas.

Arquitectura

En el siguiente diagrama, AWS Lambda, Amazon EC2 y DynamoDB están todos en la misma cuenta. En este escenario, las funciones de Lambda y las instancias de Amazon Elastic Compute Cloud (Amazon EC2) pueden acceder a DynamoDB.

Si los recursos de una cuenta de AWS diferente intentan acceder a DynamoDB, es necesario configurar el acceso entre cuentas y una relación de confianza. Por ejemplo, en el siguiente diagrama, para habilitar el acceso entre DynamoDB en la cuenta A y la función de Lambda en la cuenta B, debe crear una relación de confianza entre las cuentas y conceder el acceso adecuado al servicio Lambda y a los usuarios, tal y como se describe en la sección Epics.

Herramientas

Servicios de AWS

- Amazon DynamoDB es un servicio de base de datos NoSQL totalmente administrado que ofrece un rendimiento rápido y predecible, así como una perfecta escalabilidad.
- AWS Lambda es un servicio informático que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo. Solo pagará por el tiempo de computación que consuma, no se aplican cargos cuando el código no se está ejecutando.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.

Código

Este patrón incluye código de muestra en la sección de Additional information (Información adicional) para ilustrar cómo se puede configurar una función de Lambda en la cuenta B para escribir y leer desde la tabla de DynamoDB de la cuenta A. El código se proporciona únicamente con fines ilustrativos y de prueba. Si va a implementar este patrón en un entorno de producción, utilice el código como referencia y personalícelo para su propio entorno.

Este patrón ilustra el acceso entre cuentas con Lambda y DynamoDB. También puede seguir los mismos pasos para otros servicios de AWS, pero asegúrese de conceder y configurar los permisos adecuados en ambas cuentas. Por ejemplo, si desea conceder acceso a una base de datos del Amazon Relational Database Service (Amazon RDS) en la cuenta A, cree un rol para esa base de datos y vincúlelo a una relación de confianza. En la cuenta B, si desea utilizar Amazon EC2 en lugar de AWS Lambda, cree la política y el rol de IAM correspondientes y, a continuación, adjúntelos a la instancia de EC2.

Epics

Crear una tabla en DynamoDB en la cuenta A

Tarea	Descripción	Habilidades requeridas
Crear una tabla en DynamoDB en la cuenta A	Tras configurar la CLI de AWS para la cuenta A, utilice el siguiente comando de la CLI de AWS para crear una tabla de DynamoDB: `aws dynamodb create-table \ --table-name Table-Acccount-A \ --attribute-definitions \ AttributeName=category,AttributeType=S \ AttributeName=item,AttributeType=S \ --key-schema \ AttributeName=category,KeyType=HASH \ AttributeName=item,KeyType=RANGE \ --provisioned-throughput \ ReadCapacityUnits=5,WriteCapacityUnits=5` Para obtener más información acerca de la creación de	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	tablas, consulte la documentación de DynamoDB.	

Crear un rol en la cuenta A

Tarea	Descripción	Habilidades requeridas
Crear un rol en la cuenta A	La cuenta B utilizará este rol para obtener permisos de acceso a la cuenta A. Para crear el rol: 1. Inicie sesión en la cuenta A en `https://<account-ID-for-Account-A>.signin.aws.amazon.com/console` . 2. Abra la consola de IAM en https://console.aws.amazon.com/iam/. 3. En el panel de navegación de la consola, elija Roles y, a continuación, seleccione Create role (Crear rol). 4. En Select trusted entity (Seleccione una entidad de confianza), elija AWS account (cuenta de AWS) y, en la sección Una cuenta de AWS, elija Another AWS account (Otra cuenta de AWS).	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	5. En Account ID (ID de cuenta), escriba el ID de la cuenta B. 6. Elija Next: Permissions (Siguiente: Permisos). 7. En el cuadro Filter policies (Políticas de filtro), escriba DynamoDB. 8. En la lista de políticas de DynamoDB, seleccione DB. AmazonDynamo FullAccess Nota: Esta política permite todas las acciones en DynamoDB. Como práctica recomendada de seguridad, siempre debe conceder únicamente los permisos necesarios. Para ver una lista de otras políticas que puede elegir en su lugar, consulte los Ejemplos de políticas en la documentación de IAM. 9. Seleccione Siguiente: asigne un nombre, revise y cree. 10. En Nombre del rol, introduzca un nombre exclusivo para el rol (por ejemplo, DynamoDB FullAccess - -For-Account-B) y añada una descripción del rol opcional.	

Tarea	Descripción	Habilidades requeridas
	11. Revise todas las secciones y (opcionalmente) añada metadatos al rol asociando etiquetas como pares clave-valor. 12. Elija Crear rol. Para obtener más informaci ón sobre los usuarios de IAM, consulte la documentación de IAM.	
Anote el ARN para el rol en la cuenta A.	1. En el panel de navegación de la consola de IAM, elija Roles. 2. En el cuadro de búsqueda, escriba DynamoDB FullAccess - -For-Account-B (o el nombre del rol que creó en la historia anterior) y elija el rol. 3. En la página de resumen del rol, copie el nombre de recurso de Amazon (ARN). Utilizará el ARN al configura r el código Lambda en la cuenta B.	AWS DevOps

Configure el acceso a la cuenta A desde la cuenta B

Tarea	Descripción	Habilidades requeridas
Crear una política de acceso a la cuenta A.	1. Inicie sesión en la cuenta B en `https://<account-`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`ID-for-Account-B>.signin.aws.amazon.com/console` . 2. Abra la consola de IAM en https://console.aws.amazon.com/iam/. 3. En el panel de navegación de la consola, elija Policies (Políticas) y, a continuación, elija Create policy (Crear política). 4. Seleccione la pestaña JSON. 5. Escriba o pegue lo siguiente en el documento JSON: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "sts:AssumeRole", "Resource": "arn:aws:iam::<Account-A-ID>:role/DynamoDB-FullAccess-For-Account-B" } ] }`	

Tarea	Descripción	Habilidades requeridas
	donde la propiedad `Resource` contiene el ARN del rol que creaste en la historia anterior en la cuenta A. 6. Elija Siguiente: etiquetas. 7. (Opcional) Agregar metadatos a la política al adjuntar las etiquetas como pares de clave-valor. 8. Elija Siguiente: Revisar. 9. En Nombre de la política, introduzca un nombre único para la política (por ejemplo, DynamoDB FullAccess - -Policy-in-Account-A) y añada una descripción de la política opcional. 10. Elija Crear política. Para obtener más información sobre la creación de políticas, consulte la documentación de IAM.	

Tarea	Descripción	Habilidades requeridas
Crear un rol basado en esta política.	Las funciones de Lambda de la cuenta B utilizan esta función para leer y escribir en la tabla de DynamoDB de la cuenta A. 1. En la cuenta B, En el panel de navegación de la consola de IAM, seleccione Roles y, a continuación, seleccione Create role (Crear rol). 2. En Select type of trusted entity (Seleccionar tipo de entidad de confianza), elija AWS service (Servicio de AWS). 3. En caso de uso, elija Lambda. 4. Elija Next: Permissions (Siguiente: Permisos). 5. En el cuadro Filter policies (Políticas de filtro), escriba DynamoDB. 6. En la lista de políticas de DynamoDB, seleccione DynamoDB FullAccess - - Policy-in-Account-A, que creó en la historia anterior. 7. Seleccione Siguiente: asigne un nombre, revise y cree.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	8. En Nombre del rol, introduzca un nombre exclusivo para el rol (por ejemplo, DynamoDB FullAccess - -in-Account-A) y añada una descripción del rol opcional. 9. Revise todas las secciones y (opcionalmente) añada metadatos al rol asociando etiquetas como pares clave-valor. 10. Elija Crear rol. Ahora puede asignar esta función a las funciones de Lambda en la próxima epopeya. Para obtener más informaci ón sobre los usuarios de IAM, consulte la documentación de IAM.	

Creación de una función de Lambda en la cuenta B

Tarea	Descripción	Habilidades requeridas
Cree una función de Lambda para escribir datos en DynamoDB.	1. Inicie sesión en la cuenta B en `https://<account-ID-for-Account-B>.signin.aws.amazon.com/console` .	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	2. Abra la consola en https://console.aws.amazon.com/lambda/. 3. En el panel de navegación de la consola de IAM, seleccione Funciones y, a continuación, seleccione Create function (Crear función). 4. En Nombre, escriba lambda_write_function. 5. En Runtime (Tiempo de ejecución), elija Python 3.8 o una versión más reciente. 6. En Permissions (Permisos), Change default execution role (Cambiar rol de ejecución predeterminado), elija Use an existing role (Utilizar un rol existente). 7. En Función existente, elija DynamoDB- FullAccess -in-Account-A. 8. Elija Crear función. 9. En la pestaña Código, pegue el código de ejemplo de la función de escritura Lambda que se proporciona en la sección Información adicional en este patrón. Asegúrese de proporcionar el ARN de rol correcto (de la epopeya Crear un	

Tarea	Descripción	Habilidades requeridas
	rol en la cuenta A) para el campo `RoleArn` y cambie `region_name` al lugar donde se crea la tabla de DynamoDB en la cuenta A (de la epopeya Crear una tabla de DynamoDB en la cuenta A). Si no lo hace, se producirá un error `ResourceNotFoundException`. 10. Para implementar el código, seleccione Implementar. 11. Para ejecutar la función, elija Test (Prueba). Esto le pide que configure un evento de prueba. Cree un nuevo evento con el nombre que prefiera, por ejemplo, y guarde la configuración MyTestEventForWrite. 12. Para ejecutar la función nuevamente, elija Test (Prueba). Esto ejecuta el código con el nombre del evento que ha proporcionado. 13. Compruebe el resultado de la función. Debe ser similar al resultado que se muestra en la sección sobre la función de escritura de Lambda de Información	

Tarea	Descripción	Habilidades requeridas
	adicional. Este resultado indica que la función accedió a la tabla de DynamoDB en la cuenta A y pudo escribir datos en ella. Para obtener más información sobre la creación de funciones de Lambda, consulte la documentación de Lambda.	

Tarea	Descripción	Habilidades requeridas
Crear una función de Lambda para leer datos en DynamoDB.	1. En el panel de navegación de la consola de Lambda, elija Functions (Funciones) y, a continuación, elija Create function (Crear una función). 2. En Nombre, escriba lambda_read_function. 3. En Runtime (Tiempo de ejecución), elija Python 3.8 o una versión más reciente. 4. En Permissions (Permisos), Change default execution role (Cambiar rol de ejecución predeterminado), elija Use an existing role (Utilizar un rol existente). 5. En Función existente, elija DynamoDB- FullAccess -in-Account-A. 6. Elija Crear función. 7. En la pestaña Code (Código), pegue el código de ejemplo de la función de lectura de Lambda que se proporciona en la sección Additional information (Información adicional) en este patrón. Asegúrese de proporcionar el ARN de rol correcto (de la epopeya Crear un rol en la cuenta A) para el campo `RoleArn` y	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	cambie `region_name` al lugar donde se crea la tabla de DynamoDB en la cuenta A (de la epopeya Crear una tabla de DynamoDB en la cuenta A). Si no lo hace, se producirá un error `ResourceNotFoundException`. 8. Para implementar el código, seleccione Implementar. 9. Para ejecutar la función, elija Test (Prueba). Esto le pide que configure un evento de prueba. Cree un nuevo evento con el nombre que prefiera, por ejemplo, y guarde la configuración MyTestEventForRead. 10. Para ejecutar la función nuevamente, elija Test (Prueba). Esto ejecuta el código con el nombre del evento que ha proporcionado. 11. Compruebe el resultado de la función. Debe ser similar al resultado que se muestra en la sección sobre la función de lectura de Lambda de Información adicional. Este resultado indica que la función	

Tarea	Descripción	Habilidades requeridas
	accedió a la tabla de DynamoDB en la cuenta A y pudo escribir leer que se añadieron a la tabla. Para obtener más información sobre la creación de funciones de Lambda, consulte la documentación de Lambda.	

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Elimine los recursos que creó.	Si ejecuta este patrón en un entorno de pruebas o de prueba de concepto (PoC), elimine los recursos que creó para evitar incurrir en costos. 1. En la cuenta B, elimine las dos funciones de Lambda y otros recursos que haya creado para conectarse a DynamoDB. 2. En la cuenta A, elimine la tabla de DynamoDB que creó. 3. Las políticas de IAM no tienen ningún coste, por lo que puede mantenerlas como están. Sin embargo, por motivos de seguridad , le recomendamos que	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	elimine las funciones y políticas siguientes que creó para este patrón: • Cuenta A: rol de DymamoDB-Full-Access-for-Account-A • Cuenta B: función en la cuenta A de DynamoDB FullAccess • Cuenta B: Política de DynamoDB en la cuenta A FullAccess	

Recursos relacionados

- Introducción a la CLI de AWS (documentación de la CLI de AWS)
- Configuración de la CLI de AWS (documentación de la CLI de AWS)
- Introducción a DynamoDB (documentación de DynamoDB)
- Introducción a Lambda (documentación de AWS Lambda)
- Creación de un rol para delegar permisos a un usuario de IAM (documentación de IAM)
- Creación de políticas de IAM (documentación de IAM)
- Lógica de evaluación de políticas entre cuentas (documentación de IAM)
- Referencia de los elementos de las políticas de JSON de IAM (documentación de IAM)

Información adicional

El código de esta sección se proporciona únicamente con fines ilustrativos y de prueba. Si va a implementar este patrón en un entorno de producción, utilice el código como referencia y personalícelo para su propio entorno.

La función de escritura Lambda

Código de muestra

```
import boto3
from datetime import datetime


sts_client = boto3.client('sts')
sts_session = sts_client.assume_role(RoleArn='arn:aws:iam::<Account-A ID>:role/
DynamoDB-FullAccess-For-Account-B', RoleSessionName='test-dynamodb-session')


KEY_ID = sts_session['Credentials']['AccessKeyId']
ACCESS_KEY = sts_session['Credentials']['SecretAccessKey']
TOKEN = sts_session['Credentials']['SessionToken']


dynamodb_client = boto3.client('dynamodb',
                               region_name='<DynamoDB-table-region-in-account-A',
                               aws_access_key_id=KEY_ID,
                               aws_secret_access_key=ACCESS_KEY,
                               aws_session_token=TOKEN)

def lambda_handler(event, context):
     now = datetime.now()
     date_time = now.strftime("%m/%d/%Y, %H:%M:%S")
     data = dynamodb_client.put_item(TableName='Table-Acccount-A', Item={"category":
 {"S": "Fruit"},"item": {"S": "Apple"},"time": {"S": date_time}})
     return data
```

Resultados de ejemplo:

Función de lectura Lambda

Código de muestra

```
import boto3
from datetime import datetime


sts_client = boto3.client('sts')
sts_session = sts_client.assume_role(RoleArn='arn:aws:iam::<Account-A ID>:role/
DynamoDB-FullAccess-For-Account-B', RoleSessionName='test-dynamodb-session')
```

```
KEY_ID = sts_session['Credentials']['AccessKeyId']
ACCESS_KEY = sts_session['Credentials']['SecretAccessKey']
TOKEN = sts_session['Credentials']['SessionToken']


dynamodb_client = boto3.client('dynamodb',
                               region_name='<DynamoDB-table-region-in-account-A>',
                               aws_access_key_id=KEY_ID,
                               aws_secret_access_key=ACCESS_KEY,
                               aws_session_token=TOKEN)


def lambda_handler(event, context):
     response = dynamodb_client.get_item(TableName='Table-Acccount-A', Key={'category':
{'S':'Fruit'}, 'item':{'S':'Apple'}})
     return response
```

Resultados de ejemplo:

Configure autenticación TLS mutua para aplicaciones ejecutadas en Amazon EKS

Creado por Mahendra Siddappa (AWS)

Entorno: PoC o piloto	Tecnologías: seguridad DevOps, identidad, conformidad	Servicios de AWS: Amazon EKS; Amazon Route 53

Resumen

La seguridad mutua de la capa de transporte (TLS) basada en certificado es un componente de TLS opcional que proporciona autenticación entre pares bidireccional para servidores y clientes. Con la TLS mutua, los clientes deben proporcionar un certificado X.509 durante el proceso de negociación de la sesión. El servidor utiliza este certificado para identificar y autenticar el cliente.

El TLS mutuo es un requisito común para las aplicaciones de Internet de las cosas (IoT) y se puede usar para business-to-business aplicaciones o estándares como la banca abierta.

Este patrón describe cómo configurar TLS mutua para aplicaciones ejecutadas en un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) mediante un controlador de entrada de NGINX. Puede habilitar las funciones de TLS mutua integradas para el controlador de entrada de NGINX anotando el recurso de entrada. Para obtener más información sobre las anotaciones de TLS mutua en los controladores NGINX, consulte Autenticación con certificados de cliente en la documentación de Kubernetes.

Importante: este patrón emplea certificados autofirmados. Se recomienda utilizar este patrón solo con clústeres de prueba y no en entornos de producción. Si desea usar este patrón en un entorno de producción, puede usar AWS Private Certificate Authority (AWS Private CA) o su estándar de infraestructura de clave pública (PKI) existente para emitir certificados privados.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta activa de Amazon Web Services (AWS).

- Un clúster existente de Amazon EKS.
- Interfaz de la línea de comandos de AWS (AWS CLI) versión 1.7, instalada y configurada en macOS, Linux o Windows.
- Utilidad de línea de comandos kubectl, instalada y configurada para acceder al clúster de Amazon EKS. Para obtener más información sobre esto, consulte Instalar kubectl en la documentación de Amazon EKS.
- Un nombre existente de sistema de nombres de dominio (DNS) para probar la aplicación.

Limitaciones

- Este patrón emplea certificados autofirmados. Se recomienda utilizar este patrón solo con clústeres de prueba y no en entornos de producción.

Arquitectura

Pila de tecnología

- Amazon EKS
- Amazon Route 53
- Kubectl

Herramientas

- Amazon Elastic Kubernetes Service (Amazon EKS) ayuda a ejecutar Kubernetes en AWS sin necesidad de instalar ni mantener su propio plano de control o nodos de Kubernetes.
- Amazon Route 53 es un servicio web de DNS escalable y de alta disponibilidad.
- Kubectl es una utilidad de línea de comandos que se usa para interactuar con un clúster de Amazon EKS.

Epics

Genere los certificados autofirmados

Tarea	Descripción	Habilidades requeridas
Genere el certificado y la clave del servidor.	Genere la clave y el certificado de la entidad de certificación (CA) mediante el siguiente comando. `openssl req -x509 -sha256 -newkey rsa:4096 -keyout ca.key -out ca.crt -days 356 -nodes -subj '/CN=Test Cert Authority'`	DevOps ingeniero
Genere la clave y el certificado del servidor y firme con el certificado de CA.	Genere la clave y el certificado del servidor y firme con el certificado de CA, utilizando el siguiente comando. `openssl req -new -newkey rsa:4096 -keyout server.key -out server.csr -nodes -subj '/CN= <your_domain_name> ' && openssl x509 -req -sha256 -days 365 -in server.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out server.crt` Importante: asegúrese de sustituir `<your_domain_name>` por su nombre de dominio actual.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Genere la clave y el certifica do del cliente y firme con el certificado de CA.	Genere la clave y el certificado del cliente, y firme la entidad de certificación (CA) mediante el siguiente comando. `openssl req -new -newkey rsa:4096 -keyout client.key -out client.csr -nodes -subj '/CN=Test' && openssl x509 -req -sha256 -days 365 -in client.csr -CA ca.crt -CAkey ca.key -set_serial 02 -out client.crt`	DevOps ingeniero

Implemente el controlador de entrada NGINX

Tarea	Descripción	Habilidades requeridas
Implemente el controlador de entrada de NGINX en el clúster de Amazon EKS.	Implemente el controlador de entrada de NGINX con el comando siguiente. `kubectl apply -f https://raw.githubusercontent.com/kubernetes/ingress-nginx/controller-v1.7.0/deploy/static/provider/aws/deploy.yaml`	DevOps ingeniero
Compruebe que el servicio de controlador de entrada de NGINX está en ejecución.	Compruebe que el servicio de controlador de entrada de NGINX está en ejecución	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	utilizando el siguiente comando. `kubectl get svc -n ingress-nginx` Importante: asegúrese de que el campo de dirección del servicio contenga el nombre de dominio del equilibrador de carga de red.	

Cree un espacio de nombres en el clúster de Amazon EKS para probar la TLS mutua

Tarea	Descripción	Habilidades requeridas
Cree un espacio de nombres en el clúster de Amazon EKS.	Ejecute el siguiente comando para crear un espacio de nombres llamado `mtls` en el clúster de Amazon EKS. `kubectl create ns mtls` Se implementará la aplicación de ejemplo para probar la TLS mutua.	DevOps ingeniero

Cree la implementación y el servicio de la aplicación de ejemplo

Tarea	Descripción	Habilidades requeridas
Cree la implementación y el servicio de Kubernetes en el espacio de nombres mtls.	Cree un archivo denominado `mtls.yaml` . Pegue el código siguiente en el archivo.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	<pre>kind: Deployment apiVersion: apps/v1 metadata: name: mtls-app labels: app: mtls spec: replicas: 1 selector: matchLabels: app: mtls template: metadata: labels: app: mtls spec: containers: - name: mtls-app image: hashicorp /http-echo args: - "-text=mTLS is working" --- kind: Service apiVersion: v1 metadata: name: mtls-service spec: selector: app: mtls ports: - port: 5678 # Default port for image</pre> Crea la implementación y el servicio de Kubernetes	

Tarea	Descripción	Habilidades requeridas
	en el espacio de nombres `mtls` ejecutando el siguiente comando. `kubectl create -f mtls.yaml -n mtls`	
Compruebe que se ha creado la implementación de Kubernetes.	Ejecute el siguiente comando para comprobar que la implementación se ha creado y que hay un pod en estado disponible. `kubectl get deploy -n mtls`	DevOps ingeniero
Compruebe que el servicio Kubernetes se ha creado.	Compruebe que el servicio de Kubernetes se haya creado ejecutando el siguiente comando. `kubectl get service -n mtls`	DevOps ingeniero

Cree un secreto en el espacio de nombres mtls

Tarea	Descripción	Habilidades requeridas
Cree un recurso para el recurso de entrada.	Ejecute el siguiente comando para crear un secreto en el controlador de entrada NGINX con los certificados que creó anteriormente.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`kubectl create secret generic mtls-certs --from-file=tls.crt=server.crt --from-file=tls.key=server.key --from-file=ca.crt=ca.crt -n mtls` Su secreto tiene un certificado de servidor para que el cliente identifique el servidor, y un certificado de CA para que el servidor verifique los certificados del cliente.	

Cree el recurso de entrada en el espacio de nombres mtls

Tarea	Descripción	Habilidades requeridas
Cree el recurso de entrada en el espacio de nombres mtls.	Cree un archivo denominado `ingress.yaml` . Pegue el siguiente código en el archivo (sustituya `<your_domain_name>` por su nombre de dominio actual). `apiVersion: networking.k8s.io/v1` `kind: Ingress` `metadata:` `  annotations:` `  nginx.ingress.kubernetes.io/auth-tls-verify-client: "on"` `  nginx.ingress.kubernetes.io/auth-tls-secret: mtls/mtls-certs`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	<pre> name: mtls-ingress spec: ingressClassName: nginx rules: - host: "*.<your_ domain_name>" http: paths: - path: / pathType: Prefix backend: service: name: mtls- service port: number: 5678 tls: - hosts: - "*.<your_ domain_name>" secretName: mtls- certs</pre>	
	Cree el recurso de entrada en el espacio de nombres `mtls` ejecutando el siguiente comando.	
	<pre>kubectl create -f ingress.yaml -n mtls</pre>	
	Así, el controlador de entrada de NGINX podrá enrutar el tráfico a su aplicación de muestra.	

Tarea	Descripción	Habilidades requeridas
Compruebe que se ha creado el recurso de entrada.	Compruebe que el servicio de entrada se haya creado ejecutando el siguiente comando. `kubectl get ing -n mtls` Importante: asegúrese de que la dirección del recurso de entrada muestre el equilibrador de carga creado para el controlador de entrada de NGINX.	DevOps ingeniero

Configure el DNS para que dirija el nombre de host al equilibrador de carga

Tarea	Descripción	Habilidades requeridas
Cree un registro CNAME que apunte al equilibrador de carga del controlador de entrada de NGINX.	Inicie sesión en la consola de administración de AWS, abra la consola de Amazon Route 53 y cree un registro de nombre canónico (CNAME) que apunte `mtls.<your_domain_name>` al equilibrador de carga del controlador de entrada de NGINX. Para obtener más información, consulte Creación de registros con la consola de Amazon Route 53 en la documentación de Route 53.	DevOps ingeniero

Pruebe la aplicación

Tarea	Descripción	Habilidades requeridas
Pruebe la configuración de TLS mutua sin certificados.	Ejecute el siguiente comando de la . `curl -k https://mtls.<your_domain_name>` Debería recibir la respuesta de error “400 No required SSL certificate was sent”.	DevOps ingeniero
Pruebe la configuración de TLS mutua sin certificados.	Ejecute el siguiente comando de la . `curl -k https://mtls.<your_domain_name> --cert client.crt --key client.key` Debería recibir la respuesta “mTLS is working”.	DevOps ingeniero

Recursos relacionados

- Creación de registros con la consola de Amazon Route 53
- Uso de un equilibrador de carga de red con el controlador de entrada de NGINX en Amazon EKS
- Autenticación con certificado de cliente

Crear un analizador de registros personalizado para Amazon ECS mediante un enrutador de registros Firelens

Creado por Varun Sharma (AWS)

Entorno: producción	Tecnologías: DevOps contenedores y microservicios	Carga de trabajo: todas las demás cargas de trabajo
AWS services: Amazon ECS		

Resumen

Firelens es un router de registros para Amazon Elastic Container Service (Amazon ECS) y AWS Fargate. Puede usar Firelens para enrutar los registros de contenedores desde Amazon ECS a Amazon CloudWatch y otros destinos (por ejemplo, Splunk o Sumo Logic). Firelens funciona con Fluentd o Fluent Bit como agente de registro, lo que significa que puede utilizar los parámetros de definición de tareas de Amazon ECS para enrutar los registros.

Al elegir analizar los registros en el nivel de origen, puede analizar los datos de registro y realizar consultas para responder de manera más eficiente y eficaz a los problemas operativos. Como las distintas aplicaciones tienen patrones de registro diferentes, es necesario utilizar un analizador personalizado que estructure los registros y facilite la búsqueda en el destino final.

Este patrón utiliza un router de registro Firelens con un analizador personalizado para enviar los registros CloudWatch desde una aplicación Spring Boot de muestra que se ejecuta en Amazon ECS. A continuación, puede utilizar Amazon CloudWatch Logs Insights para filtrar los registros en función de los campos personalizados generados por el analizador personalizado.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta activa de Amazon Web Services (AWS).
- Interfaz de la línea de comandos de AWS (AWS CLI), instalada y configurada en su máquina local.
- Docker, instalado y configurado en su equipo local.

- Una aplicación en contenedores existente basada en Spring Boot en Amazon Elastic Container Registry (Amazon ECR).

Arquitectura

Pila de tecnología

- CloudWatch
- Amazon ECR
- Amazon ECS
- Fargate
- Docker
- Fluent Bit

Herramientas

- Amazon ECR: Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado por AWS que es seguro, escalable y fiable.
- Amazon ECS: Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores altamente escalable y rápido que facilita la tarea de ejecutar, detener y administrar contenedores en un clúster.
- AWS Identity and Access Management (IAM): IAM es un servicio web para controlar el acceso seguro a los recursos de AWS.
- AWS CLI: la Interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que permite interactuar con los servicios de AWS mediante comandos en el intérprete de comandos de línea de comandos.
- Docker – Docker es una plataforma abierta para desarrollar, enviar y ejecutar aplicaciones.

Código

Los siguientes archivos se adjuntan a este patrón:

- `customFluentBit.zip` – Contiene los archivos para añadir el análisis y las configuraciones personalizados.
- `firelens_policy.json` – Contiene el documento de política para crear una política de IAM.
- `Task.json` – Contiene una muestra de definición de tarea para Amazon ECS.

Epics

Crear una imagen de Fluent Bit personalizada

Tarea	Descripción	Habilidades requeridas
Cree un repositorio de Amazon ECR.	Inicie sesión en la consola de administración de AWS, abra la consola de Amazon ECR y cree un repositorio llamado `fluentbit_custom` . Para obtener más informaci ón al respecto, consulte Creación de un repositorio en la documentación de Amazon ECR.	Administrador de sistemas, desarrollador
Descomprima el paquete customFluentBit .zip.	1. Descargue el paquete `customFluentBit.zip` (adjunto) en su máquina local. 2. Descomprima en el directorio `customFluentBit` ejecutando el siguiente comando: `unzip -d customFluentBit.zip` 3. El directorio contiene los siguientes archivos que	

Tarea	Descripción	Habilidades requeridas
	son necesarios para añadir el análisis y las configuraciones personalizados: • `parsers/springboot_parser.conf` – Contiene la directiva del analizador y define el patrón de expresión regular (regex) del analizador personalizado. Puede añadir el patrón de expresiones regulares para su analizador específico. • `conf/parse_springboot.conf` – Contiene el filtro y la directiva de servicio. • El Dockerfile	

Tarea	Descripción	Habilidades requeridas
Cree la imagen de Docker personalizada.	1. Cambie el directorio a `customFluentBit .` 2. Abra la consola Amazon ECR, seleccione el repositorio `fluentbit _custom` y, a continuación, seleccione Ver comandos push. 3. Cargar su proyecto 4. Una vez que finalice el proceso de carga, copie la URL de la compilación. Esta URL es obligatoria al crear un contenedor en Amazon ECS Para más informaciónf sobre esto, consulte Insertar una imagen de Docker en la documentación de Amazon ECR.	Administrador de sistemas, desarrollador

Configure el clúster de Amazon ECS

Tarea	Descripción	Habilidades requeridas
Cree un clúster de Amazon ECS.	Cree un clúster de Amazon ECS siguiendo las instrucciones de la sección sobre Plantillas exclusivas para redes de la sección Creación de un clúster de la documentación de Amazon ECS.	Administrador de sistemas, desarrollador

Tarea	Descripción	Habilidades requeridas
	Nota: Asegúrese de seleccionar Crear VPC para crear una nueva nube privada virtual (VPC) para su clúster de Amazon ECS.	

Configurar la tarea de Amazon ECS

Tarea	Descripción	Habilidades requeridas
Configurar el rol de IAM de ejecución de tareas de Amazon ECS	Cree un rol de IAM de ejecución de tareas de Amazon ECS con la política `AmazonECSTaskExecutionRolePolicy` administrada. Para obtener más información al respecto, consulte Rol de IAM de ejecución de tareas de Amazon ECS en la documentación de Amazon ECS. Nota: Asegúrese de registrar el Nombre de recurso de Amazon (ARN) del rol de IAM.	Administrador de sistemas, desarrollador
Adjunte la política de IAM al rol de IAM de ejecución de tareas de Amazon ECS.	1. Cree una política de IAM mediante el documento de política `firelens_policy.json` (adjunto). Para obtener más información al respecto, consulte Creación de políticas en la pestaña JSON de la documentación de IAM.	Administrador de sistemas, desarrollador

Tarea	Descripción	Habilidades requeridas
	2. Adjunte esta política al rol de IAM de ejecución de tareas de Amazon ECS que creó anteriormente. Para obtener más información al respecto, consulte Añadir políticas de IAM (AWS CLI) en la documentación de IAM.	

Tarea	Descripción	Habilidades requeridas
Configure la definición de tarea de Amazon ECS.	1. Actualice las siguientes secciones de la definición de tarea de muestra `Task.json` (adjunta): • Actualice `executionRoleArn` y `taskRoleArn` con el ARN del rol de IAM de ejecución de tareas • Actualice la imagen en `containerDefinitions` con la imagen de Docker personalizada de Fluent Bit que creó anteriormente • Actualice la imagen en `containerDefinitions` con el nombre de la imagen de su aplicación 2. Abra la consola de Amazon ECS, seleccione Definiciones de tareas, seleccione Crear nueva definición de tarea y, a continuación, seleccione Fargate en la página de Selección de compatibilidades. 3. Seleccione Configurar mediante Json, pegue el archivo `Task.json` actualizado en el área de texto y, a continuación, seleccione Guardar.	Administrador de sistemas, desarrollador

Tarea	Descripción	Habilidades requeridas
	4. Crear una definición de tarea. Para obtener más informaci ón al respecto, consulte Crear una definición de tarea en la documentación de Amazon ECS.	

Ejecutar la tarea de Amazon ECS

Tarea	Descripción	Habilidades requeridas
Ejecute la tarea de Amazon ECS.	En la consola de Amazon ECS, seleccione Clústeres, seleccione el clúster que creó anteriormente y, a continuac ión, ejecute la tarea independi ente. Para obtener más información al respecto, consulte Ejecutar una tarea independiente en la documentación de Amazon ECS.	Administrador de sistemas, desarrollador

Verifica los registros CloudWatch

Tarea	Descripción	Habilidades requeridas
Verifique los registros.	1. Abra la CloudWatch consola, elija Grupos de registros y, a continuac ión, elija`/aws/ecs/`	Administrador de sistemas, desarrollador

Tarea	Descripción	Habilidades requeridas
	`containerinsights/{{cluster_ARN}}/firelens/application`. 2. Verifique los registros, en particular los campos personalizados agregados por el analizador personalizado. 3. Se utiliza CloudWatch para filtrar los registros en función de los campos personalizados.	

Recursos relacionados

- Conceptos básicos de Docker para Amazon ECS
- Amazon ECS en AWS Fargate
- Configuración de parámetros de servicio básicos

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Cree una canalización y una AMI con CodePipeline un HashiCorp empaquetador

Documento creado por Akash Kumar (AWS)

Entorno: PoC o piloto	Fuente: DevOps	Destino: Imágenes de máquina de Amazon (AMI)
Tipo R: volver a alojar	Carga de trabajo: todas las demás cargas de trabajo	Tecnologías: DevOps; Modernización; aplicaciones web y móviles

Resumen

Este patrón proporciona ejemplos de código y pasos para crear una canalización en la nube de Amazon Web Services (AWS) mediante AWS CodePipeline y una imagen de máquina de Amazon (AMI) mediante HashiCorp Packer. El patrón se basa en la práctica de integración continua, que automatiza la compilación y las pruebas de código con un sistema de control de versiones basado en Git. En este patrón, se crea y se clona un repositorio de código mediante AWS CodeCommit. A continuación, cree un proyecto y configure el código fuente mediante AWS CodeBuild. Por último, cree una AMI que se asigne a su repositorio.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una AMI de Amazon Linux para lanzar instancias de Amazon Elastic Compute Cloud (Amazon EC2)
- HashiCorp Packer 0.12.3 o posterior
- Amazon CloudWatch Events (opcional)
- Amazon CloudWatch Logs (opcional)

Arquitectura

El siguiente diagrama muestra un ejemplo de código de aplicación que automatiza la creación de una AMI mediante la arquitectura de este patrón.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El desarrollador confirma los cambios de código en un repositorio CodeCommit Git privado. A continuación, se CodePipeline utiliza CodeBuild para iniciar la compilación y añadir nuevos artefactos que estén listos para su implementación en el bucket de Amazon Simple Storage Service (Amazon S3).
2. CodeBuild usa Packer para agrupar y empaquetar la AMI en función de una plantilla JSON. Si está habilitada, CloudWatch Events puede iniciar automáticamente la canalización cuando se produce un cambio en el código fuente.

Pila de tecnología

- CodeBuild
- CodeCommit
- CodePipeline
- CloudWatch Eventos (opcional)

Herramientas

- AWS CodeBuild: AWS CodeBuild es un servicio de compilación en la nube totalmente gestionado. CodeBuild compila su código fuente, ejecuta pruebas unitarias y produce artefactos que están listos para su implementación.
- AWS CodeCommit: AWS CodeCommit es un servicio de control de versiones que le permite almacenar y gestionar de forma privada los repositorios de Git en la nube de AWS. CodeCommit elimina la necesidad de administrar su propio sistema de control de código fuente o de preocuparse por escalar su infraestructura.
- AWS CodePipeline: AWS CodePipeline es un servicio de entrega continua que puede utilizar para modelar, visualizar y automatizar los pasos necesarios para lanzar su software.

- HashiCorp Packer: HashiCorp Packer es una herramienta de código abierto para automatizar la creación de imágenes de máquinas idénticas a partir de una configuración de fuente única. Packer es ligero, se ejecuta en todos los sistemas operativos principales y crea imágenes de máquinas para múltiples plataformas en paralelo.

Código

Este patrón incluye los siguientes archivos adjuntos:

- `buildspec.yml`— Este archivo se utiliza CodeBuild para construir y crear un artefacto para su despliegue.
- `amazon-linux_packer-template.json` – Este archivo usa Packer para crear una AMI de Amazon Linux.

Epics

Configurar el repositorio de código

Tarea	Descripción	Habilidades requeridas
Cree el repositorio.	Crea un CodeCommit repositorio.	Administrador de sistemas de AWS
Clonar el repositorio.	Conéctese al CodeCommit repositorio clonando el repositorio.	Desarrollador de aplicaciones
Envíe el código fuente al repositorio remoto.	1. Crear una confirmación para añadir los archivos `buildspec.yml` y `amazon-linux_packer-template.json` a su repositorio local. 2. Envía la confirmación de tu repositorio local al CodeCommit repositorio remoto.	Desarrollador de aplicaciones

Crea un CodeBuild proyecto para la aplicación

Tarea	Descripción	Habilidades requeridas
Cree un proyecto de compilación.	1. Inicie sesión en la consola de administración de AWS, abra la CodeBuild consola de AWS y, a continuación, elija Create build project. 2. En Nombre del proyecto, introduzca el nombre de su proyecto. 3. En el caso del proveedor de código fuente, elija AWS CodeCommit. 4. En Repositorio, seleccione el repositorio en el que desee compilar la canalización de código. 5. Para Imagen de entorno, elija Imagen administrada o Imagen personalizada. 6. En Operating system (Sistema operativo), elija Ubuntu. 7. Para RunTime(s), elija Estándar. 8. En Imagen, elija aws/codebuild/standard:4.0. 9. En Version de la imagen, elija Utilizar siempre la imagen más reciente para esta versión del tiempo de ejecución. 10. Para Entorno, elija Linux.	Administrador de sistemas de AWS, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	11. Seleccione la casilla Confidencial. 12. En Rol de servicio, seleccione Nuevo rol de servicio o Rol de servicio existente. 13. En Especificaciones de construcción, elija Usar un archivo de especificaciones de compilación o Insertar comandos de compilación. 14. (Opcional) En Tipo, en la sección Artefactos, seleccione Sin artefactos. 15. (Recomendado) Para cargar los registros de salida de la compilación en Logs, CloudWatch elija registros. CloudWatch 16. (Opcional) Para cargar los registros de salida de la compilación a Amazon S3, seleccione la casilla Registros de S3. 17. Elija Crear el proyecto de compilación.	

Configurar la canalización

Tarea	Descripción	Habilidades requeridas
Nombre de canalización	1. Inicie sesión en la consola de administración de AWS, abra la CodePipeline consola de AWS y, a continuación, elija Create pipeline. 2. En Nombre de la canalización, especifique un nombre para la canalización. 3. En Rol de servicio, seleccione Nuevo rol de servicio o Rol de servicio existente. 4. Escriba un nombre para el rol en Nombre de rol. 5. En la sección Configuración avanzada, en Tienda de artefactos, seleccione Ubicación predeterminada si desea que Amazon S3 cree un bucket y almacene los artefactos en el bucket. Para utilizar un bucket de S3 existente, elija Ubicación personalizada. Elija Siguiente. 6. En el caso del proveedor de código fuente, elija AWS CodeCommit. 7. En Nombre del repositorio, seleccione el repositor	Administrador de sistemas de AWS, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	io que clonó anteriorm ente. En Nombre de rama, seleccione la rama de su código fuente. 8. Para ver las opciones de detección de cambios, elige Amazon CloudWatc h Events (recomendado) para iniciar la canalizac ión o AWS CodePipeline para comprobar periódica mente si hay cambios. Elija Siguiente. 9. Como proveedor de compilación, elija AWS CodeBuild. 10. En Nombre del proyecto, elija el proyecto de compilación que creó en la epopeya Crear un CodeBuild proyecto para la aplicación. 11. Elija sus opciones de compilación y después elija Siguiente. 12. Seleccione Omitir la fase de implementación. 13. Seleccione Create pipeline.	

Recursos relacionados

- Trabajar con repositorios en AWS CodeCommit
- Trabajar con proyectos de compilación

- Trabajar con canalizaciones en CodePipeline

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Cree una canalización e implemente actualizaciones de artefactos en instancias EC2 locales mediante CodePipeline

Documento creado por Akash Kumar (AWS)

Entorno: PoC o piloto	Fuente: DevOps	Destino: Amazon EC2/en las instalaciones
Tipo R: volver a alojar	Tecnologías: DevOps; Modernización; Aplicaciones web y móviles	Servicios de AWS: AWS CodeBuild CodeCommit; AWS CodeDeploy; AWS CodePipeline

Resumen

Este patrón proporciona ejemplos de código y pasos para crear una canalización en la nube de Amazon Web Services (AWS) e implementar artefactos actualizados en instancias locales de Amazon Elastic Compute Cloud (Amazon EC2) en AWS. CodePipeline El patrón se basa en la práctica de integración continua. Esta práctica automatiza la compilación y las pruebas de código con un sistema de control de versiones basado en Git. En este patrón, se crea y se clona un repositorio de código mediante AWS CodeCommit. A continuación, crea un proyecto y configura el código fuente mediante AWS CodeBuild. Por último, debe crear la aplicación y configurar su entorno de destino para las instancias EC2 locales mediante AWS. CodeDeploy

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Etiquetas definidas por el usuario para identificar las instancias EC2 durante la implementación
- CodeDeploy agente, instalado en instancias EC2
- El software de tiempo de ejecución necesario, instalado en las instancias EC2
- Amazon Corretto 8 para el kit de desarrollo de Java
- Servidor web Apache Tomcat, instalado
- Amazon CloudWatch Events (opcional)

- Un par de claves para iniciar sesión en el servidor web (opcional)
- Un proyecto de aplicación Apache Maven para una aplicación web

Arquitectura

El siguiente diagrama muestra un ejemplo de aplicación web Java que se implementa en instancias en las instalaciones EC2 mediante la arquitectura de este patrón.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El desarrollador confirma los cambios de código en un repositorio CodeCommit Git privado.
2. CodePipeline CodeBuild se utiliza para iniciar la compilación y añadir nuevos artefactos que estén listos para su implementación en el bucket de Amazon Simple Storage Service (Amazon S3).
3. CodePipeline utiliza el CodeDeploy agente para preinstalar todas las dependencias necesarias para los cambios en los artefactos de implementación.
4. CodePipeline utiliza el CodeDeploy agente para implementar los artefactos del bucket de S3 en las instancias de EC2 de destino. Si está habilitada, CloudWatch Events puede iniciar automáticamente la canalización cuando se produce un cambio en el código fuente.

Pila de tecnología

- CodeBuild
- CodeCommit
- CodeDeploy
- CodePipeline
- CloudWatch Eventos (opcional)

Herramientas

- AWS CodeBuild es un servicio de compilación totalmente gestionado que le ayuda a compilar código fuente, ejecutar pruebas unitarias y producir artefactos listos para su implementación. CodeBuild compila su código fuente, ejecuta pruebas unitarias y produce artefactos listos para su implementación.

- AWS CodeCommit es un servicio de control de versiones que le ayuda a almacenar y gestionar repositorios de Git de forma privada, sin necesidad de gestionar su propio sistema de control de código fuente.
- AWS CodeDeploy automatiza las implementaciones en Amazon Elastic Compute Cloud (Amazon EC2) o en instancias locales, funciones de AWS Lambda o servicios de Amazon Elastic Container Service (Amazon ECS).
- AWS le CodePipeline ayuda a modelar y configurar rápidamente las diferentes etapas de una versión de software y a automatizar los pasos necesarios para publicar cambios de software de forma continua.

Código

Este patrón incluye los siguientes archivos adjuntos:

- `buildspec.yml`— Este archivo especifica las acciones necesarias CodeBuild para construir y crear un artefacto para su despliegue.
- `appspec.yml`— Este archivo especifica las acciones necesarias para crear una aplicación y configurar un entorno de destino para las instancias de EC2 locales. CodeDeploy
- `install_dependencies.sh` – Este archivo instala las dependencias del servidor web Apache Tomcat.
- `start_server.sh` – Este archivo inicia el servidor web Apache Tomcat.
- `stop_server.sh` – Este archivo detiene el servidor web Apache Tomcat.

Epics

Configurar el repositorio de código

Tarea	Descripción	Habilidades requeridas
Cree el repositorio.	Cree un CodeCommit repositorio.	Administrador de sistemas de AWS
Clonar el repositorio.	Conéctese al CodeCommit repositorio clonando el repositorio.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Envíe el código fuente al repositorio remoto.	1. Crear una confirmación para añadir los archivos `buildspec.yml` y `appspec.yml` a su repositorio local. 2. Envía la confirmación de tu repositorio local al CodeCommit repositorio remoto.	Desarrollador de aplicaciones

Crea un CodeBuild proyecto para la aplicación

Tarea	Descripción	Habilidades requeridas
Cree un proyecto de compilación.	1. Inicie sesión en la consola de administración de AWS, abra la CodeBuild consola de AWS y, a continuación, elija Create build project. 2. En Nombre del proyecto, introduzca el nombre de su proyecto. 3. En el caso del proveedor de código fuente, elija AWS CodeCommit. 4. En Repositorio, seleccione el repositorio en el que desee compilar la canalización de código. 5. Para Imagen de entorno, elija Imagen administrada o Imagen personalizada.	Administrador de AWS, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	6. En Operating system (Sistema operativo), elija Amazon Linux 2. 7. Para RunTime(s), elija Estándar. 8. En Imagen, elija aws/codebuild/amazonlinux2-aarch64-standard:2.0. 9. En Version de la imagen, elija Utilizar siempre la imagen más reciente para esta versión del tiempo de ejecución. 10. En Rol de servicio, seleccione Nuevo rol de servicio o Rol de servicio existente. 11. En Especificaciones de construcción, elija Usar un archivo de especificaciones de compilación o Insertar comandos de compilación. 12. (Opcional) Seleccione Añadir artefacto para configurar los artefactos. 13. (Opcional) Para subir los registros de salida de compilaciones a Amazon CloudWatch, selecciona CloudWatch logs. 14. Elija Crear el proyecto de compilación.	

Configurar la implementación de artefactos para instancias EC2 en las instalaciones

Tarea	Descripción	Habilidades requeridas
Cree la aplicación.	1. Inicie sesión en la consola de administración de AWS, abra la CodeDeploy consola de AWS y, a continuación, seleccione Crear aplicación. 2. En Nombre de la aplicación, especifique un nombre para su aplicación. 3. Para Plataforma de computación, elija EC2/en las instalaciones. 4. Seleccione Crear aplicación y, a continuación, seleccione Crear grupo de implementación. 5. En Nombre del grupo de implementación, introduzca un nombre. 6. Cree un rol de servicio para CodeDeploy. Nota: El rol de servicio debe tener permisos para conceder CodeDeploy acceso al entorno de destino. 7. En Rol de servicio, seleccione la función de servicio que creó en el paso 6. 8. Para el Tipo de implementación, seleccione Presencia	Administrador de sistemas de AWS, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	l o Azul/Verde en función de los requisitos de su empresa. 9. Para la Configuración del entorno, seleccione las opciones que cumplan sus requisitos empresariales. 10. (Opcional) Cree un grupo objetivo para su balanceador de carga por separado en la consola Amazon EC2 y, a continuación, regrese a la página Crear grupo de implementación de la consola de CodeDeploy y AWS para elegir el balanceador de carga y el grupo objetivo. 11. Elija Crear grupo de implementación.	

Configurar la canalización

Tarea	Descripción	Habilidades requeridas
Cree la canalización.	1. Inicie sesión en la consola de administración de AWS, abra la CodePipeline consola de AWS y, a continuación, elija Create pipeline.	Administrador de sistemas de AWS, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	2. En Nombre de la canalización, especifique un nombre para la canalización. 3. En Rol de servicio, seleccione Nuevo rol de servicio o Rol de servicio existente. 4. Escriba un nombre para el rol en Nombre de rol. 5. En la sección Configuración avanzada, en Tienda de artefactos, seleccione Ubicación predeterminada si desea que Amazon S3 cree un bucket y almacene los artefactos en el bucket. Para utilizar un bucket de S3 existente, elija Ubicación personalizada. Elija Siguiente. 6. En el caso del proveedor de código fuente, elija AWS CodeCommit. 7. En Nombre del repositorio, seleccione el repositorio que clonó anteriormente. En Nombre de rama, seleccione la rama de su código fuente. 8. Para ver las opciones de detección de cambios, elige Amazon CloudWatch Events (recomendado)	

Tarea	Descripción	Habilidades requeridas
	o AWS CodePipeline. Elija Siguiente. 9. Como proveedor de compilación, elija AWS CodeBuild. 10. En Nombre del proyecto, elija el proyecto de compilación que creó en la sección Crear un CodeBuild proyecto para la aplicación de este patrón. 11. Elija sus opciones de compilación y después elija Siguiente. 12. Para Deploy provider, elija AWS CodeDeploy. 13. Seleccione un nombre de aplicación y un grupo de implementación y, a continuación, seleccione Siguiente. 14. Seleccione Create pipeline.	

Recursos relacionados

- Trabajar con repositorios en AWS CodeCommit
- Trabajar con proyectos de compilación
- Trabajar con aplicaciones en CodeDeploy
- Trabajando con tuberías en CodePipeline

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Crear automáticamente canalizaciones de CI dinámicas para proyectos de Java y Python

Creado por Aromal Raj Jayarajan (AWS), Amarnath Reddy (AWS), MAHESH RAGHUNANDANAN (AWS) y Vijesh Vijayakumaran Nair (AWS)

Repositorio de código: automated-ci-pipeline-creation	Entorno: PoC o piloto	Tecnologías: infraestructura DevOps, sin servidor, nativa de la nube
Carga de trabajo: todas las demás cargas de trabajo	Servicios de AWS: AWS CodeBuild CodePipeline; AWS Lambda; AWS Step Functions; AWS CodeCommit	

Resumen

Este patrón muestra cómo crear automáticamente canalizaciones de integración continua (CI) dinámicas para proyectos de Java y Python mediante las herramientas para desarrolladores de AWS.

A medida que las pilas de tecnología se diversifican y las actividades de desarrollo aumentan, puede resultar difícil crear y mantener canalizaciones de CI que sean coherentes en toda la organización. Al automatizar el proceso en AWS Step Functions, puede asegurarse de que sus canalizaciones de CI sean coherentes en su uso y enfoque.

Para automatizar la creación de canalizaciones de CI dinámicas, este patrón utiliza las siguientes entradas variables:

- Lenguaje de programación (solo Java o Python)
- Nombre de canalización
- Etapas de canalización requeridas

Nota: Step Functions orquestra la creación de canalizaciones mediante varios servicios de AWS. Para obtener más información sobre los servicios de AWS que se utilizan en esta solución, consulte la sección Herramientas de este patrón.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un bucket de Amazon S3 en la misma región de AWS en la que se está implementando esta solución
- Un director de AWS Identity and Access Management (IAM) que cuente con los CloudFormation permisos de AWS necesarios para crear los recursos necesarios para esta solución

Limitaciones

- Este patrón solo admite proyectos de Java y Python.
- Los roles de IAM aprovisionadas en este patrón siguen el principio del privilegio mínimo. Los permisos de los roles de IAM deben actualizarse en función de los recursos específicos que necesite crear su canalización de CI.

Arquitectura

Pila de tecnología de destino

- AWS CloudFormation
- AWS CodeBuild
- AWS CodeCommit
- AWS CodePipeline
- IAM
- Amazon Simple Storage Service (Amazon S3)
- AWS Systems Manager
- AWS Step Functions
- AWS Lambda
- Amazon DynamoDB

Arquitectura de destino

El siguiente diagrama muestra un ejemplo de flujo de trabajo para crear automáticamente canalizaciones de CI dinámicas para proyectos de Java y Python mediante las herramientas para desarrolladores de AWS.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un usuario de AWS proporciona los parámetros de entrada para la creación de canalizaciones de CI en formato JSON. Esta entrada inicia un flujo de trabajo de Step Functions (máquina de estados) que crea una canalización de CI mediante las herramientas para desarrolladores de AWS.
2. Una función de Lambda lee una carpeta denominada input-reference, que está almacenada en un bucket de Amazon S3 y, a continuación, genera un archivo buildspec.yml. Este archivo generado define las etapas de la canalización de CI y se vuelve a almacenar en el mismo bucket de Amazon S3 que almacena las referencias de los parámetros.
3. Step Functions comprueba las dependencias del flujo de trabajo de creación de canalizaciones de CI para detectar cualquier cambio y actualiza la pila de dependencias según sea necesario.
4. Step Functions crea los recursos de la canalización de CI en una CloudFormation pila, que incluye un CodeCommit repositorio, un CodeBuild proyecto y una CodePipeline canalización.
5. La CloudFormation pila copia el código fuente de muestra de la pila de tecnología seleccionada (Java o Python) y el archivo buildspec.yml en el repositorio. CodeCommit
6. Los detalles del tiempo de ejecución de la canalización de CI se almacenan en una tabla de DynamoDB.

Automatizar y escalar

- Este patrón se utiliza únicamente en un entorno de desarrollo único. Se requieren cambios de configuración para su uso en varios entornos de desarrollo.
- Para añadir compatibilidad con más de una CloudFormation pila, puedes crear plantillas adicionales. CloudFormation Para obtener más información, consulte Introducción a AWS CloudFormation en la CloudFormation documentación.

Herramientas

Herramientas

- AWS Step Functions es un servicio de orquestación sin servidor que le permite combinar funciones de Lambda AWS y otros servicios de AWS para crear aplicaciones esenciales desde el punto de vista empresarial.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS CodeBuild es un servicio de compilación totalmente gestionado que le ayuda a compilar código fuente, ejecutar pruebas unitarias y producir artefactos listos para su implementación.
- AWS CodeCommit es un servicio de control de versiones que le ayuda a almacenar y gestionar repositorios de Git de forma privada, sin necesidad de gestionar su propio sistema de control de código fuente.
- AWS le CodePipeline ayuda a modelar y configurar rápidamente las diferentes etapas de una versión de software y a automatizar los pasos necesarios para publicar cambios de software de forma continua.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Key Management Service (AWS KMS) facilita poder crear y controlar claves criptográficas para proteger los datos.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- El Almacén de parámetros de AWS Systems Manager proporciona un almacenamiento seguro y jerárquico para administrar los datos de configuración y los secretos.

Código

El código de este patrón está disponible en el GitHub automated-ci-pipeline-creationrepositorio. El repositorio contiene las CloudFormation plantillas necesarias para crear la arquitectura de destino descrita en este patrón.

Prácticas recomendadas

- No introduzcas credenciales (secretos), como identificadores o contraseñas, directamente en las CloudFormation plantillas o en las configuraciones de acciones de Step Functions. Si lo hace, la información se mostrará en los registros de DynamoDB. En su lugar, utilice AWS Secrets Manager para configurar y almacenar secretos. A continuación, consulte los secretos almacenados en Secrets Manager dentro de las CloudFormation plantillas y las configuraciones de acciones de Step Functions, según sea necesario. Para obtener más información, consulte ¿Qué es AWS Secrets Manager? en la documentación de AWS Secrets Manager.
- Configure el cifrado del lado del servidor para los CodePipeline artefactos almacenados en Amazon S3. Para obtener más información, consulte Configurar el cifrado del lado del servidor para los artefactos almacenados en Amazon S3 CodePipeline en la CodePipeline documentación.
- Aplique permisos de privilegios mínimos al configurar roles de IAM. Para obtener más información, consulte Aplicar permisos de privilegio mínimo en la documentación de IAM.
- Asegúrese de que su bucket de Amazon S3 no sea de acceso público. Para obtener más información, consulte Configurar la configuración de bloqueo de acceso público para sus buckets de S3 en la documentación de Amazon S3.
- Asegúrese de activar el control de versiones de su bucket de Amazon S3. Para más información, consulte Uso de control de versiones en buckets de S3 en la documentación de Amazon S3.
- Utilice IAM Access Analyzer al configurar las políticas de IAM. La herramienta proporciona recomendaciones prácticas para ayudarle a crear políticas de IAM seguras y funcionales. Para más información, consulte Utilizar el analizador de acceso de AWS Identity and Access Management en la documentación de IAM.
- Cuando sea posible, defina condiciones de acceso específicas al configurar las políticas de IAM.
- Activa el CloudWatch registro de Amazon con fines de supervisión y auditoría. Para obtener más información, consulta ¿Qué es Amazon CloudWatch Logs? en la CloudWatch documentación.

Epics

Configurar los requisitos previos

Tarea	Descripción	Habilidades requeridas
Crear un bucket de Amazon S3.	Cree un depósito de Amazon S3 (o utilice uno existente	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	) para almacenar las CloudFormation plantillas, el código fuente y los archivos de entrada necesarios para la solución. Para obtener más informaci ón, consulte Paso 1: Crear su primer bucket de S3 en la documentación de Amazon S3. Nota: El bucket de Amazon S3 debe estar en la misma región de AWS en la que está implementando la solución.	
Clona el GitHub repositorio.	Clone el GitHub automated-ci-pipeline-creationrepositor io ejecutando el siguiente comando en una ventana de terminal: `git clone https://g ithub.com/aws-samp les/automated-ci-p ipeline-creation.git` Para obtener más informaci ón, consulte Clonación de un repositorio en la GitHub documentación.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Cargue la carpeta Solution Templates del GitHub repositorio clonado a su bucket de Amazon S3.	Copie el contenido de la carpeta Solution-Templates clonada y cárguelo en el bucket de Amazon S3 que creó. Para obtener más información, consulte Carga de objetos en la documentación de Amazon S3. Nota: Asegúrese de cargar únicamente el contenido de la carpeta Solution-Templates . Puede cargar los archivos únicamente en el nivel raíz del bucket de Amazon S3.	AWS DevOps

Implementar la solución

Tarea	Descripción	Habilidades requeridas
Cree una CloudFormation pila para implementar la solución mediante el archivo template. yml del repositorio clonado. GitHub	1. Inicie sesión en la consola de administración de AWS y, a continuación, abra la CloudFormation consola de AWS. 2. Seleccione Crear pila. Se muestra una lista desplegable. 3. En la lista desplegable, seleccione Con nuevos recursos (standard). Se abre la página Crear pila.	Administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	4. En la sección Especificar plantilla elija casilla allado de Cargar un archivo de plantilla. 5. Seleccione Choose file (Elegir archivo). A continuación, vaya a la carpeta raíz del GitHub repositorio clonado y seleccione el archivo template.yml. A continuación, seleccione Abrir. 6. Seleccione Siguiente. Se abrirá la página Especificar los detalles de la pila. 7. En la sección Parámetros, especifique los siguientes parámetros: • Para S3 TemplateBucketName, introduzca el nombre del bucket de Amazon S3 que creó anteriormente, que contiene el código fuente y las referencias de esta solución. Asegúrese de que el parámetro de nombre de bucket esté en minúsculas. • En DynamoDBTable, introduzca un nombre para la tabla de DynamoDB que crea la pila. CloudFormation	

Tarea	Descripción	Habilidades requeridas
	• Para StateMachineName, introduzca un nombre para la máquina de estados Step Functions que crea la CloudFormation pila. 8. Seleccione Siguiente. Se abre la página Configurar opciones de pilas. 9. En la página Configurar opciones de pila, elija Siguiente. No cambie ninguno de los valores predeterminados. Se abre la página de Revisión. 10. Revise la configuración de creación de la pila. A continuación, seleccione Crear pila para lanzar su pila. Nota: Mientras se está creando la pila, aparecerá en la página Stacks (Pilas) con un estado CREACIÓN_EN_PROGRESO. Asegúrese de esperar a que el estado de la pila cambie a CREATE_COMPLETE antes de completar los pasos restantes de este patrón.	

Prueba de la configuración

Tarea	Descripción	Habilidades requeridas
Ejecute la función que ha creado.	1. Inicie sesión en la consola de administración de AWS y, a continuación, abra la consola Step Functions. 2. Abra la función escalonada que ha creado. 3. Seleccione Iniciar ejecución . A continuación, introduzc a los valores de entrada para el flujo de trabajo en formato JSON (consulte los siguientes ejemplos de entradas). 4. Seleccione Iniciar ejecución . Formato JSON `{ "details": { "tech_stack": "Name of the Tech Stack (python/java)", "project_name": "Name of the Project that you want to create with", "pre_build": "Choose the step if it required in the buildspec.yml file i.e., yes/no", "build": "Choose the step if it required in`	Administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas

```
 the buildspec.yml file
 i.e., yes/no",
    "post_build":
 "Choose the step if
 it required in the
 buildspec.yml file
 i.e., yes/no",
    "reports": "Choose
 the step if it required
 in the buildspec.yml
 file i.e., yes/no",
  }
}
```

Ejemplo de entrada JSON en Java

```
{
  "details": {
    "tech_stack":
 "java",
    "project_name":
 "pipeline-java-pjt",
    "pre_build": "yes",
    "build": "yes",
    "post_build":
 "yes",
    "reports": "yes"
  }
}
```

Ejemplo de entrada JSON en Python

```
{
  "details": {
    "tech_stack":
 "python",
```

Tarea	Descripción	Habilidades requeridas
	<pre>"project_name": "pipeline-python-p jt", "pre_build": "yes", "build": "yes", "post_build": "yes", "reports": "yes" } }</pre>	
Confirme que se creó el CodeCommit repositorio para la canalización de CI.	1. Inicie sesión en la consola de administración de AWS y, a continuación, abra la CodeCommit consola. 2. En la página Repositorios, compruebe que el nombre del CodeCommit repositorio que ha creado aparece en la lista de repositorios. Al nombre del repositorio se le añade lo siguiente: -Repo pipeline-java-pjt 3. Abre el CodeCommit repositorio y comprueba que el código fuente del ejemplo junto con los archivos buildspec.yml se hayan enviado a la rama principal.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Consulte los recursos CodeBuild del proyecto.	1. Inicie sesión en la consola de administración de AWS y, a continuación, abra la CodeBuild consola. 2. En la página Crear proyectos, compruebe que el nombre del CodeBuild proyecto que ha creado aparece en la lista de proyectos. Al nombre del proyecto se le añade lo siguiente: pipeline-java-pjt - Build 3. Seleccione el nombre de su CodeBuild proyecto para abrirlo. A continuación, revise y valide las siguiente s configuraciones: • Configuración del proyecto • Origen • Entorno • Buildspec • Configuración por lotes • Artefactos	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Valide las CodePipeline etapas.	1. Inicie sesión en la consola de administración de AWS y, a continuación, abra la CodePipeline consola. 2. En la página Canalizaciones, verifique que el nombre de la canalización que ha creado aparece en la lista de canalizaciones. Al nombre de la canalización se le añade lo siguiente: pipeline-java-pjt -Pipeline 3. Seleccione el nombre de su canalización para abrir la canalización. A continuación, revise y valide cada etapa de la canalización, incluyendo la Confirmación y la Implementación.	AWS DevOps
Confirme que la canalización de CI se haya ejecutado correctamente.	1. En la CodePipeline consola, en la página Pipelines, seleccione el nombre de la canalización para ver el estado de la canalización. 2. Verifique que cada etapa de la canalización tenga el estado de Logrado.	AWS DevOps

Eliminación de sus recursos

Tarea	Descripción	Habilidades requeridas
Elimine la pila de recursos CloudFormation.	Elimine la pila de recursos de la canalización de CI CloudFormation. Para obtener más informaci ón, consulte Eliminar una pila en la CloudFormation consola de AWS en la CloudFormation documentación. Nota: Asegúrese de eliminar la pila denominada <project_ name>-stack.	AWS DevOps
Elimine las dependencias de la canalización de CI en Amazon S3 y CloudFormation.	1. Vacíe el depósito de Amazon S3 denominado DeploymentArtifactBucket. Para más información, consulte Vaciar un bucket en la documentación de Amazon S3. 2. Elimine la pila de dependencias de la canalización de CI CloudFormation. Para obtener más informaci ón, consulte Eliminar una pila en la CloudFormation consola de AWS en la CloudFormation documenta ción.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	Nota: Asegúrese de eliminar la pila nombrada pipeline-creation-dependencies-stack.	
Elimine el bucket de plantilla de Amazon S3.	Elimine el bucket de Amazon s3 que creó en la sección Configurar los requisitos previos de este patrón, que almacena las plantillas de esta solución. Para obtener más informaci ón, consulte Eliminación de un bucket en la documentación de Amazon S3.	AWS DevOps

Recursos relacionados

- Creación de una máquina de estados de Step Functions que utilice Lambda (documentación de AWS Step Functions)
- AWS Step Functions WorkFlow Studio (documentación de AWS Step Functions)
- DevOps y AWS
- ¿Cómo CloudFormation funciona AWS? (CloudFormation documentación de AWS)
- CI/CD completo con AWS, CodeCommit AWS CodeDeploy, CodeBuild AWS y AWS (entrada del blog de CodePipeline AWS)
- Cuotas de IAM y AWS STS, requisitos de nombre y límites de caracteres (documentación de IAM)

Despliega canarios de CloudWatch Synthetics con Terraform

Creado por Dhrubajyoti Mukherjee (AWS) y Jean-Francois Landreau (AWS)

Repositorio de código: despliega CloudWatch Synthetics Canaries con Terraform	Entorno: producción	Tecnologías: productividad empresarial DevOps, desarrollo y pruebas de software, infraestructura, aplicaciones web y móviles
Servicios de AWS: Amazon CloudWatch; Amazon S3; Amazon SNS; Amazon VPC; AWS Identity and Access Management		

Resumen

Es importante validar el estado de un sistema desde la perspectiva del cliente y confirmar que los clientes pueden conectarse. Esto resulta más difícil cuando los clientes no llaman constantemente al punto de conexión. Amazon CloudWatch Synthetics admite la creación de canarios, que pueden probar puntos de conexión públicos y privados. Al usar valores controlados, puede conocer el estado de un sistema incluso si no está en uso. Estos valores controlados son scripts de Node.js Puppeteer o scripts de Python Selenium.

Este patrón describe cómo usar HashiCorp Terraform para implementar canarios que prueben puntos de enlace privados. Incorpora un script de Puppeteer que comprueba si una URL devuelve `200-OK`. A continuación, el script de Terraform se puede integrar con el script que implementa el punto de conexión privado. También puede modificar la solución para monitorear puntos de conexión públicos.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de Amazon Web Services (AWS) activa con una nube privada virtual (VPC) y subredes privadas

- La URL del punto de conexión al que se puede acceder desde las subredes privadas
- Terraform instalado en el entorno de implementación

Limitaciones

La solución actual funciona para las siguientes versiones de tiempo de ejecución de CloudWatch Synthetics:

- syn-nodejs-puppeteer-3.4
- syn-nodejs-puppeteer-3,5
- syn-nodejs-puppeteer-3,6
- syn-nodejs-puppeteer-3,7

Cuando se publiquen nuevas versiones de tiempo de ejecución, podría tener que actualizar la solución actual. También tendrá que modificar la solución para mantenerse al día con las actualizaciones de seguridad.

Versiones de producto

- Terraform 1.3.0

Arquitectura

Amazon CloudWatch Synthetics se basa en CloudWatch Lambda y Amazon Simple Storage Service (Amazon S3). Amazon CloudWatch ofrece un asistente para crear los canarios y un panel de control que muestra el estado de los canarios. La función de Lambda ejecuta el script. Amazon S3 almacena los registros y las capturas de pantalla de las ejecuciones de valores controlados.

Este patrón simula un punto de conexión privado a través de una instancia de Amazon Elastic Compute Cloud (Amazon EC2) implementada en las subredes de destino. La función de Lambda requiere interfaces de red elásticas en la VPC en la que se implementa el punto de conexión privado.

En el diagrama se muestra lo siguiente:

1. El valor controlado de Synthetics inicia la función de Lambda del valor controlado.
2. La función de Lambda del valor controlado se conecta a la interfaz de red elástica.

3. La función de Lambda del valor controlado monitorea el estado del punto de conexión.
4. Synthetics Canary envía los datos de ejecución al bucket y las métricas del S3. CloudWatch
5. Se inicia una CloudWatch alarma en función de las métricas.
6. La CloudWatch alarma inicia el tema Amazon Simple Notification Service (Amazon SNS).

Herramientas

Servicios de AWS

- Amazon le CloudWatch ayuda a monitorizar las métricas de sus recursos de AWS y las aplicaciones que ejecuta en AWS en tiempo real.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esta red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS. Este patrón utiliza puntos de conexión de VPC e interfaces de red elásticas.

Otros servicios

- HashiCorp Terraform es una herramienta de código abierto de infraestructura como código (IaC) que le ayuda a usar el código para aprovisionar y administrar la infraestructura y los recursos de la nube. Este patrón utiliza Terraform para implementar la infraestructura.
- Puppeteer es una biblioteca de Node.js. El motor de ejecución CloudWatch Synthetics utiliza el marco Puppeteer.

Código

La solución está disponible en el repositorio en la nube. GitHub watch-synthetics-canary-terraform
Para obtener más información, consulte la sección Información adicional.

Epics

Implementar la solución para monitorear una URL privada

Tarea	Descripción	Habilidades requeridas
Reunir los requisitos para monitorear la URL privada.	Reúna la definición completa de la URL: dominio, parámetros y encabezados. Para comunicarse de forma privada con Amazon S3 y Amazon CloudWatch, utilice puntos de enlace de VPC. Observe cómo se puede acceder a la VPC y a las subredes desde el punto de conexión. Tenga en cuenta la frecuencia de las ejecuciones de valores controlados.	Arquitecto de la nube, administrador de redes
Modifique la solución existente para monitorear la URL privada.	Modifique el archivo `terraform.tfvars` : • `name`: el nombre de su valor controlado. • `runtime_version` : la versión de tiempo de ejecución del valor controlado. Recomendamos usar syn-nodejs-puppeteer -3.7. • `take_screenshot` : si se debe hacer una captura de pantalla.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	• `api_hostname` : el nombre de host del punto de conexión que se monitorea. • `api_path`: la ruta del punto de conexión que se monitorea. • `vpc_id`: la ID de la VPC que utiliza la función de Lambda del valor controlado. • `subnet_ids` : las ID de subred que utiliza la función de Lambda del valor controlado. • `frequency` : la frecuencia de ejecución del valor controlado en minutos. • `alert_sns_topic` — El tema de SNS al que se envía la notificación de CloudWatch alarma.	

Tarea	Descripción	Habilidades requeridas
Implementar y utilizar la solución.	Para implementar la solución, haga lo siguiente: 1. Inicialice Terraform desde el directorio `cloudwatch-synthetics-canary-terraform` de su entorno de desarrollo. `terraform init` 2. Planifique y revise los cambios. `terraform plan` 3. Implemente la solución. `terraform apply`	Arquitecto de nube, ingeniero DevOps

Solución de problemas

Problema	Solución
La eliminación de los recursos aprovisionados se bloquea.	Elimine manualmente la función de Lambda del valor controlado, la interfaz de red elástica correspondiente y el grupo de seguridad, en ese orden.

Recursos relacionados

- Uso del monitoreo sintético
- Supervise los puntos de enlace de API Gateway con Amazon CloudWatch Synthetics (entrada del blog)

Información adicional

Artefactos del repositorio

Los artefactos del repositorio tienen la siguiente estructura.

```
.
### README.md
### main.tf
### modules
#   ### canary
#   ### canary-infra
### terraform.tfvars
### tf.plan
### variable.tf
```

El archivo `main.tf` contiene el módulo principal e implementa dos módulos secundarios:

- `canary-infra` implementa la infraestructura necesaria para los valores controlados.
- `canary` implementa los valores controlados.

Los parámetros de entrada de la solución se encuentran en el archivo `terraform.tfvars`. Puede utilizar el siguiente código de ejemplo para crear un valor controlado.

```
module "canary" {
    source = "./modules/canary"
    name   = var.name
    runtime_version = var.runtime_version
    take_screenshot = var.take_screenshot
    api_hostname = var.api_hostname
    api_path = var.api_path
    reports-bucket = module.canary_infra.reports-bucket
    role = module.canary_infra.role
    security_group_id = module.canary_infra.security_group_id
    subnet_ids = var.subnet_ids
    frequency = var.frequency
    alert_sns_topic = var.alert_sns_topic
}
```

A continuación, se muestra el archivo .var correspondiente.

```
name   = "my-canary"
runtime_version = "syn-nodejs-puppeteer-3.7"
take_screenshot = false
api_hostname = "mydomain.internal"
api_path = "/path?param=value"
vpc_id = "vpc_id"
subnet_ids = ["subnet_id1"]
frequency = 5
alert_sns_topic = "arn:aws:sns:eu-central-1:111111111111:yyyyy"
```

Limpieza de la solución

Si está haciendo las pruebas en un entorno de desarrollo, puede limpiar la solución para evitar acumular costos.

1. En la consola de administración de AWS, vaya a la consola de Amazon S3. Vacíe el bucket de Amazon S3 creado por la solución. Asegúrese de realizar una copia de seguridad de los datos en caso necesario.
2. En su entorno de desarrollo, ejecute el comando `destroy` desde el directorio `cloudwatch-synthetics-canary-terraform`.

   ```
   terraform destroy
   ```

Implemente una canalización de CI/CD para microservicios de Java en Amazon ECS

Creado por Vijay Thompson (AWS) y Sandeep Bondugula (AWS)

Entorno: PoC o piloto	Tecnologías: DevOps contenedores y microservicios	Servicios de AWS: AWS CodeBuild; Amazon EC2 Container Registry; Amazon ECS; AWS Fargate; AWS CodePipeline

Resumen

Este patrón lo guía a través de los pasos para implementar una canalización de integración y entrega continuas (CI/CD) para microservicios de Java en un clúster de Amazon Elastic Container Service (Amazon ECS) existente mediante AWS. CodeBuild Cuando el desarrollador confirma los cambios, se inicia la canalización de CI/CD y comienza el proceso de creación. CodeBuild Cuando se completa la compilación, el artefacto se envía a Amazon Elastic Container Registry (Amazon ECR) y la última compilación de Amazon ECR se recoge y se envía al servicio Amazon ECS.

Requisitos previos y limitaciones

Requisitos previos

- Una aplicación de microservicios Java existente que se ejecuta en Amazon ECS
- Familiaridad con AWS CodeBuild y AWS CodePipeline

Arquitectura

Pila de tecnología de origen

- Microservicios Java que se ejecutan en Amazon ECS
- Repositorio de código en Amazon ECR
- AWS Fargate

Arquitectura de origen

Pila de tecnología de destino

- Amazon ECR
- Amazon ECS
- AWS Fargate
- AWS CodePipeline
- AWS CodeBuild

Arquitectura de destino

Automatizar y escalar

CodeBuild `buildspec.yml`archivo:

```
version: 0.2

phases:
  pre_build:
    commands:
      - echo Logging in to Amazon ECR...
      - aws --version
      - $(aws ecr get-login --region $AWS_DEFAULT_REGION --no-include-email)
      - REPOSITORY_URI=$AWS_ACCOUNT_ID.dkr.ecr.$AWS_DEFAULT_REGION.amazonaws.com/
$IMAGE_REPO
      - COMMIT_HASH=$(echo $CODEBUILD_RESOLVED_SOURCE_VERSION | cut -c 1-7)
      - IMAGE_TAG=build-$(echo $CODEBUILD_BUILD_ID | awk -F":" '{print $2}')
  build:
    commands:
      - echo Build started on `date`
      - echo building the Jar file
      - mvn clean install
      - echo Building the Docker image...
      - docker build -t $REPOSITORY_URI:$BUILD_TAG .
      - docker tag $REPOSITORY_URI:$BUILD_TAG $REPOSITORY_URI:$IMAGE_TAG
  post_build:
```

```
    commands:
      - echo Build completed on `date`
      - echo Pushing the Docker images...
      - docker push $REPOSITORY_URI:$BUILD_TAG
      - docker push $REPOSITORY_URI:$IMAGE_TAG
      - echo Writing image definitions file...
      - printf '[{"name":"%s","imageUri":"%s"}]' $DOCKER_CONTAINER_NAME
 $REPOSITORY_URI:$IMAGE_TAG > imagedefinitions.json
      - cat imagedefinitions.json
artifacts:
    files:
     - imagedefinitions.json
     - target/DockerDemo.jar
```

Herramientas

Servicios de AWS

- AWS CodeBuild es un servicio de compilación totalmente gestionado que le ayuda a compilar código fuente, ejecutar pruebas unitarias y producir artefactos listos para su implementación. AWS CodeBuild escala de forma continua y procesa varias compilaciones al mismo tiempo, por lo que sus compilaciones no se quedan en la cola.
- AWS le CodePipeline ayuda a modelar y configurar rápidamente las diferentes etapas de una versión de software y a automatizar los pasos necesarios para publicar cambios de software de forma continua. Puede integrar AWS CodePipeline con servicios de terceros GitHub, como o utilizar un servicio de AWS, como AWS CodeCommit o Amazon ECR.
- Amazon Elastic Container Registry (Amazon ECR) es un registro de contenedores de Docker completamente administrado que facilita el almacenamiento, la administración y la implementación de imágenes de contenedores de Docker. Amazon ECR está integrado con Amazon ECS para simplificar su development-to-production flujo de trabajo. Amazon ECR aloja las imágenes en una arquitectura escalable y de alta disponibilidad, lo que le permite implementar contenedores para sus aplicaciones con fiabilidad. La integración con AWS Identity and Access Management (IAM) proporciona un control a nivel de recursos de cada repositorio.
- Amazon Elastic Container Service (Amazon ECS) es un servicio de orquestación de contenedores de alto rendimiento y escalado que admite contenedores de Docker y facilita la ejecución y el escalado de aplicaciones en contenedores en AWS. Amazon ECS elimina la necesidad de instalar y operar su propio software de orquestación de contenedores, administrar y escalar un clúster de máquinas virtuales o programar contenedores en esas máquinas virtuales.

- AWS Fargate es un motor de cómputo para Amazon ECS que le permite ejecutar contenedores sin tener que administrar servidores o clústeres. Con AWS Fargate ya no tendrá que aprovisionar, configurar ni escalar clústeres de máquinas virtuales para ejecutar los contenedores. De esta manera, se elimina la necesidad de elegir tipos de servidores, decidir cuándo escalar los clústeres u optimizar conjuntos de clústeres.

Otras herramientas

- Docker le ayuda a crear, probar y entregar aplicaciones en paquetes llamados contenedores.
- Git es un sistema de control de versiones distribuido que rastrea los cambios en el código fuente durante el desarrollo del software. Está diseñado para coordinar el trabajo entre los programadores, pero se puede utilizar para realizar un seguimiento de los cambios en cualquier conjunto de archivos. Sus objetivos incluyen la velocidad, la integridad de los datos y la compatibilidad con flujos de trabajo distribuidos y no lineales. También puede utilizar AWS CodeCommit como alternativa a Git.

Epics

Configurar el proyecto de compilación en AWS CodeBuild

Tarea	Descripción	Habilidades requeridas
Cree un proyecto de CodeBuild construcción.	En la CodeBuild consola de AWS, cree un proyecto de compilación y especifique su nombre.	Administrador de sistemas de AWS, desarrollador de aplicaciones
Seleccione el origen.	Este patrón usa Git como repositorio de código, así que elige GitHub de la lista de opciones disponibles. Elige un repositorio público o desde tu GitHub cuenta.	Administrador de sistemas de AWS, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Seleccione un repositorio.	Seleccione el repositorio desde el que desea compilar el código.	Administrador de sistemas de AWS, desarrollador de aplicaciones
Seleccione el entorno.	Puede seleccionar una imagen de una lista de imágenes administradas u optar por una imagen personalizada mediante Docker. Este patrón utiliza la siguiente imagen administr ada: • Amazon Linux 2 • Tiempo de ejecución: estándar • Versión de la imagen: 1.0	Administrador de sistemas de AWS, desarrollador de aplicaciones
Elija un rol de servicio.	Puede crear un rol de servicio o seleccionarlo de una lista de roles existentes.	Administrador de sistemas de AWS, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Añada variables de entorno.	En la sección Configuración adicional, configure las siguientes variables de entorno: • AWS_DEFAULT_REGION para la región de AWS predeterminada • AWS_ACCOUNT_ID para el número de cuenta de usuario • IMAGE_REPO para el repositorio privado de Amazon ECR • BUILD_TAG para la versión de la compilación (la última compilación es el valor de esta variable) • DOCKER_CONTAINER_NAME para el nombre del contenedor de la tarea Estas variables son marcadores de posición en el archivo `buildspec.yml` y se sustituirán por sus valores respectivos.	Administrador de sistemas de AWS, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Cree un archivo buildspec.	Puede crear un archivo `buildspec.yml` en la misma ubicación como `pom.xml` y añadir la configuración que se proporciona en este patrón, o bien utilizar el editor buildspec en línea y añadir la configuración. Configure las variables de entorno con los valores adecuados siguiendo los pasos que se indican.	Administrador de sistemas de AWS, desarrollador de aplicaciones
Configure el proyecto para los artefactos.	(Opcional) Configure el proyecto de compilado de los artefactos, si es necesario.	Administrador de sistemas de AWS, desarrollador de aplicaciones
Configura Amazon CloudWatch Logs.	(Opcional) Configure Amazon CloudWatch Logs para el proyecto de compilación, si es necesario. Este paso es opcional, pero recomendable.	Administrador de sistemas de AWS, desarrollador de aplicaciones
Configure los registros de Amazon S3.	(Opcional) Configure los registros de Amazon Simple Storage Service (Amazon S3) para el proyecto de compilación, si desea almacenar los registros.	Administrador de sistemas de AWS, desarrollador de aplicaciones

Configurar la canalización en AWS CodePipeline

Tarea	Descripción	Habilidades requeridas
Crear una canalización.	En la CodePipeline consola de AWS, cree una canalización y especifique su nombre. Para obtener más información sobre la creación de una canalización, consulte la CodePipeline documentación de AWS.	Administrador de sistemas de AWS, desarrollador de aplicaciones
Seleccione un rol de servicio.	Cree un rol de servicio o selecciónelo de una lista de roles existentes. Si va a crear un rol de servicio, proporcione un nombre para el rol y seleccione la opción CodePipeline para crearlo.	Administrador de sistemas de AWS, desarrollador de aplicaciones
Elija una tienda de artefactos.	En la configuración avanzada, si desea que Amazon S3 cree un bucket y almacene los artefactos en él, utilice la ubicación predeterminada para el almacén de artefactos. O bien, seleccione una ubicación personalizada y especifique un bucket existente. También puede optar por cifrar el artefacto mediante una clave de cifrado.	Administrador de sistemas de AWS, desarrollador de aplicaciones
Especificar el proveedor de código fuente.	En Proveedor de origen, elija GitHub (versión 2).	Administrador de sistemas de AWS, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Seleccione el repositorio y la rama del código.	Si no ha iniciado sesión, proporcione los detalles de conexión a los que desea conectarse y GitHub, a continuación, seleccione el nombre del repositorio y el nombre de la rama.	Administrador de sistemas de AWS, desarrollador de aplicaciones
Opciones de detección de cambios.	Seleccione Iniciar la canalización en el cambio del código fuente y pase a la página siguiente.	Administrador de sistemas de AWS, desarrollador de aplicaciones
Seleccione un proveedor de compilación.	Como proveedor de compilación, elija AWS y CodeBuild, a continuación, proporcione la región de AWS y los detalles del nombre del proyecto de compilación. En Tipo de compilación, elija Compilación única.	Administrador de sistemas de AWS, desarrollador de aplicaciones
Elija un proveedor de implementación.	En Proveedor de implementación, elija Amazon ECS. Elija el nombre del clúster, el nombre del servicio, el archivo de definiciones de imágenes, si lo hubiera, y un valor de tiempo de espera de implementación, si es necesario. Elija Crear canalización.	Administrador de sistemas de AWS, desarrollador de aplicaciones

Recursos relacionados

- Documentación de AWS ECS
- Documentación de AWS ECR
- CodeBuild Documentación de AWS
- CodeCommit Documentación de AWS
- CodePipeline Documentación de AWS
- Cree un canal de entrega continua para las imágenes de sus contenedores con Amazon ECR como origen (entrada del blog)

Utilice AWS CodeCommit y AWS CodePipeline para implementar una canalización de CI/CD en varias cuentas de AWS

Documento creado por Kirankumar Chandrashekar (AWS)

Entorno: PoC o piloto	Tecnologías: DevOps	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: AWS CodeCommit; AWS CodePipeline		

Resumen

Este patrón le muestra cómo implementar una canalización de integración y entrega continuas (CI/CD) para sus cargas de trabajo de código de aplicación en cuentas de Amazon Web Services (AWS) independientes para flujos de trabajo de desarrollador DevOps, puesta en escena y producción.

Puede utilizar una estrategia de varias cuentas de AWS para proporcionar un alto nivel de aislamiento de recursos o seguridad, optimizar los costos y separar el flujo de trabajo de producción.

El código de su aplicación permanece idéntico en todas estas cuentas de AWS independientes y se mantiene en un CodeCommit repositorio central de AWS alojado en su DevOps cuenta. Tus cuentas de desarrollador, de puesta en escena y de producción tienen ramas de Git independientes en este CodeCommit repositorio.

Por ejemplo, cuando el código se envía a la rama de Git para desarrolladores de tu CodeCommit repositorio central, Amazon EventBridge de tu DevOps cuenta notifica los cambios EventBridge en el repositorio a tu cuenta de desarrollador. En su cuenta de desarrollador, AWS CodePipeline y la fase de origen entran en `InProgress` estado. La etapa de origen se configura desde la rama de Git para desarrolladores en el CodeCommit repositorio central y CodePipeline asume una función de servicio para la DevOps cuenta.

El contenido del CodeCommit repositorio de la rama de desarrolladores se carga en un almacén de artefactos en un bucket de Amazon Simple Storage Service (Amazon S3) y se cifra con una clave de AWS Key Management Service (AWS KMS). Cuando el estado de la etapa de origen cambie a `Succeeded` in CodePipeline, el código pasará a la siguiente etapa de la ejecución del proceso.

Requisitos previos y limitaciones

Requisitos previos

- Cuentas de AWS existentes para cada entorno necesario (desarrolladorDevOps, puesta en escena y producción). AWS Organizations puede alojar estas cuentas.
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada.

Arquitectura

Pila de tecnología

- AWS CodeBuild
- AWS CodeCommit
- AWS CodePipeline
- Amazon EventBridge
- AWS Identity y Access Management (IAM)
- AWS KMS
- AWS Organizations
- Amazon S3

Herramientas

- AWS CodeBuild: CodeBuild es un servicio de integración continua totalmente gestionado que compila el código fuente, ejecuta pruebas y produce paquetes de software listos para su implementación.
- AWS CodeCommit: CodeCommit es un servicio de control de código fuente totalmente gestionado que aloja repositorios seguros basados en Git
- AWS CodePipeline: CodePipeline es un servicio de entrega continua totalmente gestionado que le ayuda a automatizar sus procesos de lanzamiento para obtener actualizaciones rápidas y fiables de las aplicaciones y la infraestructura.
- Amazon EventBridge: EventBridge es un servicio de bus de eventos sin servidor para conectar sus aplicaciones con datos de diversas fuentes.

- AWS Identity and Access Management (IAM): IAM es un servicio web que ayuda a controlar de forma segura el acceso a los recursos de AWS.
- AWS KMS: AWS Key Management Service (AWS KMS) le ayuda a crear y administrar claves criptográficas y a controlar su uso en una amplia gama de servicios de AWS y en sus aplicaciones.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet.

Epics

Cree recursos en su cuenta DevOps de AWS

Tarea	Descripción	Habilidades requeridas
Cree un CodeCommit repositorio.	Inicie sesión en la consola de administración de AWS de su DevOps cuenta y abra la CodeCommit consola. Cree un repositorio y configure todas las ramas de Git necesarias para sus cuentas de AWS de desarrollador, provisional y de producción. Para obtener más información sobre esta y otras explicaciones, consulte la sección “Recursos relaciona dos”.	DevOps ingeniero
Cree credenciales de acceso para el CodeCommit repositor io.	En la consola de IAM, cree credenciales de acceso para que los desarrolladores de aplicaciones puedan introduci r y extraer el código base de la aplicación del CodeCommit repositorio.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Cree un rol de IAM para los roles CodePipeline de servicio.	En la consola de IAM, cree un rol de IAM que puedan utilizar todos sus roles de CodePipeline servicio para acceder al repositorio central. CodeCommit	Administrador de la nube
Configure las EventBridge reglas para sus otras cuentas de AWS.	En la EventBridge consola de Amazon, configure reglas para enviar notificac iones sobre los cambios relevantes EventBridge en el CodeCommit repositorio a las cuentas de AWS individuales de desarrollador, provisional y de producción.	Administrador de la nube
Crear una clave de AWS KMS.	En la consola de AWS KMS, cree una clave de KMS que permita CodePipeline a sus cuentas de AWS individuales de desarrollador, provisional y de producción cifrar y descifrar artefactos.	Administrador de la nube

Cree recursos en sus otras cuentas de AWS

Tarea	Descripción	Habilidades requeridas
EventBridge Configúrelo para recibir eventos de la cuenta de DevOps AWS.	Inicie sesión en la consola de administración de AWS de una de sus cuentas de AWS individuales (desarrollador, provisional o de producción). En la EventBridge consola	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	de Amazon, configúrala EventBridge para recibir los eventos de cambio de CodeCommit repositorio de tu DevOps cuenta.	
Crear un bucket de S3.	En la consola Amazon S3, cree un bucket de S3 para almacenar CodePipeline los artefactos.	Administrador de la nube
Cree todos los recursos de AWS necesarios para CodePipeline las etapas.	Cree todos los demás recursos de AWS que requerirán las CodePipel ine etapas. Estos recursos variarán en función del rol de cada cuenta de AWS en su canalización de CI/CD.	Administrador de la nube
Crear un rol de IAM.	En la consola de IAM, cree un rol de IAM para el rol de CodePipeline servicio. Esta función de servicio debe poder asumir la función de IAM en la DevOps cuenta para acceder al repositorio. CodeCommit	Administrador de la nube
Cree una canalización en CodePipeline.	En la CodePipeline consola, crea una canalización. Luego, crea una etapa de origen que apunte al CodeCommi t repositorio de la DevOps cuenta para su rama de Git individual.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Repita los pasos para todas sus cuentas de AWS.	Repita estos pasos para todas las cuentas de AWS que necesite como parte de su estrategia de CI/CD.	Administrador de la nube

Recursos relacionados

Cree recursos en su cuenta DevOps de AWS

- Cree un CodeCommit repositorio
- Configura un CodeCommit repositorio
- Crea y comparte una rama en tu CodeCommit repositorio
- Crea credenciales de acceso para el CodeCommit repositorio
- Cree un rol de IAM para los roles CodePipeline de servicio
- Configure la regla en EventBridge
- Crear una clave de AWS KMS
- Configure las políticas y funciones de la cuenta para CodePipeline

Cree recursos en sus otras cuentas de AWS

- Actívela EventBridge para recibir eventos de su cuenta de DevOps AWS
- Cree un depósito de S3 para CodePipeline artefactos
- Cree todos los demás recursos de AWS necesarios para CodePipeline las etapas
- Cree un rol de IAM para el rol CodePipeline de servicio
- Cree una canalización en CodePipeline
- Cree una canalización CodePipeline que utilice recursos de otra cuenta de AWS

Otros recursos

- Establecer su entorno de AWS de mejores prácticas
- Autenticación y control de acceso para CodeCommit

Implemente un firewall con AWS Network Firewall y AWS Transit Gateway

Creado por Shrikant Patil (AWS)

Repositorio de códigos: aws-network-firewall-deployment - with-transit-gateway	Entorno: PoC o piloto	Tecnologías: redes DevOps; seguridad, identidad y conformidad
Servicios de AWS: AWS Network Firewall; AWS Transit Gateway; Amazon VPC; Amazon CloudWatch		

Resumen

Este patrón muestra cómo implementar un firewall mediante AWS Network Firewall y AWS Transit Gateway. Los recursos de Network Firewall se implementan mediante una CloudFormation plantilla de AWS. Network Firewall escala automáticamente con el tráfico de la red y puede admitir cientos de miles de conexiones, por lo que no tiene que preocuparse por crear y mantener su propia infraestructura de seguridad de red. Una puerta de enlace de tránsito es un centro de tránsito de red que puede utilizar para interconectar las nubes virtuales privadas (VPC) y las redes en las instalaciones.

En este patrón, también aprenderá a incluir una VPC de inspección en la arquitectura de su red. Por último, este patrón explica cómo utilizar Amazon CloudWatch para supervisar la actividad de su firewall en tiempo real.

Consejo: se recomienda evitar el uso de una subred de Network Firewall para implementar otros servicios de AWS. Esto se debe a que Network Firewall no puede inspeccionar el tráfico de fuentes o destinos dentro de la subred de un firewall.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa

- Permisos de rol y política de AWS Identity and Access Management (IAM)
- CloudFormation permisos de plantilla

Limitaciones

Es posible que tenga problemas con el filtrado de dominios y que necesite un tipo diferente de configuración. Para obtener más información, consulte grupos de reglas de lista de dominios con estado en AWS Network Firewall en la documentación de Network Firewall.

Arquitectura

Pila de tecnología

- Amazon CloudWatch Logs
- Amazon VPC
- AWS Network Firewall
- AWS Transit Gateway

Arquitectura de destino

El siguiente diagrama muestra cómo utilizar Network Firewall y Transit Gateway para inspeccionar el tráfico:

La arquitectura incluye los siguientes componentes:

- Su aplicación está alojada en las VPC de dos radios. Las VPC se supervisan mediante Network Firewall.
- La VPC de salida tiene acceso directo a la puerta de enlace de Internet, pero no está protegida por Network Firewall.
- La VPC de inspección es donde se implementa Network Firewall.

Automatizar y escalar

Puede usarlo CloudFormationpara crear este patrón mediante el uso de la infraestructura como código.

Herramientas

Servicios de AWS

- Amazon CloudWatch Logs le ayuda a centralizar los registros de todos sus sistemas, aplicaciones y servicios de AWS para que pueda supervisarlos y archivarlos de forma segura.
- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esta red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.
- AWS Network Firewall es un servicio de detección y prevención de intrusiones y de firewall de red con estado y administrado para nubes privadas virtuales (VPC) en la nube de AWS.
- AWS Transit Gateway es un concentrador central que conecta las VPC y las redes en las instalaciones.

Código

El código de este patrón está disponible en el repositorio de implementación de GitHub AWS Network Firewall con Transit Gateway. Puede usar la CloudFormation plantilla de este repositorio para implementar una sola VPC de inspección que utilice Network Firewall.

Epics

Cree la VPC radial y la VPC de inspección

Tarea	Descripción	Habilidades requeridas
Prepare e implemente la CloudFormation plantilla.	1. Descarga la `cloudformation/aws_nw_fw.yml` plantilla del GitHub repositorio. 2. Actualice la plantilla con sus valores. 3. Implemente la plantilla.	AWS DevOps

Cree la puerta de enlace de tránsito y las rutas

Tarea	Descripción	Habilidades requeridas
Cree una puerta de enlace de tránsito.	1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon VPC. 2. En el panel de navegación, elija Transit Gateways (Puertas de enlace de tránsito). 3. Elija Create Transit Gateway (Crear puerta de enlace de tránsito). 4. En Name tag (Etiqueta de nombre), puede escribir un nombre para la puerta de enlace de tránsito. 5. En Description (Descripción), escriba una descripción para la puerta de enlace de tránsito. 6. En número de sistema autónomo (ASN) de Amazon, deje el valor ASN predeterminado. 7. Seleccione la opción de compatibilidad con DNS. 8. Seleccione la opción de compatibilidad con VPN ECMP. 9. Seleccione la opción de asociación de tablas de enrutamiento predeterm	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	inada. Esta opción asocia automáticamente las conexiones de puerta de enlace de tránsito a la tabla de enrutamiento predeterm inada de la puerta de enlace de tránsito. 10. Seleccione la opción de propagación de tablas de enrutamiento predeterm inada. Esta opción propaga automáticamente las conexiones de puerta de enlace de tránsito a la tabla de enrutamiento predeterm inada de la puerta de enlace de tránsito. 11. Elija Create Transit Gateway (Crear puerta de enlace de tránsito).	

Tarea	Descripción	Habilidades requeridas
Cree conexiones de puerta de enlace de tránsito.	Cree una conexión de puerta de enlace de tránsito para lo siguiente: • Una conexión de inspección en la subred de LA VPC de inspección y Transit Gateway • Una conexión de SpokeVPCA en la VPCA radial y en la subred privada • Una conexión de SpokeVPCB en la VPCB radial y en la subred privada • Una conexión de EgressVPC en la VPC de salida y en la subred privada	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Cree una tabla de enrutamiento de la puerta de enlace de tránsito.	1. Cree una tabla de enrutamiento de la puerta de enlace de tránsito para la VPC radial.. Esta tabla de enrutamiento debe estar asociada a todas las VPC distintas de la VPC de inspección. 2. Cree una tabla de enrutamiento de la puerta de enlace de tránsito para el firewall. Esta tabla de enrutamiento debe estar asociada a la VPC solamente. 3. Añada una ruta a la tabla de enrutamiento de la puerta de enlace de tránsito para el firewall. • Para `0.0.0/0`, utilice la conexión EgressVPC. • Para el bloque CIDR de SpokeVPCA, utilice la conexión SpokeVPC1. • Para el bloque CIDR de SpokeVPCB, utilice el adjunto SpokeVPC2. 4. Añada una ruta a la tabla de enrutamiento de la puerta de enlace de tránsito para la VPC radial. Para `0.0.0/0`, utilice la	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	conexión de la VPC de inspección.	

Cree el firewall y las rutas

Tarea	Descripción	Habilidades requeridas
Crea un firewall en la VPC de inspección.	1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon VPC. 2. En el panel de navegación, en Firewall de red, seleccione Firewalls. 3. Seleccione Crear firewall. 4. En Nombre, introduzca el nombre que desea utilizar para identificar este firewall. No puede cambiar el nombre de un firewall después de crearlo. 5. Para la VPC, seleccione la VPC de inspección. 6. En Zona de disponibilidad y subred, seleccione la zona y la subred del firewall que identificó. 7. En la sección Política de firewall asociada, elija Asociar una política de firewall existente y, a continuación, seleccione la	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	política de firewall que creó anteriormente. 8. Seleccione Crear firewall.	

Tarea	Descripción	Habilidades requeridas
Cree una política de firewall.	1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon VPC. 2. En el panel de navegació n, en Network Firewall, elija Políticas de firewall. 3. En la página Describir la política de firewall, elija Crear política de firewall. 4. En Nombre, introduzca el nombre que desea utilizar para la política de firewall. Utilizará el nombre para identificar la política cuando la asocie al firewall más adelante en este patrón. No se puede cambiar el nombre de una política de firewall después de crearla. 5. Elija Siguiente. 6. En la página Añadir grupos de reglas, en la sección Grupos de reglas sin estado, elija Añadir grupos de reglas sin estado. 7. En el cuadro de diálogo Añadir desde grupos de reglas existentes, active la casilla de verificación del grupo de reglas sin estado que creó anteriormente. Seleccione Añadir grupos	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	de reglas. Nota: En la parte inferior de la página, el contador de capacidad de la política de firewall muestra la capacidad consumida al añadir este grupo de reglas junto a la capacidad máxima permitida para una política de firewall. 8. Establece la acción predeterminada sin estado en Reenviar a reglas con estado. 9. En la sección Grupo de reglas con estado, elija Añadir grupos de reglas con estado y, a continuación, active la casilla de verificación del grupo de reglas con estado que creó anteriormente. Seleccione Añadir grupos de reglas. 10. Elija Siguiente para recorrer el resto del asistente de configuración y, a continuación, elija Crear política de firewall.	

Tarea	Descripción	Habilidades requeridas
Actualizar las tablas de enrutamiento de la VPC.	Tablas de enrutamiento de la VPC de inspección 1. En la tabla de enrutamiento de subred ANF (`Inspection-ANFRT `), añada `0.0.0/0` al ID de Transit Gateway. 2. En la tabla de enrutamiento de subred de Transit Gateway (`Inspection-TGWRT`), añada `0.0.0/0` al EgressVPC. Tabla de enrutamiento de SpokeVPCA En la tabla de enrutamiento privada, añada `0.0.0.0/0` al ID de Transit Gateway. Tabla de enrutamiento de VPCB radial En la tabla de enrutamiento privada, añada `0.0.0.0/0` al ID de Transit Gateway. Tablas de enrutamiento de la VPC de egreso En la tabla de enrutamiento pública de egreso, añada el bloque CIDR SpokeVPCA y SpokeVPCB al ID de Transit	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	Gateway. Repita el mismo paso para la subred privada.	

Configurado CloudWatch para realizar una inspección de red en tiempo real

Tarea	Descripción	Habilidades requeridas
Actualice la configuración de registro del firewall.	1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon VPC. 2. En el panel de navegació n, en Firewall de red, elija Firewalls. 3. En la página Firewalls, elija el nombre del firewall que desea editar. 4. Seleccione la pestaña de detalles de Firewall. En la sección Registro, elija Editar. 5. Ajuste las selecciones Tipos de registro según sea necesario. Puede configurar el registro para los registros de alertas y flujos. • Alerta: envía registros del tráfico que coincide con cualquier regla de estado en la que la acción esté configurada como Alerta o Cancelación. Para obtener más informaci	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	ón sobre las reglas con estado y los grupos de regla, consulte Grupos de regla en AWS Network Firewall. • Flujo: envía registros de todo el tráfico de red que el motor sin estado reenvía al motor de reglas con estado. 6. Para cada tipo de registro seleccionado, elija el tipo de destino y, a continuación, proporcione la informaci ón del destino del registro. Para obtener más informaci ón, consulte los destinos de registro de AWS Network Firewall en la documenta ción de Network Firewall. 7. Seleccione Guardar.	

Verifique la configuración

Tarea	Descripción	Habilidades requeridas
Lance una instancia EC2 para probar la configuración.	Lance dos instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la VPC radial: una para Jumpbox y otra para la conectividad de prueba.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Compruebe las métricas.	Las métricas se agrupan en primer lugar por el espacio de nombres de servicio y, a continuación, por las diversas combinaciones de dimension es dentro de cada espacio de nombres. El espacio de CloudWatch nombres de Network Firewall es. `AWS/NetworkFirewall` 1. Inicie sesión en la consola de administración de AWS y abra la consola de CloudWatch . 2. En el panel de navegación, seleccione Métricas. 3. En la pestaña Todas las métricas, elija la región y, a continuación, AWS/NetworkFirewall.	AWS DevOps

Recursos relacionados

- Arquitectura simple de una sola zona con una puerta de enlace de Internet
- Arquitectura de un varias zonas con una puerta de enlace de Internet
- Arquitectura con una puerta de enlace de Internet y una puerta de enlace NAT

Implemente un trabajo de AWS Glue con una canalización de CodePipeline CI/CD de AWS

Documento creado por Bruno Klein (AWS) y Luis Henrique Massao Yamada (AWS)

Entorno: Producción	Tecnologías: DevOps Big data	Servicios de AWS: AWS Glue CodeCommit; AWS CodePipeline; AWS Lambda

Resumen

Este patrón demuestra cómo puede integrar Amazon Web Services (AWS) CodeCommit y AWS CodePipeline con AWS Glue y utilizar AWS Lambda para lanzar trabajos en cuanto un desarrollador envía sus cambios a un repositorio remoto de AWS. CodeCommit

Cuando un desarrollador envía un cambio a un repositorio de extracción, transformación y carga (ETL) y envía los cambios a AWS CodeCommit, se invoca una nueva canalización. La canalización inicia una función de Lambda que lanza un trabajo de AWS Glue con estos cambios. El trabajo de AWS Glue lleva a cabo la tarea de ETL.

Esta solución resulta útil en situaciones en las que las empresas, los desarrolladores y los ingenieros de datos desean lanzar sus trabajos tan pronto como se implementan los cambios y se envíen a los repositorios de destino. Facilita poder lograr un mayor nivel de automatización y reproducibilidad y, por lo tanto, evita errores durante el lanzamiento y el ciclo de vida del trabajo.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Git instalado en el equipo local
- Kit de desarrollo en la nube de Amazon (Amazon CDK) instalado en el equipo local
- Python instalado en el equipo local
- El código de la sección Attachments

Limitaciones

- La canalización finaliza en cuanto el trabajo de AWS Glue se inicia correctamente. No espera a que finalice el trabajo.
- El código que se proporciona en el archivo adjunto está destinado únicamente a fines de demostración.

Arquitectura

Pila de tecnología de destino

- AWS Glue
- AWS Lambda
- AWS CodePipeline
- AWS CodeCommit

Arquitectura de destino

El proceso consta de estos pasos:

1. El desarrollador o el ingeniero de datos realiza una modificación en el código ETL, confirma y envía el cambio a AWS CodeCommit.
2. El envío inicia la canalización.
3. La canalización inicia una función de Lambda, que llama a `codecommit:GetFile` en el repositorio y carga el archivo en Amazon Simple Storage Service (Amazon S3).
4. La función de Lambda lanza un nuevo trabajo de AWS Glue con el código ETL.
5. La función de Lambda finaliza la canalización.

Automatizar y escalar

En el ejemplo adjunto se muestra cómo puede integrar AWS Glue con AWS CodePipeline. Proporciona un ejemplo básico que se puede personalizar o ampliar para el propio uso. Para más información, consulte la sección Epics.

Herramientas

- AWS CodePipeline: AWS CodePipeline es un servicio de entrega continua totalmente gestionado que le ayuda a automatizar sus procesos de lanzamiento para obtener actualizaciones rápidas y fiables de las aplicaciones y la infraestructura.
- AWS CodeCommit: AWS CodeCommit es un servicio de control de código fuente totalmente gestionado que aloja repositorios seguros basados en Git.
- AWS Lambda: AWS Lambda es un servicio informático sin servidor que permite ejecutar código sin aprovisionar ni administrar servidores.
- AWS Glue: AWS Glue es un servicio de integración de datos sin servidor que facilita la detección, preparación y combinación de datos para análisis, machine learning y desarrollo de aplicaciones.
- Cliente Git: Git proporciona herramientas de GUI, o puedes usar la línea de comandos o una herramienta de escritorio para comprobar los artefactos necesarios GitHub.
- AWS CDK: AWS CDK es un marco de desarrollo de software de código abierto que ayuda a definir los recursos de las aplicaciones en la nube mediante lenguajes de programación conocidos.

Epics

Implementar el código de muestra

Tarea	Descripción	Habilidades requeridas
Configure la AWS CLI.	Configure la interfaz de la línea de comandos de AWS (AWS CLI) para señalar y autenticarse con su cuenta de AWS actual. Para obtener instrucciones, consulte la documentación de AWS CLI.	Desarrollador, DevOps ingeniero
Extraiga los archivos de muestra del proyecto.	Extraiga los archivos del adjunto para crear una carpeta que contenga los archivos del proyecto de muestra.	Desarrollador, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Implemente el código de muestra.	Después de extraer los archivos, ejecute los comandos siguientes desde la ubicación de extracción para crear un ejemplo de referenci a: `cdk bootstrap` `cdk deploy` `git init` `git remote add origin <code-commit-repository-url>` `git stage .` `git commit -m "adds sample code"` `git push --set-upstream origin main` Una vez emitido el último comando, puede supervisar el estado de la canalización y el trabajo de AWS Glue.	Desarrollador, DevOps ingeniero
Personalice el código.	Personalice el código del archivo etl.py de acuerdo con los requisitos de su empresa. Puede revisar el código ETL, modificar las etapas del proceso o ampliar la solución.	Ingeniero de datos

Recursos relacionados

- Getting started with the AWS CDK (Introducción a los AWS CDK)
- Adding jobs in AWS Glue (Agregar trabajos a AWS Glue)

- Integraciones de acciones fuente en CodePipeline
- Invoque una función de AWS Lambda en una canalización en CodePipeline
- AWS Glue programming (Programación con AWS Glue)
- CodeCommit GetFile API DE AWS

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Implementar un clúster de Amazon EKS desde AWS Cloud9 mediante un perfil de instancia de EC2

Documento creado por Sagar Panigrahi (AWS)

Entorno: producción	Tecnologías: DevOps contenedores y microservicios	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon EKS; AWS Cloud9; AWS Identity and Access Management; AWS CloudFormation		

Resumen

Este patrón describe cómo usar AWS Cloud9 y AWS CloudFormation para crear un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) que se puede operar sin habilitar el acceso programático a los usuarios de su cuenta de Amazon Web Services (AWS).

AWS Cloud9 es un entorno de desarrollo integrado (IDE) basado en la nube que se utiliza para escribir, ejecutar y depurar código a través de un navegador. AWS Cloud9 se utiliza como centro de control que aprovisiona un clúster de Amazon EKS mediante perfiles de instancia de Amazon Elastic Compute Cloud (Amazon EC2) y plantillas de AWS. CloudFormation

Puede utilizar este patrón si no desea crear usuarios de AWS Identity and Access Management (IAM) y, en cambio, desea utilizar roles de IAM. El control de acceso basado en roles (RBAC) regula el acceso a los recursos en función de los roles de los usuarios individuales. Este patrón muestra cómo actualizar el RBAC dentro de un clúster de Amazon EKS para permitir el acceso a un rol de IAM específico.

La configuración del patrón también ayuda a su DevOps equipo a utilizar las características de AWS Cloud9 para mantener y desarrollar los recursos de infraestructura como código (IaC) para crear la infraestructura de Amazon EKS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Permisos para crear políticas y roles de IAM para la cuenta. El rol de IAM del usuario debe incluir la política `AWSCloud9Administrator`. Los roles `AWSServiceRoleForAmazonEKS` y `eksNodeRoles` también se deben crear porque son necesarios para crear un clúster de Amazon EKS.
- Conocimiento de los conceptos de Kubernetes.

Limitaciones

- Este patrón describe cómo crear un clúster de Amazon EKS básico. En el caso de los clústeres de producción, debe actualizar la CloudFormation plantilla de AWS.
- El patrón no implementa componentes adicionales de Kubernetes (por ejemplo, Fluentd, ingress controllers o storage controllers).

Arquitectura

Pila de tecnología

- AWS Cloud9
- AWS CloudFormation
- Amazon EKS
- IAM

Automatizar y escalar

Puede ampliar este patrón e incorporarlo en los procesos de integración e implementación continuas (CI/CD) para automatizar el aprovisionamiento completo de Amazon EKS.

Herramientas

- AWS CloudFormation: AWS lo CloudFormation ayuda a modelar y configurar sus recursos de AWS para que pueda dedicar menos tiempo a administrarlos y más tiempo a centrarse en sus aplicaciones.
- AWS Cloud9: AWS Cloud9 ofrece una completa experiencia de edición de código, compatible con varios lenguajes de programación y depuradores de tiempo de ejecución, además de un terminal integrado.
- AWS CLI : la Interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que permite interactuar con los servicios de AWS mediante comandos en el intérprete de comandos de línea de comandos.
- Kubectl: `kubectl` es un programa de utilidad de línea de comandos que puede utilizar para interactuar con un clúster de Amazon EKS.

Epics

Crear los roles de IAM para el perfil de instancia de EC2

Tarea	Descripción	Habilidades requeridas
Cree la política de IAM.	Inicie sesión en la consola de administración de AWS, abra la consola de IAM, seleccione Policies (Políticas) y, a continuación, Create policy (Crear política). Elija la pestaña JSON y pegue el contenido del policy-role-eks-instance archivo profile-for-cloud 9.json (adjunto). Resuelva las advertencias de seguridad, errores o advertencias generales que se hayan generado durante la validación de la política y, a continuac	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	ión, seleccione Review policy (Revisar política). Introduzc a un Nombre para la política. Recomendamos utilizar `eks-instance-profile-for-cloud9` para el nombre de la política administrada. Revise el Summary (Resumen) de la política para ver los permisos concedido s por su política. A continuac ión, seleccione Create policy (Crear política).	

Tarea	Descripción	Habilidades requeridas
Cree un rol de IAM mediante la política.	En la consola de IAM, seleccione Roles y, a continuación, Create Role (Crear rol). Seleccione AWS Service (Servicio de AWS) y, a continuación, EC2 de la lista. Seleccione Next: Permissio ns (Siguiente: permisos) y busque la política de IAM que creó anteriormente. Seleccion e las etiquetas adecuadas para sus necesidades. En la sección Review (Revisar), especifique un nombre para el rol. Recomendamos utilizar `role-eks-instance-profile-for-cloud9` para el nombre del rol. A continuación, seleccione Create role.	Administrador de la nube

Cree la política de IAM y el rol de IAM para Amazon EKS RBAC

Tarea	Descripción	Habilidades requeridas
Cree la política de IAM.	En la consola de IAM, seleccione Policies (Política s) y, a continuación, Create policy (Crear política). Seleccione la pestaña JSON y pegue el contenido del policy-	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	for-eks-rbac archivo.json (adjunto). Resuelva las advertencias de seguridad, errores o advertencias generales que se hayan generado durante la validación de la política y, a continuación, seleccione Review policy (Revisar política). Introduzca un Nombre para la política. Recomendamos utilizar `policy-for-eks-rbac` para el nombre de la política administrada. Revise el Summary (Resumen) de la política para ver los permisos concedidos por su política. A continuación, seleccione Create policy (Crear política).	

Tarea	Descripción	Habilidades requeridas
Cree un rol de IAM mediante la política.	En la consola de IAM, seleccione Roles y, a continuación, Create Role (Crear rol). Seleccione AWS Service (Servicio de AWS) y, a continuación, EC2 de la lista. Seleccione Next: Permissio ns (Siguiente: permisos) y busque la política de IAM que creó anteriormente. Seleccion e las etiquetas adecuadas para sus necesidades. En la sección Review (Revisar), especifique un nombre para el rol. Recomendamos utilizar `role-eks-admin-for-rbac` para el nombre del rol. A continuación, seleccione Create role.	Administrador de la nube

Cree el entorno de AWS Cloud9

Tarea	Descripción	Habilidades requeridas
Cree el entorno de AWS Cloud9.	Abra la consola de AWS Cloud9 y seleccione Create environment (Crear entorno). En la página Name environme nt (Asignar nombre al entorno), especifique un nombre para el entorno. Recomendamos utilizar `eks-`	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	`management-env` para el nombre del entorno. Configure los ajustes restantes de acuerdo con sus requisitos y, a continuación, seleccione Next step (Paso siguiente). En la página Review (Revisión), elija Create environme nt (Crear entorno). Espere mientras AWS Cloud9 crea el entorno. Esto puede tardar varios minutos. Para obtener más informaci ón sobre las opciones de configuración disponibles, consulte Creating an EC2 environment (Crear un entorno EC2) en la documentación de AWS Cloud9.	
Elimine las credenciales de IAM temporales para AWS Cloud9.	Una vez aprovisionado su entorno AWS Cloud9, seleccione Settings (Configur ación) en el icono de engranaje. En Preferences, seleccione AWS settings (Configuración de AWS) y, a continuación, seleccione Credentials. Desactive las credenciales temporales administradas por AWS y cierre la pestaña.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Asocie el perfil de instancia de EC2 a la instancia de EC2 subyacente.	En la consola de Amazon EC2, seleccione la instancia de EC2 que se adapte a su entorno en AWS Cloud9. Si usó el nombre que recomendamos, la instancia EC2 se llamará `aws-cloud9-eks-management-env` . Seleccione la instancia de EC2, elija Actions y, a continuación, Instance settings (Configuración de la instancia). Seleccione Attach/replace IAM role (Adjuntar/sustituir rol de IAM). Busque `role-eks-instance-profile-for-cloud9` o el nombre del rol de IAM que creó anteriormente y, a continuación, seleccione Apply.	Administrador de la nube

Crear el clúster de Amazon EKS

Tarea	Descripción	Habilidades requeridas
Cree el clúster de Amazon EKS.	Descargue y abra la plantilla eks-cfn.yaml (adjunta) para AWS. CloudFormation Edite la plantilla de acuerdo con sus necesidades. Abra el entorno de AWS Cloud9 y seleccione New file (Nuevo archivo). Pegue la	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	CloudFormation plantilla de AWS que creó anteriormente en el campo. Se recomiend a utilizar eks-cfn.yaml como nombre de plantilla. En el terminal de AWS Cloud9, ejecute el comando siguiente para crear el clúster de Amazon EKS: `aws cloudformation create-stack --stack-name eks-cluster --template-body file://eks-cfn.yaml --region <your_AWS_Region>` Si la CloudFormation llamada de AWS se realiza correctamente, recibirá el nombre de recurso de Amazon (ARN) de la CloudFormation pila de AWS en el resultado. La creación de la pila puede tardar entre 10 y 20 minutos.	

Tarea	Descripción	Habilidades requeridas
Verifique el estado del clúster de Amazon EKS.	En la CloudFormation consola de AWS, abra la página Stacks y, a continuación, elija el nombre de la pila. La pila se crea cuando el código de estado de la pila muestra `CREATE_COMPLETE` . Para obtener más información, consulte Visualización de los datos y recursos de la CloudFormation pila de AWS en la CloudFormation documentación de AWS.	Administrador de la nube

Acceda a los recursos de Kubernetes en el clúster de Amazon EKS

Tarea	Descripción	Habilidades requeridas
Instale kubectl en el entorno AWS Cloud9.	Instale `kubectl` en su entorno AWS Cloud9 siguiendo las instrucciones de Installing kubectl de la documentación de Amazon EKS.	Administrador de la nube
Actualice la nueva configuración de Amazon EKS en AWS Cloud9.	Ejecute el comando siguiente en el terminal AWS Cloud9 para actualizar el `kubeconfig` del clúster Amazon EKS al entorno AWS Cloud9: `aws eks update-kubeconfig --name`	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	`EKS-DEV2 --region <your_AWS_Region>` Importante: `EKS-DEV2` es el nombre del clúster de Amazon EKS en la CloudFormation plantilla de AWS que utilizó para crear el clúster. Ejecute el comando `kubectl get all -A` para ver todos los recursos de Kubernetes.	

Tarea	Descripción	Habilidades requeridas
Agregue el rol de IAM de administrador en el RBAC de Kubernetes.	Ejecute el comando siguiente en el terminal de AWS Cloud9 para abrir el mapa de configuración de RBAC para Amazon EKS en modo de edición: `kubectl edit cm/aws-auth -n kube-system` Agregue las líneas siguientes a la sección `mapRoles`: `- groups:` `- system:masters` `rolearn: <ARN_of_IAM_role _from_second_epic>` `username: eksadmin` Borre el archivo con formato YAML para evitar errores de sintaxis. Guarde el archivo mediante comandos `vi` y, a continuación, salga del archivo. Nota: Al agregar esta sección, se informa al RBAC de Kubernetes de que `<ARN_of_IAM_role _from_second_epic>` va a recibir acceso de administrador completo al clúster de Amazon EKS. Esto significa que el rol de IAM identific	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	ado puede llevar a cabo acciones administrativas en el clúster de Kubernetes. AWS agrega la sección existente en `mapRoles` mientras se aprovisiona el clúster de Amazon EKS.	

Recursos relacionados

Referencias

- Modular and scalable Amazon EKS architecture (Arquitectura modular y escalable de Amazon EKS) (Inicio rápido)
- Managing users or IAM roles for your Amazon EKS cluster (Administrar usuarios o roles de IAM para su clúster de Amazon EKS)
- CloudFormation Plantilla de AWS para crear un nuevo plano de control de Amazon EKS

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Implemente código en varias regiones de AWS mediante AWS CodePipeline CodeCommit, AWS y AWS CodeBuild

Creado por Rama Anand Krishna Varanasi (AWS)

Creado por: AWS	Entorno: PoC o piloto	Tecnologías: gestión y gobierno; DevOps
Servicios de AWS: AWS CodeCommit CodePipeline; AWS CodeBuild		

Resumen

Este patrón demuestra cómo crear una infraestructura o arquitectura en varias regiones de Amazon Web Services (AWS) mediante AWS CloudFormation. Incluye integración continua (CI) e implementación continua (CD) en varias regiones de AWS para lograr implementaciones más rápidas. Por ejemplo, se probaron los pasos de este patrón para crear un CodePipeline trabajo de AWS para implementarlo en tres regiones de AWS. Puede cambiar el número de regiones en función del caso de uso.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Dos funciones de AWS Identity and Access Management (IAM) para AWS CodeBuild y AWS CloudFormation con las políticas adecuadas CodeBuild para realizar las tareas de CI consistentes en probar, agrupar, empaquetar los artefactos e implementarlos en varias regiones de AWS en paralelo. Nota: Compruebe las políticas creadas por CodePipeline para comprobar que CodeBuild AWS CloudFormation tiene los permisos adecuados en las fases de CI y CD.
  - Un CodeBuild puesto en Amazon S3 FullAccess y CloudWatchFullAccessen las políticas. Estas políticas permiten CodeBuild ver eventos de AWS a CodeCommit través de Amazon CloudWatch y utilizar Amazon Simple Storage Service (Amazon S3) como almacén de artefactos.

- Un CloudFormation rol de AWS con las siguientes políticas, que permiten a AWS CloudFormation, en la fase final de creación, crear o actualizar las funciones de AWS Lambda, enviar o ver CloudWatch los registros de Amazon y crear y actualizar conjuntos de cambios.
  - AWSLambdaFullAccess
  - AWSCodeDeployFullAccess
  - CloudWatchFullAccess
  - AWSCloudFormationFullAccess
  - AWSCodePipelineFullAccess

Arquitectura

La arquitectura y el flujo de trabajo de varias regiones de este patrón comprenden los siguientes pasos.

1. Envía el código a un CodeCommit repositorio.
2. Al recibir cualquier actualización o confirmación de código, CodeCommit invoca un CloudWatch evento que, a su vez, inicia un CodePipeline trabajo.
3. CodePipeline activa el CI gestionado por. CodeBuild Se realizan las siguientes tareas.
   - Prueba de las CloudFormation plantillas de AWS (opcional)
   - Empaquetado de las CloudFormation plantillas de AWS para cada región incluidas en la implementación. Por ejemplo, este patrón se implementa en paralelo en tres regiones de AWS, por lo que CodeBuild empaqueta las CloudFormation plantillas de AWS en tres grupos de S3, uno en cada región especificada. Los depósitos de S3 se utilizan únicamente CodeBuild como repositorios de artefactos.
4. CodeBuild empaqueta los artefactos como entrada para la siguiente fase de implementación, que se ejecuta en paralelo en las tres regiones de AWS. Si especifica un número diferente de regiones, CodePipeline se desplegará en esas regiones.

Herramientas

Herramientas

- AWS CodePipeline: CodePipeline es un servicio de entrega continua que puede utilizar para modelar, visualizar y automatizar los pasos necesarios para publicar los cambios de software de forma continua.
- AWS CodeBuild: CodeBuild es un servicio de compilación totalmente gestionado que compila el código fuente, ejecuta pruebas unitarias y produce artefactos listos para su implementación.
- AWS CodeCommit: CodeCommit es un servicio de control de versiones hospedado por Amazon Web Services que puede utilizar para almacenar y gestionar activos (como código fuente y archivos binarios) en la nube de forma privada.
- AWS CloudFormation: AWS CloudFormation es un servicio que le ayuda a modelar y configurar sus recursos de Amazon Web Services para que pueda dedicar menos tiempo a gestionar esos recursos y más a centrarse en las aplicaciones que se ejecutan en AWS.
- AWS Identity and Access Management: AWS Identity and Access Management (IAM) es un servicio web que le ayuda a controlar de forma segura el acceso a los recursos de AWS.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet. Está diseñado para facilitar a los desarrolladores recursos de computación escalables basados en Web.

Código

El siguiente código de ejemplo es para el archivo `BuildSpec.yaml` (fase de compilación).

```
---
artifacts:
discard-paths: true
files:
- packaged-first-region.yaml
- packaged-second-region.yaml
- packaged-third-region.yaml
phases:
build:
commands:
- echo "********BUILD PHASE - CF PACKAGING**********"
- "aws cloudformation package --template-file sam-template.yaml --s3-bucket
 $S3_FIRST_REGION --output-template-file packaged-first-region.yaml --region
 $FIRST_REGION"
- "aws cloudformation package --template-file sam-template.yaml --s3-bucket
 $S3_SECOND_REGION --output-template-file packaged-second-region.yaml --region
 $SECOND_REGION"
```

```
- "aws cloudformation package --template-file sam-template-anand.yaml --s3-bucket
 $S3_THIRD_REGION --output-template-file packaged-third-region.yaml --region
 $THIRD_REGION"
install:
commands:
- echo "********BUILD PHASE - PYTHON SETUP**********"
runtime-versions:
python: 3.8
post_build:
commands:
- echo "********BUILD PHASE - PACKAGING COMPLETION**********"
pre_build:
commands:
- echo "********BUILD PHASE - DEPENDENCY SETUP**********"
- "npm install --silent --no-progress"
- echo "********BUILD PHASE - DEPENDENCY SETUP DONE**********"
version: 0.2
```

Epics

Prepare el código y el CodeCommit repositorio

Tarea	Descripción	Habilidades requeridas
Seleccione la región de AWS principal para la implement ación.	Inicie sesión en su cuenta de AWS y elija la región principal para la implementación. El CodeCommit repositorio estará en la región principal.	DevOps
Cree el CodeCommit repositor io.	Cree el CodeCommit repositor io e introduzca el código necesario en él. Por lo general, el código incluye las plantillas de AWS CloudForm ation o AWS SAM, el código Lambda, si lo hubiera, y los CodeBuild `buildspec .yaml` archivos como entrada a AWS. CodePipeline	DevOps

Tarea	Descripción	Habilidades requeridas
Inserte el código en el CodeCommit repositorio.	En la sección de adjuntos, descargue el código de este ejemplo y, a continuación, inserte el código necesario en él. Por lo general, el código puede incluir plantillas de AWS CloudFormation o AWS SAM, código Lambda y los CodeBuild `buildspec .yaml` archivos como entrada a la canalización.	DevOps

Fase de origen: Crear la canalización

Tarea	Descripción	Habilidades requeridas
Cree el CodePipeline trabajo.	En la CodePipeline consola, selecciona Crear canalización.	DevOps
Asigne un nombre al CodePipeline trabajo y elija la configuración del rol de servicio.	Introduzca un nombre para el trabajo y mantenga la configuración de rol de servicio predeterminada para CodePipeline crear el rol con las políticas necesarias adjuntas.	DevOps
Especifique la ubicación del almacén de artefactos.	En Configuración avanzada, mantenga la opción predeterminada para CodePipeline crear un bucket de S3 que se utilizará como almacenamiento de artefactos de código. Si en su lugar utiliza un	DevOps

Tarea	Descripción	Habilidades requeridas
	bucket de S3 existente, el bucket debe estar en la región principal que especificó en la primera épica.	
Especifique la clave de cifrado.	Elimine la opción predeterminada, clave administrada de AWS predeterminada o utilice la clave administrada por el cliente de AWS Key Management Service (AWS KMS).	DevOps
Especifique el proveedor de origen.	En Proveedor de código fuente, elija AWS CodeCommit.	DevOps
Especifique el repositorio.	Elige el CodeCommit repositorio que creaste en la primera epopeya. Si ha colocado el código en una ramificación, elija la rama.	DevOps
Especifique cómo se detectan los cambios en el código.	Mantenga el valor predeterminado, Amazon CloudWatch Events, como activador del cambio CodeCommit para iniciar el CodePipeline trabajo.	DevOps

Fase de creación: configure la canalización

Tarea	Descripción	Habilidades requeridas
Especifique el proveedor de compilación.	Para el proveedor de compilación, elija AWS CodeBuild.	DevOps
Especifique la Región de AWS.	Elija la región principal que especificó en la primera épica.	DevOps

Fase de compilación: cree y configure el proyecto

Tarea	Descripción	Habilidades requeridas
Creación del proyecto	Elija Crear proyecto e especifique un nombre para el proyecto.	DevOps
Especifique la imagen del entorno.	Para esta demostración del patrón, utilice la imagen CodeBuild gestionada por defecto. También tiene la opción de utilizar una imagen de Docker personalizada si tiene una.	DevOps
Especifique el sistema operativo.	Elija Amazon Linux 2 o Ubuntu.	DevOps
Especifique el rol de servicio.	Elija el rol para el que creó CodeBuild antes de empezar a crear el CodePipeline trabajo. (Consulte la sección Requisitos previos.)	DevOps
Establezca opciones adicional es.	Para Tiempo de espera y el Tiempo de espera en	DevOps

Tarea	Descripción	Habilidades requeridas
	cola, mantenga los valores predeterminados. En el caso del certificado, mantenga la configuración predeterminada a menos que desee utilizar un certificado personalizado.	
Crear las variables de entorno.	Para cada región de AWS en la que desee realizar la implementación, cree variables de entorno proporcionando el nombre del bucket de S3 y el nombre de la región (por ejemplo, us-east-1).	DevOps
Proporcione el nombre del archivo buildspec, si no es buildspec.yml.	Mantenga este campo en blanco si el nombre del archivo es el predeterminado, `buildspec.yaml` . Si ha cambiado el nombre del archivo buildspec, introdúzcalo aquí. Asegúrese de que coincide con el nombre del archivo que está en el CodeCommit repositorio.	DevOps
Especifique el registro.	Para ver los registros de Amazon CloudWatch Events, mantenga la configuración predeterminada. O bien, puede definir cualquier nombre de grupo o registrador específico.	DevOps

Omitir la fase de implementación

Tarea	Descripción	Habilidades requeridas
Omita la fase de implement ación y complete la creación de la canalización.	Al configurar la canalización, CodePipeline solo puede crear una etapa en la fase de implementación. Para realizar la implementación en varias regiones de AWS, omita esta fase. Una vez creada la canalización, puede añadir varias etapas de la fase de implementación.	DevOps

Fase de implementación: configure la canalización para la implementación en la primera región

Tarea	Descripción	Habilidades requeridas
Agregue una etapa a la fase de implementación.	Edite la canalización y elija Agregar etapa en la fase de implementación. Esta primera etapa es para la región principal.	DevOps
Proporcione un nombre de acción para la etapa.	Introduzca un nombre único que refleje la primera etapa (principal) y la región. Por ejemplo, introduzca primary_<region>_deploy.	DevOps
Especifique el proveedor de acciones.	En Action provider, elija AWS CloudFormation.	DevOps
Configure la región para la primera etapa.	Elija la primera región (principal), la misma región en CodePipeline la CodeBuild	DevOps

Tarea	Descripción	Habilidades requeridas
	que están configuradas. Esta es la región principal en la que desea implementar la pila.	
Especifique el artefacto de entrada.	Elige BuildArtifact. Este es el resultado de la fase de construcción.	DevOps
Especifique la acción que se va a realizar.	Para Modo acción, elija Crear o actualizar una pila.	DevOps
Introduzca un nombre para la CloudFormation pila.		DevOps
Especifique la plantilla para la primera región.	Seleccione el nombre del paquete específico de la región que empaquetó CodeBuild y descargó en el depósito de S3 de la primera región (principal).	DevOps
Especifique las capacidades.	Las capacidades son necesarias si la plantilla de pila incluye recursos de IAM o si se crea una pila directamente a partir de una plantilla que contiene macros. Para este patrón, utilice CAPABILITY_IAM, CAPABILITY_NAMED_IAM y CAPABILITY_AUTO_EXPAND.	DevOps

Fase de despliegue: configure la canalización para la implementación en la segunda región

Tarea	Descripción	Habilidades requeridas
Añada la segunda etapa a la fase de despliegue.	Para añadir una etapa para la segunda región, edite la canalización y elija Añadir etapa en la fase de despliegue. Importante: el proceso de creación de la segunda región es el mismo que el de la primera región, excepto por los siguientes valores.	DevOps
Proporcione un nombre de acción para la segunda etapa.	Introduzca un nombre único que refleje la segunda etapa y la segunda región.	DevOps
Configure la región para la segunda etapa.	Elija la segunda región en la que desea implementar la pila.	DevOps
Especifique la plantilla para la segunda región.	Seleccione el nombre del paquete específico de la región que empaquetó CodeBuild y descargó en el depósito de S3 de la segunda región.	DevOps

Fase de implementación: configure la canalización para la implementación en la tercera región

Tarea	Descripción	Habilidades requeridas
Añada la tercera etapa a la fase de implementación.	Para añadir una etapa para la tercera región, edite la canalización y elija Añadir etapa en la fase de implementación. Importante: el proceso	DevOps

Tarea	Descripción	Habilidades requeridas
	de creación de la segunda región es el mismo que el de las dos regiones anteriores, excepto por los siguientes valores.	
Proporcione un nombre de acción para la tercera etapa.	Introduzca un nombre único que refleje la tercera etapa y la tercera región.	DevOps
Configure la región para la tercera etapa.	Elija la tercera región en la que desea implementar la pila.	DevOps
Especifique la plantilla para la tercera región.	Seleccione el nombre del paquete específico de la región que empaquetó CodeBuild y descargó en el depósito de S3 de la tercera región.	DevOps

Eliminar la implementación

Tarea	Descripción	Habilidades requeridas
Eliminación de los recursos de AWS.	Para limpiar la implement ación, elimine las CloudForm ation pilas de cada región. A continuación CodeCommi t, elimine los CodePipeline recursos CodeBuild, y de la región principal.	DevOps

Recursos relacionados

- ¿Qué es AWS CodePipeline?
- Modelo de aplicación sin servidor de AWS
- AWS CloudFormation
- Referencia de estructura de CloudFormation arquitectura de AWS para AWS CodePipeline

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Exportar los informes de AWS Backup de toda la organización en AWS Organizations como un archivo CSV

Creado por Aromal Raj Jayarajan (AWS) y Purushotham G K (AWS)

Repositorio de código: aws-backup-report-generator	Entorno: PoC o piloto	Tecnologías: DevOps Infraestructura
Carga de trabajo: todas las demás cargas de trabajo	Servicios de AWS: AWS Backup; AWS Identity and Access Management; AWS Lambda; Amazon S3; Amazon EventBridge	

Resumen

Este patrón muestra cómo exportar los informes de trabajos de AWS Backup de toda una organización en AWS Organizations como un archivo CSV. La solución utiliza AWS Lambda y Amazon EventBridge para clasificar los informes de trabajos de AWS Backup en función de su estado, lo que puede ayudar a configurar las automatizaciones basadas en el estado.

AWS Backup ayuda a las organizaciones a administrar y automatizar de forma centralizada la protección de datos en todos los servicios de AWS, en la nube y en las instalaciones. Sin embargo, para los trabajos de AWS Backup configurados en AWS Organizations, los informes consolidados solo están disponibles en la consola de administración de AWS de la cuenta de administración de cada organización. Sacar estos informes de la cuenta de administración puede reducir el esfuerzo necesario para la auditoría y aumentar el alcance de las automatizaciones, las notificaciones y las alertas.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una organización activa en AWS Organizations que incluye al menos una cuenta de administración y una cuenta de miembro

- AWS Backup configurado a nivel organizativo en AWS Organizations (para obtener más información, consulte Automate centralized backup at scale across AWS services using AWS Backup en el blog de AWS)
- Git, instalado y configurado en su equipo local

Limitaciones

La solución proporcionada en este patrón identifica los recursos de AWS que están configurados únicamente para trabajos de AWS Backup. El informe no puede identificar los recursos de AWS que no estén configurados para realizar copias de seguridad mediante AWS Backup.

Arquitectura

Pila de tecnología de destino

- AWS Backup
- AWS CloudFormation
- Amazon EventBridge
- AWS Lambda
- AWS Security Token Service (AWS STS)
- Amazon Simple Storage Service (Amazon S3)
- AWS Identity y Access Management (IAM)

Arquitectura de destino

El siguiente diagrama muestra un ejemplo de flujo de trabajo para exportar informes de trabajos de AWS Backup de toda una organización en AWS Organizations como un archivo CSV.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Una regla de EventBridge eventos programados invoca una función Lambda en la cuenta de AWS del miembro (informante).
2. A continuación, la función de Lambda utiliza AWS STS para asumir un rol de IAM que tiene los permisos necesarios para conectarse a la cuenta de administración.
3. La función de Lambda lleva a cabo lo siguiente:

- Solicita el informe consolidado de trabajos de AWS Backup al servicio AWS Backup
- Clasifica los resultados según el estado del trabajo de AWS Backup
- Convertir la respuesta en un archivo CSV
- Carga los resultados en un bucket de Amazon S3 de la cuenta de informes, dentro de carpetas etiquetadas según su fecha de creación.

Herramientas

Herramientas

- AWS Backup es un servicio totalmente administrado que le ayuda a centralizar y automatizar la protección de datos en todos los servicios de AWS, en la nube y en las instalaciones.
- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, las funciones de Lambda de AWS, los puntos de conexión de invocación HTTP que utilizan destinos de API o los buses de eventos de otras cuentas de AWS.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Código

El código de este patrón está disponible en el GitHub aws-backup-report-generatorrepositorio.

Prácticas recomendadas

- Prácticas recomendadas de seguridad para Amazon S3 (Guía del usuario de Amazon S3)

- Prácticas recomendadas para trabajar con las funciones de AWS Lambda (Guía para desarrolladores de AWS Lambda)
- Prácticas recomendadas para la cuenta de administración (Guía del usuario de AWS Organizations)

Epics

Implementar los componentes de la solución

Tarea	Descripción	Habilidades requeridas
Clona el GitHub repositorio.	Clone el GitHub aws-backup-report-generatorrepositorio ejecutando el siguiente comando en una ventana de terminal: `git clone https://github.com/aws-samples/aws-backup-report-generator.git` Para obtener más información, consulta Cómo clonar un repositorio en los GitHub documentos.	AWS DevOps, DevOps ingeniero
Implemente los componentes de la solución en la cuenta de AWS del miembro (informante).	1. En la cuenta de miembro (informante), inicie sesión en la consola de administración de AWS y, a continuación, abra la CloudFormation consola. 2. Elija Create stack (Crear pila), y, a continuación, elija With new resources	DevOps ingeniero, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	(standard) (Con nuevos recursos [estándar]). 3. En la página Crear pila, en la sección Especificar plantilla, seleccione Cargar un archivo de plantilla. 4. Seleccione Choose file (Elegir archivo). A continuación, vaya a la carpeta raíz del GitHub repositorio clonado en su estación de trabajo local y elija template-reporting.yaml. 5. Elija Abrir y, a continuación, elija Siguiente. 6. En la página Especificar los detalles de la pila, en Nombre de la pila, introduce un nombre para la pila. CloudFormation 7. En ManagementAccountID, introduzca el ID de la cuenta de AWS de la cuenta de administración de su organización en AWS Organizations. 8. Seleccione Siguiente. 9. En la página Configurar opciones de pila, elija Siguiente. 10. En la página de revisión, seleccione la casilla de verificación para	

Tarea	Descripción	Habilidades requeridas
	confirmar que ha revisado la configuración. 11. Seleccione Crear pila. La pila muestra el estado CREATE_COMPLETE cuando los componentes de la solución se implementan en la cuenta del miembro (informante).	

Pruebe la solución

Tarea	Descripción	Habilidades requeridas
Asegúrese de que la EventBridge regla se ejecute antes de la prueba.	Asegúrese de que la EventBridge regla se ejecute esperando al menos 24 horas o aumentando la frecuencia de los informes en el archivo CloudFormation template-reporting.yml de la plantilla. Para aumentar la frecuencia de los informes 1. Abra el archivo template-reporting.yml en el repositorio clonado. 2. En la regla de eventos con el identificador lógico '', busque el 'LambdaSchedule'. ScheduleExpression	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	3. Edita la clave ScheduleE xpression" para que incluya una expresión cron válida. Por ejemplo, la siguiente expresión cron programa la regla de eventos para que se ejecute cada cinco minutos: `“cron (* /5 * * * *)”`	

Tarea	Descripción	Habilidades requeridas
Consulte el bucket de Amazon S3 para ver el informe generado.	1. En la cuenta de miembro (informante), inicie sesión en la consola de administración de AWS y, a continuación, abra la CloudFormation consola. 2. En el panel Pilas, seleccione el nombre de la pila que creó. A continuación, elija la pestaña Recursos. 3. En el panel Recursos, en la columna ID lógica, busque BackupReportS3Bucket. A continuación, abra el bucket de Amazon S3 asociado en una pestaña nueva. Para ello, seleccione el enlace en la columna ID física situada junto a ese ID lógico. 4. <Mon><yyyy>Asegúrese de que el depósito contenga un informe generado en el siguiente formato: BackupReports//// BackupReport- - - - .csv <yyyy><mm><dd><BACKUP JOB STATUS><dd>	AWS DevOps, DevOps ingeniero

Eliminación de sus recursos

Tarea	Descripción	Habilidades requeridas
Elimine los componentes de la solución de la cuenta del miembro (informante).	1. En la cuenta del miembro (informante), abra el bucket de Amazon S3 de la solución. Para obtener instrucciones, consulte los pasos 2 a 4 de la historia Comprobar el bucket de S3 para ver el informe generado de la sección Probar la solución de este patrón. 2. Elimine el contenido del bucket y vacíelo. Para obtener instrucciones, consulte Vaciar un bucket en la Guía del usuario de Amazon S3. 3. En la cuenta de miembro (informante), inicie sesión en la consola de administración de AWS y, a continuación, abra la CloudFormation consola. 4. En el panel Pilas, seleccione la casilla de verificación situada junto al nombre de la pila que creó. A continuación, elija Eliminar.	AWS DevOps, DevOps ingeniero
Elimine los componentes de la solución de la cuenta de administración.	1. En la cuenta de administración, inicie sesión en la consola de administración	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	de AWS y, a continuación, abra la CloudFormation consola. 2. En el panel Pilas, seleccione la casilla de verificación situada junto al nombre de la pila que creó. A continuación, elija Eliminar.	

Recursos relacionados

- Tutorial: Uso de AWS Lambda con eventos programados (documentación de AWS Lambda)
- Creación de eventos programados para ejecutar funciones de AWS Lambda (AWS SDK para obtener JavaScript documentación)
- Tutorial de IAM: delegue el acceso a todas las cuentas de AWS mediante funciones de IAM (documentación de IAM)
- Terminología y conceptos de AWS Organizations (Guía del usuario de AWS Organizations)
- Creación de planes de informes mediante la consola de AWS Backup (documentación de AWS Backup)
- Crear un informe de auditoría (documentación de AWS Backup)
- Creación de informes bajo demanda (documentación de AWS Backup)
- ¿Qué es AWS Backup? (Documentación de AWS Backup)
- Automatice el backup centralizado a escala en todos los servicios de AWS mediante AWS Backup (entrada del blog de AWS)

Exportación de etiquetas para una lista de instancias de Amazon EC2 a un archivo CSV

Creado por Sida Ju (AWS) y Pac Joonhyun (AWS)

Repositorio de código: busque y exporte etiquetas EC2	Entorno: producción	Tecnologías: DevOps
Servicios de AWS: Amazon EC2		

Resumen

Este patrón muestra cómo exportar mediante programación las etiquetas de una lista de instancias de Amazon Elastic Compute Cloud (Amazon EC2) a un archivo CSV.

Con el ejemplo de script de Python que se proporciona, puede reducir el tiempo que se tarda en revisar y clasificar las instancias de Amazon EC2 por etiquetas específicas. Por ejemplo, puede usar el script para identificar y categorizar rápidamente una lista de instancias que su equipo de seguridad ha marcado como actualizaciones de software.

Requisitos previos y limitaciones

Requisitos previos

- Python 3 instalado y configurado
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada

Limitaciones

El script de Python de ejemplo que se proporciona en este patrón puede buscar instancias de Amazon EC2 basándose únicamente en los siguientes atributos:

- ID de instancia
- Direcciones IPv4 privadas
- Direcciones IPv4 públicas

Herramientas

- Python es un lenguaje de programación informático de uso general.
- virtualenv le ayuda a crear entornos Python aislados.
- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.

Repositorio de código

El script Python de ejemplo para este patrón está disponible en el repositorio GitHub search-ec2 -. instances-export-tags

Epics

Instalar y configurar los requisitos previos

Tarea	Descripción	Habilidades requeridas
Clona el repositorio. GitHub	Nota: Si recibe errores al ejecutar los comandos de la CLI de AWS, asegúrese de utilizar la versión más reciente de la CLI de AWS. Clona el instances-export-tags repositorio GitHub search-ec2- ejecutando el siguiente comando de Git en una ventana de terminal: `git clone https://github.com/aws-samples/search-ec2-instances-export-tags.git`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Instale y active virtualenv.	1. Instale virtualenv ejecutando el siguiente comando: `python3 -m pip install virtualenv` 2. Cree un nuevo entorno virtual ejecutando el siguiente comando: `python3 -m venv env` 3. Active el nuevo entorno virtual ejecutando el siguiente comando: `source env/bin/activate` Para más información, consulte la Guía del usuario de virtualenv.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Instale las dependencias.	1. Abra el directorio de código ejecutando el siguiente comando en el terminal: `cd search-ec2-instances-export-tags` 2. Instale el archivo `requirements.txt` ejecutando el siguiente comando pip: `pip3 install -r requirements.txt`	DevOps ingeniero
Configure un perfil con nombre de AWS.	Si aún no lo ha hecho, configure un perfil con nombre de AWS que incluya las credenciales necesarias para ejecutar el script. Para crear un perfil con nombre, ejecute el comando aws configure. Para obtener más información, consulte Uso de perfiles con nombre en la documentación de la CLI de AWS.	DevOps ingeniero

Configurar y ejecutar el script de Python

Tarea	Descripción	Habilidades requeridas
Cree el archivo de entrada.	Cree un archivo de entrada que contenga una lista de las instancias de Amazon	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	EC2 para las que desea que el script busque y exporte etiquetas. Puede enumerar ID de instancias, direcciones IPv4 privadas o direcciones IPv4 públicas. Importante: asegúrese de que cada instancia de Amazon EC2 aparezca en su propia línea en el archivo de entrada. Ejemplo de archivo de entrada `1 i-0547c351bdfe85b9f` `2 54.157.194.156` `3 172.31.85.33` `4 54.165.198.144` `5 i-0b6223b5914111a4b` `6 172.31.85.44` `7 54.165.198.145` `8 172.31.80.219` `9 172.31.94.199`	

Tarea	Descripción	Habilidades requeridas
Ejecute el script de Python.	Ejecute el siguiente comando en el terminal para ejecutar el siguiente comando: `python search_instances.py -i INPUTFILE -o OUTPUTFILE -r REGION [-p PROFILE]` Nota: Cambie `INPUTFILE` por el nombre del archivo de entrada. Cambie `OUTPUTFILE` por el nombre que desea otorgar al archivo CSV resultante. Sustituya `REGION` por la región de AWS en la que se encuentran los recursos de Amazon EC2. Si utiliza un perfil con nombre de AWS, sustituya `PROFILE` por el perfil con nombre que está utilizando. Para obtener una lista de parámetros compatibles y su descripción, ejecute el siguiente comando: `python search_instances.py -h` Para obtener más información y ver un ejemplo de archivo de salida, consulte el `README.md` archivo en el	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	repositorio GitHub search-ec2 -. instances-export-tags	

Recursos relacionados

- Configuración de la CLI de AWS (Guía del usuario de la CLI de AWS)

Genere una CloudFormation plantilla de AWS que contenga las reglas administradas por AWS Config mediante Troposphere

Creado por Lucas Nation (AWS) y Freddie Wilson (AWS)

Entorno: producción	Tecnologías: DevOps gestión y gobierno; seguridad, identidad y cumplimiento	Carga de trabajo: Microsoft; código abierto
Servicios de AWS: AWS Config; AWS CloudFormation		

Resumen

Muchas organizaciones utilizan las reglas administradas de AWS Config para evaluar la conformidad de sus recursos de Amazon Web Services (AWS) con respecto a las prácticas recomendadas habituales. Sin embargo, el mantenimiento de estas reglas puede llevar mucho tiempo y este patrón lo ayuda a aprovechar Troposphere, una biblioteca de Python, para generar y administrar reglas administradas por AWS Config.

El patrón le ayuda a administrar las reglas administradas por AWS Config mediante un script de Python para convertir una hoja de cálculo de Microsoft Excel que contiene reglas administradas por AWS en una CloudFormation plantilla de AWS. Troposphere actúa como infraestructura como código (IaC), lo que significa que puede actualizar la hoja de cálculo de Excel con reglas administradas en lugar de utilizar un archivo con formato JSON o YAML. A continuación, utilice la plantilla para lanzar una CloudFormation pila de AWS que cree y actualice las reglas administradas en su cuenta de AWS.

La CloudFormation plantilla de AWS define cada regla gestionada por AWS Config mediante la hoja de cálculo de Excel y le ayuda a evitar la creación manual de reglas individuales en la consola de administración de AWS. El script establece de forma predeterminada los parámetros de cada regla administrada en un diccionario vacío y los `ComplianceResourceTypes` valores predeterminados del ámbito son. `THE_RULE_IDENTIFIER.template file` Para obtener más información sobre el identificador de la regla, consulte Creación de reglas administradas de AWS Config con CloudFormation plantillas de AWS en la documentación de AWS Config.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Familiaridad con el uso de CloudFormation plantillas de AWS para crear reglas administradas de AWS Config. Para obtener más información al respecto, consulte Creación de reglas administradas de AWS Config con CloudFormation plantillas de AWS en la documentación de AWS Config.
- Python 3, instalado y configurado. Para obtener más información, consulte la Documentación de Python.
- Un entorno de desarrollo integrado (IDE) existente, como AWS Cloud9. Para obtener más información, consulte ¿Qué es AWS Cloud9? en la documentación de AWS Cloud9.
- Identifique sus unidades organizativas (UO) en una columna de la hoja de cálculo de Excel de muestra `excel_config_rules.xlsx` (adjunta).

Epics

Personalice y configure las reglas administradas de AWS Config

Tarea	Descripción	Habilidades requeridas
Actualice la hoja de cálculo de Excel de muestra.	Descargue la hoja de cálculo de Excel de muestra `excel_config_rules.xlsx` (adjunta) y etiquétela como `Implemented` con las reglas administradas de AWS Config que desee usar. Las reglas marcadas como se `Implemented` añadirán a la CloudFormation plantilla de AWS.	Desarrollador
(Opcional) Actualice el archivo config_rules_params.json con	Algunas reglas administradas por AWS Config requieren parámetros y deben pasarse	Desarrollador

Tarea	Descripción	Habilidades requeridas
los parámetros de las reglas de AWS Config.	al script de Python como un archivo JSON mediante la opción `--param-file` . Por ejemplo, la regla administrada `access-keys-rotated` usa el siguiente parámetro `maxAccessKeyAge` : `{ "access-keys-rotated": { "InputParameters": { "maxAccessKeyAge": 90 } } }` En este parámetro de ejemplo, `maxAccessKeyAge` se establece en 90 días. El script lee el archivo de parámetros y añade cualquier `InputParameters` que encuentra.	

Tarea	Descripción	Habilidades requeridas
(Opcional) Actualice el archivo config_rules_params.json con AWS Config. ComplianceResourceTypes	De forma predeterminada, el script de Python recupera `ComplianceResourceTypes` de las plantillas definidas por AWS. Si desea anular el ámbito de una regla gestionada por AWS Config específica, debe pasarla al script de Python como un archivo JSON mediante la opción `--param-file` . Por ejemplo, el siguiente código de ejemplo muestra cómo el `ComplianceResourceTypes` para `ec2-volume-inuse-check` se establece en la lista `["AWS::EC2::Volume"]` : `{ "ec2-volume-inuse-check": { "Scope": { "ComplianceResourceTypes": [ "AWS::EC2::Volume" ] } } }`	Desarrollador

Ejecute el script de Python

Tarea	Descripción	Habilidades requeridas
Instalar los paquetes pip desde el archivo requirements.txt.	Descargue el archivo `requirements.txt` (adjunto) y ejecute el siguiente comando en su IDE para instalar los paquetes de Python: `pip3 install -r requirements.txt`	Desarrollador
Ejecute el script de Python.	1. Descargue el archivo `aws_config_rules.py` (adjunto) en el equipo local. 2. Ejecute el comando `python3 aws_config_rules.py --ou <OU_NAME>`. Nota: `--ou` Define qué columna de OU elegir en la hoja de cálculo de Excel. También puede incluir los siguientes parámetros opcionales: • `--config-rule-option`: define las reglas a elegir de la hoja de cálculo de Excel. El parámetro determinado es `Implemented`.	Desarrollador

Tarea	Descripción	Habilidades requeridas
	• `--excel-file` : la ruta de la hoja de cálculo de Excel. El valor predeterminado es `aws_config_rules.xlsx` . • `--param-file` : la ruta del archivo JSON de parámetros. El valor predeterminado es `config_rules_params.json` . • `--max-execution-frequency` : define la frecuencia con la que se evalúan las reglas administradas de AWS Config. Las opciones son `One_Hour`, `Three_Hours` , `Six_Hours` , `Twelve_Hours` o `TwentyFour_Hours` . El valor predeterminado es `TwentyFour_Hours` .	

Implemente las reglas administradas en AWS Config

Tarea	Descripción	Habilidades requeridas
Lance la CloudFormation pila de AWS.	1. Inicie sesión en la consola de administración de AWS, abra la CloudFormation consola de AWS y, a continuación, elija Create stack.	Desarrollador

Tarea	Descripción	Habilidades requeridas
	2. En la página Especificar plantilla, elija Cargar un archivo de plantilla y, a continuación, cargue su CloudFormation plantilla de AWS. 3. Especifique el nombre de la pila y elija Next (Siguiente). 4. Especifique las etiquetas y, a continuación, elija Next (Siguiente). 5. Seleccione Crear pila.	

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Otorgue a las instancias de SageMaker notebook acceso temporal a un CodeCommit repositorio de otra cuenta de AWS

Creado por Helge Aufderheide (AWS)

Entorno: producción	Tecnologías: análisis DevOps, aprendizaje automático e inteligencia artificial, gestión y gobierno	Servicios de AWS: AWS CodeCommit; AWS Identity and Access Management; Amazon SageMaker

Resumen

Este patrón muestra cómo conceder a las instancias de Amazon SageMaker Notebook y a los usuarios acceso temporal a un CodeCommit repositorio de AWS que se encuentra en otra cuenta de AWS. También indica cómo conceder permisos detallados para acciones específicas que cada entidad puede realizar en un repositorio.

Las organizaciones suelen almacenar CodeCommit los repositorios en una cuenta de AWS diferente a la cuenta que aloja su entorno de desarrollo. Esta configuración de múltiples cuentas ayuda a controlar el acceso a los repositorios y reduce el riesgo de que se eliminen accidentalmente. Para conceder estos permisos entre cuentas, se recomienda usar roles de AWS Identity and Access Management (IAM). Las identidades de IAM predefinidas en cada cuenta de AWS podrán asumir temporalmente los roles para crear una cadena de confianza controlada en todas las cuentas.

Nota: Puede aplicar un procedimiento similar para conceder a otras identidades de IAM el acceso multicuenta a un repositorio. CodeCommit Para obtener más información, consulte Configurar el acceso multicuenta a un CodeCommit repositorio de AWS mediante roles en la Guía del CodeCommit usuario de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa con un CodeCommit repositorio (cuenta A)
- Una segunda cuenta de AWS activa con una instancia de SageMaker notebook (cuenta B)
- Un usuario de AWS con permisos suficientes para crear y modificar roles de IAM en la cuenta A

- Un segundo usuario de AWS con permisos suficientes para crear y modificar roles de IAM en la cuenta B

Arquitectura

En el siguiente diagrama se muestra un ejemplo de flujo de trabajo para conceder a una instancia de SageMaker Notebook y a los usuarios de una cuenta de AWS acceso multicuenta a un CodeCommit repositorio:

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El rol de usuario de AWS y el rol de instancia de SageMaker notebook en la cuenta B asumen un perfil con nombre.
2. La política de permisos del perfil mencionado especifica un rol de CodeCommit acceso en la cuenta A que luego asume el perfil.
3. La política de confianza del rol de CodeCommit acceso en la cuenta A permite que el perfil designado en la cuenta B asuma el rol de CodeCommit acceso.
4. La política de permisos de IAM del CodeCommit repositorio en la cuenta A permite que el CodeCommit rol de acceso acceda al CodeCommit repositorio.

Pila de tecnología

- CodeCommit
- Git
- IAM
- pip
- SageMaker

Herramientas

- AWS CodeCommit es un servicio de control de versiones que le ayuda a almacenar y gestionar repositorios de Git de forma privada, sin necesidad de gestionar su propio sistema de control de código fuente.

- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- Git es un sistema de control de versiones distribuido que rastrea los cambios en el código fuente durante el desarrollo del software.
- git-remote-codecommites una utilidad que te ayuda a insertar y extraer código de CodeCommit los repositorios mediante la extensión de Git.
- pip es el instalador de paquetes para Python. Puede usar pip para instalar paquetes desde Python Package Index y otros índices.

Prácticas recomendadas

Cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para llevar a cabo una tarea. Para obtener más información, consulte Aplicar permisos de privilegio mínimo en la documentación de IAM.

Al implementar este patrón, asegúrese de hacer lo siguiente:

- Confirme que los principios de IAM solo tienen los permisos necesarios para realizar acciones específicas y necesarias en cada repositorio. Por ejemplo, se recomienda permitir que los principios de IAM aprobados envíen y combinen los cambios en ramificaciones específicas del repositorio, pero que solo puedan solicitar combinaciones en las ramificaciones protegidas.
- Confirme que a los principios de IAM se les asignen diferentes roles de de IAM en función de los roles y responsabilidades respectivos de cada proyecto. Por ejemplo, un desarrollador tendrá permisos de acceso diferentes a los de un administrador de versiones o un administrador de AWS.

Epics

Configuración roles de IAM

Tarea	Descripción	Habilidades requeridas
Configura el rol de CodeCommit acceso y la política de permisos.	Nota: Para automatizar el proceso de configuración manual documentado en esta epopeya, puede utilizar una	AWS general, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	CloudFormation plantilla de AWS. En la cuenta que contiene el CodeCommit repositorio (cuenta A), haga lo siguiente: 1. Cree una función de IAM que pueda asumir la función de instancia de SageMaker bloc de notas de la cuenta B. 2. Cree una política de IAM que conceda acceso al repositorio y asocie la política al rol. Solo con fines de prueba, elija la política administr ada por AWSCodeCo mmitPowerUserAWS. Esta política concede todos los CodeCommit permisos excepto la posibilidad de eliminar recursos. 3. Modifique la política de confianza del rol para que la cuenta B aparezca como entidad de confianza. Importante: antes de trasladar esta configuración a su entorno de producción, se recomienda redactar su propia política de IAM que aplique permisos de privilegio mínimo.	

Tarea	Descripción	Habilidades requeridas
	Para obtener más informaci ón, consulte la sección de Información adicional de este patrón.	

Tarea	Descripción	Habilidades requeridas
Conceda permisos a la instancia de SageMaker bloc de notas en la cuenta B para que asuma la función de CodeCommit acceso en la cuenta A.	En la cuenta que contiene la función de IAM de la instancia de SageMaker bloc de notas (cuenta B), haga lo siguiente: 1. Cree una política de IAM que permita a un usuario o rol de IAM asumir el rol de CodeCommit acceso en la cuenta A. Ejemplo de política de permisos de IAM que permite a un usuario o rol de IAM asumir un rol entre cuentas `{ "Version": "2012-10-17", "Statement": [ { "Sid": "VisualEditor0", "Effect": "Allow", "Action": "sts:AssumeRole", "Resource": "arn:aws:iam:::accountA_ID:role/accountArole_ID" } }` 2. Adjunta la política a la función de la instancia de tu SageMaker bloc de notas en la cuenta B.	AWS general, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	3. Haga que la función de la instancia de SageMaker bloc de notas en la cuenta B asuma la función de CodeCommit acceso en la cuenta A. Nota: Para ver el nombre de recurso de Amazon (ARN) de su repositorio, consulte Ver detalles del CodeCommit repositorio en la Guía CodeCommit del usuario de AWS.	

Configure su instancia de SageMaker notebook en la cuenta B

Tarea	Descripción	Habilidades requeridas
Configure un perfil de usuario en la instancia de AWS SageMaker Notebook para que asuma el rol en la cuenta A.	Importante: asegúrese de tener instalada la última versión de la interfaz de la línea de comandos de AWS (AWS CLI). En la cuenta que contiene la instancia de SageMaker bloc de notas (cuenta B), haga lo siguiente: 1. Inicie sesión en la consola de administración de AWS y abra la consola de SageMaker .	AWS general, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	2. Acceda a la instancia de su SageMaker bloc de notas. Se abrirá la interfaz de Jupyter. 3. Seleccione Nuevo y, a continuación, seleccione Terminal. Se abrirá una nueva ventana de terminal en su entorno de Jupyter. 4. Navegue hasta el archivo ~/.aws/config de la instancia del SageMaker bloc de notas. A continuación, añada un perfil de usuario al archivo introduciendo la siguiente instrucción: `------.aws/config-------------[profile remoterepouser]role_arn = arn:aws:iam::<ID of Account A>:role/<rolename>role_session_name = remoteaccesssessionregion = eu-west-1credential_source = Ec2InstanceMetadata----------------------------------`	

Tarea	Descripción	Habilidades requeridas
Instale la git-remote-codecommit utilidad.	Siga las instrucciones del paso 2: Instalación de git-remote-codecommit la Guía del CodeCommit usuario de AWS.	Científico de datos

Acceda al repositorio

Tarea	Descripción	Habilidades requeridas
Acceda al CodeCommit repositorio mediante los comandos de Git o SageMaker.	Uso en Git Los directores de IAM que asumen la función de la instancia de SageMaker bloc de notas en la cuenta B ahora pueden ejecutar comandos de Git para acceder al CodeCommit repositorio de la cuenta A. Por ejemplo, los usuarios pueden ejecutar comandos como `git clonegit pull`, y. `git push` Para obtener instrucciones, consulte Conectarse a un CodeCommit repositorio de AWS en la Guía del CodeCommit usuario de AWS. Para obtener información sobre cómo usar Git con CodeCommit, consulte Introducción a AWS	Git, consola bash

Tarea	Descripción	Habilidades requeridas
	CodeCommit en la Guía del CodeCommit usuario de AWS. Para usar SageMaker Para usar Git desde la SageMaker consola, debes permitir que Git recupere las credenciales de tu CodeCommit repositor io. Para obtener instrucci ones, consulte Asociar un CodeCommit repositorio de una cuenta de AWS diferente a una instancia de notebook en la SageMaker documenta ción.	

Recursos relacionados

- Configurar el acceso multicuenta a un CodeCommit repositorio de AWS mediante roles (CodeCommit documentación de AWS)
- Tutorial de IAM: delegue el acceso a todas las cuentas de AWS mediante funciones de IAM (documentación de IAM)

Información adicional

Restringir los CodeCommit permisos a acciones específicas

Para restringir las acciones que un responsable de IAM puede realizar en el CodeCommit repositorio, modifique las acciones que están permitidas en la política de CodeCommit acceso.

Para obtener más información sobre las operaciones de la CodeCommit API, consulte la referencia de CodeCommit permisos en la Guía del CodeCommit usuario de AWS.

Nota: También puede editar la política gestionada por AWSCodeCommitPowerUserAWS para adaptarla a su caso de uso.

Restringir CodeCommit los permisos a repositorios específicos

Para crear un entorno multiusuario en el que solo usuarios específicos puedan acceder a más de un repositorio de código, haga lo siguiente:

1. Cree varios roles de CodeCommit acceso en la cuenta A. A continuación, configure la política de confianza de cada rol de acceso para permitir que usuarios específicos de la cuenta B asuman el rol.
2. Restrinja los repositorios de código que puede asumir cada función añadiendo una condición de «recurso» a la política de cada función de CodeCommit acceso.

Ejemplo de condición de «recurso» que restringe el acceso de un director de IAM a un repositorio específico CodeCommit

```
"Resource" : [<REPOSITORY_ARN>,<REPOSITORY_ARN> ]
```

Nota: para ayudar a identificar y diferenciar varios repositorios de código en la misma cuenta de AWS, puede asignar distintos prefijos a los nombres de los repositorios. Por ejemplo, puede asignar nombres a los repositorios de código con prefijos que correspondan a distintos grupos de desarrolladores, como myproject-subproject1-repo1 y myproject-subproject2-repo1. A continuación, puede crear un rol de IAM para cada grupo de desarrolladores en función de sus prefijos asignados. Por ejemplo, puedes crear un rol denominado myproject-subproject1-repoaccess y concederle acceso a todos los repositorios de código que incluyen el prefijo myproject-subproject1.

Ejemplo de condición “Recurso” que hace referencia a un ARN de repositorio de código que incluye un prefijo específico

```
"Resource" : arn:aws:codecommit:<region>:<account-id>:myproject-subproject1-*
```

Implemente una estrategia GitHub de ramificación de Flow para entornos de cuentas múltiples DevOps

Creado por Mike Stephens (AWS) y Abhilash Vinod (AWS)

Repositorio de código: - multiaccount-devops git-branching-strategies-for	Entorno: producción	Tecnologías: desarrollo y pruebas de software DevOps; estrategia multicuenta
Servicios de AWS: AWS CodeArtifact CodeBuild; AWS CodeCommit; AWS CodeDeploy; AWS CodePipeline		

Resumen

Al gestionar un repositorio de código fuente, las diferentes estrategias de ramificación afectan a los procesos de desarrollo y publicación de software que utilizan los equipos de desarrollo. Algunos ejemplos de estrategias de ramificación habituales son Trunk, GitHub Flow y Gitflow. Estas estrategias utilizan diferentes ramas y las actividades que se realizan en cada entorno son diferentes. Organismos que están implementando DevOps procesos se beneficiarían de una guía visual que les ayude a entender las diferencias entre estas estrategias de ramificación. El uso de este elemento visual en su organización ayuda a los equipos de desarrollo a alinear su trabajo y seguir los estándares de la organización. Este patrón proporciona esta imagen y describe el proceso de implementación de una estrategia de ramificación de GitHub Flow en su organización.

Este patrón forma parte de una serie de documentos sobre la elección e implementación de estrategias de DevOps ramificación para organizaciones con múltiples sucursales. Cuentas de AWS Esta serie está diseñada para ayudarlo a aplicar la estrategia correcta y las mejores prácticas desde el principio, a fin de optimizar su experiencia en la nube. GitHub El flujo es solo una posible estrategia de ramificación que su organización puede utilizar. Esta serie de documentación también cubre los modelos de ramificación de Trunk y Gitflow. Si aún no lo has hecho, te recomendamos que revises Cómo elegir una estrategia de ramificación de Git para DevOps entornos de múltiples

cuentas antes de implementar la guía de este patrón. Usa la diligencia debida para elegir la estrategia de ramificación adecuada para tu organización.

Esta guía proporciona un diagrama que muestra cómo una organización podría implementar la estrategia GitHub Flow. Se recomienda revisar la Guía de AWS DevOps Well-Architected para revisar las mejores prácticas. Este patrón incluye las tareas, los pasos y las restricciones recomendados para cada paso del DevOps proceso.

Requisitos previos y limitaciones

Requisitos previos

- Git, instalado. Se utiliza como herramienta de repositorio de código fuente.
- Draw.io, instalado. Esta aplicación se utiliza para ver y editar el diagrama.

Arquitectura

Arquitectura de destino

El siguiente diagrama se puede utilizar como un cuadrado de Punnett (Wikipedia). Alinee las ramas en el eje vertical con los AWS entornos en el eje horizontal para determinar qué acciones realizar en cada escenario. Los números indican la secuencia de las acciones del flujo de trabajo. En este ejemplo, se pasa de una `feature` sucursal a la implementación en producción.

Para obtener más información sobre los Cuentas de AWS entornos y las ramas en un enfoque de GitHub flujo, consulta Cómo elegir una estrategia de ramificación de Git para entornos de múltiples cuentas DevOps .

Automatizar y escalar

La integración y la entrega continuas (CI/CD) son el proceso de automatización del ciclo de vida de las versiones de software. Automatiza gran parte o la totalidad de los procesos manuales que tradicionalmente se requerían para pasar del código nuevo a la producción desde un principio. Una canalización de CI/CD abarca los entornos sandbox, de desarrollo, de pruebas, de puesta en escena y de producción. En cada entorno, la canalización de CI/CD proporciona cualquier infraestructura necesaria para implementar o probar el código. Mediante el uso de la CI/CD, los equipos de desarrollo pueden realizar cambios en el código que luego se prueban e implementan automáticamente. Los procesos de CI/CD también proporcionan control y protección a los equipos de

desarrollo al garantizar la coherencia, los estándares, las mejores prácticas y unos niveles mínimos de aceptación para la aceptación y el despliegue de las funciones. Para obtener más información, consulte Practicar la integración continua y la entrega continua en. AWS

AWS ofrece un conjunto de servicios para desarrolladores diseñados para ayudarle a crear canalizaciones de CI/CD. Por ejemplo, AWS CodePipelinees un servicio de entrega continua totalmente gestionado que le ayuda a automatizar sus procesos de lanzamiento para obtener actualizaciones rápidas y fiables de las aplicaciones y la infraestructura. AWS CodeCommitestá diseñado para alojar de forma segura repositorios Git escalables y AWS CodeBuildcompila el código fuente, ejecuta pruebas y produce paquetes de ready-to-deploy software. Para obtener más información, consulte las Herramientas para desarrolladores en. AWS

Herramientas

AWS servicios y herramientas

AWS proporciona un conjunto de servicios para desarrolladores que puede utilizar para implementar este patrón:

- AWS CodeArtifactes un servicio de repositorio de artefactos gestionado y altamente escalable que le ayuda a almacenar y compartir paquetes de software para el desarrollo de aplicaciones.
- AWS CodeBuildes un servicio de compilación totalmente gestionado que le ayuda a compilar código fuente, ejecutar pruebas unitarias y producir artefactos listos para su despliegue.
- AWS CodeCommites un servicio de control de versiones que te ayuda a almacenar y gestionar de forma privada los repositorios de Git, sin necesidad de gestionar tu propio sistema de control de código fuente.
- AWS CodeDeployautomatiza las implementaciones en Amazon Elastic Compute Cloud (Amazon EC2) o en instancias, AWS Lambda funciones locales o servicios de Amazon Elastic Container Service (Amazon ECS).
- AWS CodePipelinele ayuda a modelar y configurar rápidamente las diferentes etapas de una versión de software y a automatizar los pasos necesarios para publicar los cambios de software de forma continua.

Otras herramientas

- Draw.io Desktop es una aplicación para hacer diagramas de flujo y diagramas. El repositorio de código contiene plantillas en formato.drawio para Draw.io.

- Figma es una herramienta de diseño online diseñada para la colaboración. El repositorio de código contiene plantillas en formato.fig para Figma.

Repositorio de código

El archivo fuente del diagrama de este patrón está disponible en el repositorio GitHub Git Branching Strategy for GitHub Flow. Incluye archivos en los formatos PNG, draw.io y Figma. Puede modificar estos diagramas para respaldar los procesos de su organización.

Prácticas recomendadas

Siga las mejores prácticas y recomendaciones de AWS DevOps Well-Architected Guidance y Eligiendo una estrategia de ramificación de Git para entornos de múltiples cuentas. DevOps Te ayudan a implementar de forma eficaz el desarrollo GitHub basado en Flow, a fomentar la colaboración, a mejorar la calidad del código y a agilizar el proceso de desarrollo.

Epics

Revisión de los GitHub flujos de trabajo de Flow

Tarea	Descripción	Habilidades requeridas
Revise el proceso GitHub de flujo estándar.	1. En el entorno sandbox, el desarrollador crea una `feature` rama a partir de la `main` rama y utiliza el patrón `feature/<ticket>_<initials>_<short description>` de nomenclatura. 2. El desarrollador agrega una o más confirmaciones a la `feature` rama, cada una de las cuales representa un cambio o mejora discretos. 3. El desarrollador abre una solicitud de fusión (MR)	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	para combinar los cambios en la `main` rama. Esto inicia un proceso de revisión. 4. Durante el proceso de revisión, los desarrolladores analizan los cambios en el código y proporcionan comentarios. El objetivo es garantizar que los cambios sean de alta calidad y cumplan con los estándares del proyecto. 5. Una vez que el desarroll ador crea la solicitud de fusión, se inicia un proceso de creación automatiz ado que implementa los cambios de la `feature` rama en el entorno de desarrollo. 6. Las pruebas automatizadas verifican la integridad y la calidad de los cambios incluidos en la solicitud de fusión. Para completar la solicitud de fusión, es necesario que la compilaci ón, la implementación y las pruebas se realicen correctamente. 7. Cuando se completa el proceso de revisión, los cambios se fusionan en la `main` rama.	

Tarea	Descripción	Habilidades requeridas
	8. Un aprobador aprueba manualmente el despliegue de los artefactos de lanzamiento en el entorno de pruebas. 9. Un aprobador aprueba manualmente el despliegue de los artefactos de lanzamiento en el entorno provisional. 10. Un aprobador aprueba manualmente el despliegue de los artefactos de lanzamiento en el entorno de producción.	

Tarea	Descripción	Habilidades requeridas
Revise el proceso de corrección de errores GitHub Flow.	1. El desarrollador crea una `bugfix` rama a partir de la `main` rama y usa el patrón `bugfix/<ticket number>_<developer initials>_<descriptor>` de nomenclatura. 2. El desarrollador corrige el problema, confirma la corrección y crea la `bugfix` rama. 3. El desarrollador abre una solicitud de fusión para fusionar la `bugfix` rama en la `main` rama. Esto inicia un proceso de revisión. 4. Durante el proceso de revisión, los desarrolladores analizan los cambios en el código y proporcionan comentarios. 5. Una vez finalizada la revisión y aprobación, el desarrollador completa la solicitud de fusión de la `bugfix` sucursal con la `main` sucursal. 6. Un aprobador aprueba manualmente el despliegue de los artefactos de lanzamiento en entornos superiores.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Revise el proceso de hotfix GitHub Flow.	GitHub Flow está diseñado para permitir una entrega continua, donde los cambios de código se implementan de manera frecuente y confiable en entornos superiores. La clave es que todas las `feature` sucursales se puedan implementar en cualquier momento. `Hotfix`las sucursales, que son parecidas a `feature` o `bugfix` sucursales, pueden seguir el mismo proceso que cualquiera de estas otras sucursales. Sin embargo, dada su urgencia, las revisiones suelen tener una prioridad más alta. En función de las políticas del equipo y de la inmediatez de la situación, algunos pasos del proceso podrían acelerarse. Por ejemplo, es posible que se aceleren las revisiones del código de las revisiones. Por lo tanto, si bien el proceso de revisión es paralelo al proceso de corrección de funciones o errores, la urgencia que rodea a las revisiones puede justificar modificaciones en el cumplimiento del procedimiento. Es fundament	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	al establecer directrices sobre la gestión de las revisione s para garantizar que se gestionen de forma eficiente y segura.	

Solución de problemas

Problema	Solución
Conflictos de sucursales	Un problema común que puede producirse con el modelo GitHub Flow es cuando es necesario realizar una revisión en la producción`feature`, `bugfix` pero el cambio correspondiente debe producirse en una `hotfix` rama o sucursal en la que se modifican los mismos recursos. Le recomendamos que fusione con frecuenci a los cambios de `main` las ramas inferiores para evitar conflictos importantes al realizar la fusión. `main`
Madurez del equipo	GitHub Flow fomenta las implementaciones diarias en entornos superiores y adopta una verdadera integración y entrega continuas (CI/ CD). Es imprescindible que el equipo tenga la madurez en ingeniería necesaria para desarroll ar funciones y crear pruebas de automatización para ellas. El equipo debe realizar una revisión exhaustiva de las solicitudes de fusión antes de que se aprueben los cambios. Esto fomenta una cultura de ingeniería sólida que promueve la calidad, la responsabilidad y la eficiencia en el proceso de desarrollo.

Recursos relacionados

Esta guía no incluye formación sobre Git; sin embargo, hay muchos recursos de alta calidad disponibles en Internet si necesitas esta formación. Te recomendamos que comiences por el sitio de documentación de Git.

Los siguientes recursos pueden ayudarte en tu proceso de ramificación de GitHub Flow en el Nube de AWS.

AWS DevOps orientación

- AWS DevOps Orientación
- AWS Arquitectura de referencia para la canalización de despliegue
- ¿Qué es DevOps?
- DevOps recursos

GitHub Guía de flujo

- GitHub Tutorial de inicio rápido de Flow () GitHub
- ¿Por qué GitHub Flow?

Otros recursos

- Metodología de aplicaciones de doce factores (12factor.net)

Implementa una estrategia de ramificación de Gitflow para entornos de múltiples cuentas DevOps

Creado por Mike Stephens (AWS), Stephen DiCato (AWS), Tim Wondergem (AWS) y Abhilash Vinod (AWS)

git-branching-strategies-forRepositorio de código: -multiaccount-devops	Entorno: producción	Tecnologías: desarrollo y pruebas de software DevOps; estrategia multicuenta
Servicios de AWS: AWS CodeArtifact CodeBuild; AWS CodeCommit; AWS CodeDeploy; AWS CodePipeline		

Resumen

Al gestionar un repositorio de código fuente, las diferentes estrategias de ramificación afectan a los procesos de desarrollo y publicación de software que utilizan los equipos de desarrollo. Algunos ejemplos de estrategias de ramificación habituales son Trunk, Gitflow y Flow. GitHub Estas estrategias utilizan diferentes ramas y las actividades que se realizan en cada entorno son diferentes. Organismos que están implementando DevOps procesos se beneficiarían de una guía visual que les ayude a entender las diferencias entre estas estrategias de ramificación. El uso de este elemento visual en su organización ayuda a los equipos de desarrollo a alinear su trabajo y seguir los estándares de la organización. Este patrón proporciona esta imagen y describe el proceso de implementación de una estrategia de ramificación de Gitflow en tu organización.

Este patrón forma parte de una serie de documentos sobre cómo elegir e implementar estrategias de DevOps ramificación para organizaciones con múltiples sucursales. Cuentas de AWS Esta serie está diseñada para ayudarlo a aplicar la estrategia correcta y las mejores prácticas desde el principio, a fin de optimizar su experiencia en la nube. Gitflow es solo una posible estrategia de ramificación que tu organización puede utilizar. Esta serie de documentación también cubre los modelos de ramificación de Trunk y GitHub Flow. Si aún no lo has hecho, te recomendamos que revises Cómo elegir una estrategia de ramificación de Git para DevOps entornos de múltiples cuentas antes de

implementar la guía de este patrón. Usa la diligencia debida para elegir la estrategia de ramificación adecuada para tu organización.

Esta guía proporciona un diagrama que muestra cómo una organización podría implementar la estrategia de Gitflow. Se recomienda revisar la Guía de AWS DevOps Well-Architected para revisar las mejores prácticas. Este patrón incluye las tareas, los pasos y las restricciones recomendados para cada paso del DevOps proceso.

Requisitos previos y limitaciones

Requisitos previos

- Git, instalado. Se utiliza como una herramienta de repositorio de código fuente.
- Draw.io, instalado. Esta aplicación se utiliza para ver y editar el diagrama.
- (Opcional) Plugin de Gitflow, instalado.

Arquitectura

Arquitectura de destino

El siguiente diagrama se puede usar como un cuadrado de Punnett (Wikipedia). Alinee las ramas en el eje vertical con los AWS entornos en el eje horizontal para determinar qué acciones realizar en cada escenario. Los números indican la secuencia de las acciones del flujo de trabajo. En este ejemplo, se pasa de una rama de funciones a la implementación en producción.

Para obtener más información sobre los Cuentas de AWS entornos y las ramas en un enfoque de Gitflow, consulta Cómo elegir una estrategia de ramificación de Git para entornos de múltiples DevOps cuentas.

Automatizar y escalar

La integración y la entrega continuas (CI/CD) son el proceso de automatización del ciclo de vida de las versiones de software. Automatiza gran parte o la totalidad de los procesos manuales que tradicionalmente se requerían para pasar del código nuevo a la producción desde un principio. Una canalización de CI/CD abarca los entornos sandbox, de desarrollo, de pruebas, de puesta en escena y de producción. En cada entorno, la canalización de CI/CD proporciona cualquier infraestructura necesaria para implementar o probar el código. Mediante el uso de la CI/CD, los equipos de desarrollo pueden realizar cambios en el código que luego se prueban e implementan

automáticamente. Los procesos de CI/CD también proporcionan control y protección a los equipos de desarrollo al garantizar la coherencia, los estándares, las mejores prácticas y unos niveles mínimos de aceptación para la aceptación y el despliegue de las funciones. Para obtener más información, consulte Practicar la integración continua y la entrega continua en. AWS

AWS ofrece un conjunto de servicios para desarrolladores diseñados para ayudarle a crear canalizaciones de CI/CD. Por ejemplo, AWS CodePipelinees un servicio de entrega continua totalmente gestionado que le ayuda a automatizar sus procesos de lanzamiento para obtener actualizaciones rápidas y fiables de las aplicaciones y la infraestructura. AWS CodeCommitestá diseñado para alojar de forma segura repositorios Git escalables y AWS CodeBuildcompila el código fuente, ejecuta pruebas y produce paquetes de ready-to-deploy software. Para obtener más información, consulte Herramientas para desarrolladores en. AWS

Herramientas

AWS servicios y herramientas

AWS proporciona un conjunto de servicios para desarrolladores que puede utilizar para implementar este patrón:

- AWS CodeArtifactes un servicio de repositorio de artefactos gestionado y altamente escalable que le ayuda a almacenar y compartir paquetes de software para el desarrollo de aplicaciones.
- AWS CodeBuildes un servicio de compilación totalmente gestionado que le ayuda a compilar código fuente, ejecutar pruebas unitarias y producir artefactos listos para su despliegue.
- AWS CodeCommites un servicio de control de versiones que te ayuda a almacenar y gestionar de forma privada los repositorios de Git, sin necesidad de gestionar tu propio sistema de control de código fuente.
- AWS CodeDeployautomatiza las implementaciones en Amazon Elastic Compute Cloud (Amazon EC2) o en instancias, AWS Lambda funciones locales o servicios de Amazon Elastic Container Service (Amazon ECS).
- AWS CodePipelinele ayuda a modelar y configurar rápidamente las diferentes etapas de una versión de software y a automatizar los pasos necesarios para publicar los cambios de software de forma continua.

Otras herramientas

- Draw.io Desktop es una aplicación para hacer diagramas de flujo y diagramas. El repositorio de código contiene plantillas en formato.drawio para Draw.io.

- Figma es una herramienta de diseño online diseñada para la colaboración. El repositorio de código contiene plantillas en formato.fig para Figma.
- (Opcional) El complemento Gitflow es una colección de extensiones de Git que proporcionan operaciones de repositorio de alto nivel para el modelo de ramificación de Gitflow.

Repositorio de código

El archivo fuente del diagrama de este patrón está disponible en el GitFlow repositorio GitHub Git Branching Strategy for. Incluye archivos en los formatos PNG, draw.io y Figma. Puede modificar estos diagramas para respaldar los procesos de su organización.

Prácticas recomendadas

Siga las mejores prácticas y recomendaciones de AWS DevOps Well-Architected Guidance y Eligiendo una estrategia de ramificación de Git para entornos de múltiples cuentas. DevOps Te ayudan a implementar de manera efectiva el desarrollo basado en Gitflow, fomentar la colaboración, mejorar la calidad del código y agilizar el proceso de desarrollo.

Epics

Revisar los flujos de trabajo de Gitflow

Tarea	Descripción	Habilidades requeridas
Revisa el proceso estándar de Gitflow.	1. En el entorno sandbox, el desarrollador crea una `feature` rama a partir de la `develop` rama y usa el patrón de nomenclatura. `feature/<ticket>_<initials>_<short description>` 2. El desarrollador desarrolla el código y lo despliega en el entorno sandbox de forma iterativa para completar el ticket.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Nota: Si lo desea, el desarrollador puede crear una `sandbox` rama para ejecutar una canalización automática de compilación o despliegue en el entorno sandbox. 3. El desarrollador crea una solicitud de fusión de una `feature` `develop` rama a otra mediante una fusión automática. 4. Una canalización de integración y entrega continuas (CI/CD) crea e implementa automátic amente la `develop` sucursal en el entorno de desarrollo. 5. (Opcional) Un desarrollador integra `feature` sucursale s adicionales en la rama de desarrollo antes de continuar con las actividad es de lanzamiento. 6. Cuando esté listo para lanzar las funciones de la `develop` rama, el desarroll ador crea una `release` rama con el nombre `release/v<number>` de la `develop` rama.	

Tarea	Descripción	Habilidades requeridas
	7. El desarrollador crea la rama de versiones, que publica los artefactos para reutilizarlos en otros entornos. 8. Un aprobador aprueba manualmente el despliegue de los artefactos de la versión en el entorno de pruebas. 9. Un aprobador aprueba manualmente el despliegue de los artefactos de lanzamiento en el entorno provisional. 10. Un aprobador aprueba manualmente el despliegue de los artefactos de lanzamiento en el entorno de producción. 11. El desarrollador fusiona la `release` rama en la rama. `main` Lo ideal es que el desarrollador utilice un script automatizado para realizar una fusión rápida. No utilices una combinación rápida. 12. El desarrollador fusiona la `release` rama en la `develop` rama. Lo ideal es que el desarrollador utilice un script automatizado para realizar una fusión rápida.	

Tarea	Descripción	Habilidades requeridas
	No utilices una combinación rápida.	

Tarea	Descripción	Habilidades requeridas
Revisa el proceso de hotfix de Gitflow.	1. El desarrollador crea una `hotfix` rama a partir de la `main` rama y usa el patrón de nomenclatura. `hotfix/<ticket>_<initials>_<short description>` 2. El desarrollador crea una `release` rama a partir de la `main` rama y le da un nombre `release/v<number>` . 3. El desarrollador corrige el problema, confirma la corrección y crea la `hotfix` rama. 4. El desarrollador crea una solicitud de fusión de una `hotfix` `release/v<number>` rama a otra mediante una combinación automática. 5. El desarrollador crea la `release` sucursal, que publica los artefactos para reutilizarlos en otros entornos. 6. Un aprobador aprueba manualmente el despliegue de los artefactos de lanzamiento en el entorno de pruebas.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	7. Un aprobador aprueba manualmente el despliegue de los artefactos de lanzamiento en el entorno provisional. 8. Un aprobador aprueba manualmente el despliegue de los artefactos de lanzamiento en el entorno de producción. 9. El desarrollador fusiona la `release` rama en la rama. `main` Lo ideal es que el desarrollador utilice un script automatizado para realizar una fusión rápida. No utilices una combinación rápida. 10. El desarrollador fusiona la `release` rama en la `develop` rama. Lo ideal es que el desarrollador utilice un script automatizado para realizar una fusión rápida. No utilices una combinación rápida. 11. Si se detecta un conflicto, los desarrolladores reciben una alerta y resuelven el conflicto con una solicitud de fusión.	

Tarea	Descripción	Habilidades requeridas
Revisa el proceso de corrección de errores de Gitflow.	1. El desarrollador crea una `bugfix` rama a partir de la `release/v<number>` rama actual y usa el patrón de nomenclatura. `bugfix/<ticket number>_<developer initials>_<descriptor>` 2. El desarrollador corrige el problema, confirma la corrección y crea la `bugfix` rama. 3. El desarrollador crea una solicitud de fusión de una `bugfix` `release/v<number>` rama a otra mediante una combinación automática. 4. El desarrollador crea la `release` sucursal, que publica los artefactos para reutilizarlos en otros entornos. 5. Un aprobador aprueba manualmente el despliegue de los artefactos de lanzamiento en el entorno de prueba. 6. Un aprobador aprueba manualmente el despliegue de los artefactos de lanzamiento en el entorno Stage.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	7. Un aprobador aprueba manualmente el despliegue de los artefactos de lanzamiento en el entorno de producción. 8. El desarrollador fusiona la `release` rama en la rama. `main` Lo ideal es que el desarrollador utilice un script automatizado para realizar una fusión rápida. No utilices una combinación rápida. 9. El desarrollador fusiona la `release` rama en la `develop` rama. Lo ideal es que el desarrollador utilice un script automatizado para realizar una fusión rápida. No utilices una combinación rápida. 10. Si se detecta un conflicto, los desarrolladores reciben una alerta y resuelven el conflicto con una solicitud de fusión.	

Solución de problemas

Problema	Solución
Conflictos de sucursales	Un problema común que puede producirse con el modelo de Gitflow es cuando es necesario

Problema	Solución
	realizar una revisión en producción, pero el cambio correspondiente debe producirse en un entorno inferior, en el que otra rama modifica los mismos recursos. Te recomendamos que solo tengas una rama de lanzamiento activa a la vez. Si tiene más de una rama activa a la vez, es posible que los cambios en los entornos colisionen y que no pueda pasar una rama a producción.
Fusión	Las versiones deben volver a fusionarse con las principales y desarrollarse lo antes posible para volver a consolidar el trabajo en las ramas principales.
Aplasta la fusión	Usa una combinación de squash solo cuando vayas a fusionar de una `feature` rama a otra. `develop` El uso de combinaciones de calabazas en las ramas más altas causa dificultades cuando la fusión vuelve a caer en las ramas más bajas.

Recursos relacionados

Esta guía no incluye formación sobre Git; sin embargo, hay muchos recursos de alta calidad disponibles en Internet si necesitas esta formación. Te recomendamos que comiences por el sitio de documentación de Git.

Los siguientes recursos pueden ayudarte en tu proceso de ramificación de Gitflow en. Nube de AWS

AWS DevOps orientación

- AWS DevOps Orientación
- AWS Arquitectura de referencia para la canalización de despliegue
- ¿Qué es DevOps?

- DevOps recursos

guía de Gitflow

- El blog original de Gitflow (entrada del blog de Vincent Driessen)
- Flujo de trabajo de Gitflow (Atlassian)
- Gitflow en GitHub: Cómo usar los flujos de trabajo de Git Flow con repositorios GitHub basados (vídeo) YouTube
- Ejemplo de Git Flow Init (YouTube vídeo)
- La rama de lanzamiento de Gitflow de principio a fin (vídeo) YouTube

Otros recursos

Metodología de aplicaciones de doce factores (12factor.net)

Implemente una estrategia de ramificación troncal para entornos de cuentas múltiples DevOps

Creado por Mike Stephens (AWS) y Rayjan Wilson (AWS)

Repositorio de código: - multiaccount-devops git-branching-strategies-for	Entorno: producción	Tecnologías: desarrollo y pruebas de software DevOps; estrategia multicuenta
Servicios de AWS: AWS CodeArtifact CodeBuild; AWS CodeCommit; AWS CodeDeploy; AWS CodePipeline		

Resumen

Al gestionar un repositorio de código fuente, las diferentes estrategias de ramificación afectan a los procesos de desarrollo y publicación de software que utilizan los equipos de desarrollo. Algunos ejemplos de estrategias de ramificación habituales son Trunk, GitHub Flow y Gitflow. Estas estrategias utilizan diferentes ramas y las actividades que se realizan en cada entorno son diferentes. Organismos que están implementando DevOps procesos se beneficiarían de una guía visual que les ayude a entender las diferencias entre estas estrategias de ramificación. El uso de este elemento visual en su organización ayuda a los equipos de desarrollo a alinear su trabajo y seguir los estándares de la organización. Este patrón proporciona esta imagen y describe el proceso de implementación de una estrategia de ramificación troncal en su organización.

Este patrón forma parte de una serie de documentos sobre la elección e implementación de estrategias de DevOps ramificación para organizaciones con múltiples sucursales. Cuentas de AWS Esta serie está diseñada para ayudarlo a aplicar la estrategia correcta y las mejores prácticas desde el principio, a fin de optimizar su experiencia en la nube. Trunk es solo una posible estrategia de ramificación que su organización puede utilizar. Esta serie de documentación también cubre los modelos de ramificación de GitHub Flow y Gitflow. Si aún no lo has hecho, te recomendamos que revises Cómo elegir una estrategia de ramificación de Git para DevOps entornos de múltiples

cuentas antes de implementar la guía de este patrón. Usa la diligencia debida para elegir la estrategia de ramificación adecuada para tu organización.

Esta guía proporciona un diagrama que muestra cómo una organización podría implementar la estrategia Trunk. Se recomienda que consulte la Guía oficial de AWS DevOps Well-Architected para revisar las mejores prácticas. Este patrón incluye las tareas, los pasos y las restricciones recomendados para cada paso del DevOps proceso.

Requisitos previos y limitaciones

Requisitos previos

- Git, instalado. Se utiliza como herramienta de repositorio de código fuente.
- Draw.io, instalado. Esta aplicación se utiliza para ver y editar el diagrama.

Arquitectura

Arquitectura de destino

El siguiente diagrama se puede utilizar como un cuadrado de Punnett (Wikipedia). Alinee las ramas en el eje vertical con los AWS entornos en el eje horizontal para determinar qué acciones realizar en cada escenario. Los números indican la secuencia de las acciones del flujo de trabajo. En este ejemplo, se pasa de una `feature` sucursal a la implementación en producción.

Para obtener más información sobre los Cuentas de AWS entornos y las ramas en un enfoque troncal, consulta Cómo elegir una estrategia de ramificación de Git para entornos con varias cuentas DevOps .

Automatizar y escalar

La integración y la entrega continuas (CI/CD) son el proceso de automatización del ciclo de vida de las versiones de software. Automatiza gran parte o la totalidad de los procesos manuales que tradicionalmente se requerían para pasar del código nuevo a la producción desde un principio. Una canalización de CI/CD abarca los entornos sandbox, de desarrollo, de pruebas, de puesta en escena y de producción. En cada entorno, la canalización de CI/CD proporciona cualquier infraestructura necesaria para implementar o probar el código. Mediante el uso de la CI/CD, los equipos de desarrollo pueden realizar cambios en el código que luego se prueban e implementan

automáticamente. Los procesos de CI/CD también proporcionan control y protección a los equipos de desarrollo al garantizar la coherencia, los estándares, las mejores prácticas y unos niveles mínimos de aceptación para la aceptación y el despliegue de las funciones. Para obtener más información, consulte Practicar la integración continua y la entrega continua en. AWS

AWS ofrece un conjunto de servicios para desarrolladores diseñados para ayudarle a crear canalizaciones de CI/CD. Por ejemplo, AWS CodePipelinees un servicio de entrega continua totalmente gestionado que le ayuda a automatizar sus procesos de lanzamiento para obtener actualizaciones rápidas y fiables de las aplicaciones y la infraestructura. AWS CodeCommitestá diseñado para alojar de forma segura repositorios Git escalables y AWS CodeBuildcompila el código fuente, ejecuta pruebas y produce paquetes de ready-to-deploy software. Para obtener más información, consulte Herramientas para desarrolladores en. AWS

Herramientas

AWS servicios y herramientas

AWS proporciona un conjunto de servicios para desarrolladores que puede utilizar para implementar este patrón:

- AWS CodeArtifactes un servicio de repositorio de artefactos gestionado y altamente escalable que le ayuda a almacenar y compartir paquetes de software para el desarrollo de aplicaciones.
- AWS CodeBuildes un servicio de compilación totalmente gestionado que le ayuda a compilar código fuente, ejecutar pruebas unitarias y producir artefactos listos para su despliegue.
- AWS CodeCommites un servicio de control de versiones que te ayuda a almacenar y gestionar de forma privada los repositorios de Git, sin necesidad de gestionar tu propio sistema de control de código fuente.
- AWS CodeDeployautomatiza las implementaciones en Amazon Elastic Compute Cloud (Amazon EC2) o en instancias, AWS Lambda funciones locales o servicios de Amazon Elastic Container Service (Amazon ECS).
- AWS CodePipelinele ayuda a modelar y configurar rápidamente las diferentes etapas de una versión de software y a automatizar los pasos necesarios para publicar los cambios de software de forma continua.

Otras herramientas

- Draw.io Desktop: una aplicación para hacer diagramas de flujo y diagramas.

- Figma es una herramienta de diseño en línea diseñada para la colaboración. El repositorio de código contiene plantillas en formato.fig para Figma.

Repositorio de código

El archivo fuente del diagrama de este patrón está disponible en el repositorio GitHub Git Branching Strategy for Trunk. Incluye archivos en los formatos PNG, draw.io y Figma. Puede modificar estos diagramas para respaldar los procesos de su organización.

Prácticas recomendadas

Siga las mejores prácticas y recomendaciones de AWS DevOps Well-Architected Guidance y Eligiendo una estrategia de ramificación de Git para entornos de múltiples cuentas. DevOps Te ayudan a implementar de forma eficaz el desarrollo basado en Trunk, a fomentar la colaboración, a mejorar la calidad del código y a agilizar el proceso de desarrollo.

Epics

Revisión del flujo de trabajo de Trunk

Tarea	Descripción	Habilidades requeridas
Revise el proceso troncal estándar.	1. En el entorno sandbox, el desarrollador crea una `feature` rama a partir de la `main` rama y utiliza el patrón `feature/<ticket>_<initials>_<short description>` de nomenclatura. 2. El desarrollador desarrolla el código y lo despliega en el entorno sandbox de forma iterativa para completar el ticket. Nota: Si lo desea, el desarrollador puede crear	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	una `sandbox` rama para ejecutar una canalización automática de compilación o despliegue en el entorno sandbox. 3. El desarrollador crea una solicitud de fusión de una `feature` `main` rama a otra mediante una fusión automática. 4. Una canalización de integración y entrega continuas (CI/CD) crea y publica automáticamente los artefactos desde la `main` sucursal hasta el entorno de desarrollo. 5. Un aprobador aprueba manualmente el despliegue de los artefactos de lanzamiento en el entorno de desarrollo. 6. Un aprobador aprueba manualmente el despliegue de los artefactos de lanzamiento en el entorno de pruebas. 7. Un aprobador aprueba manualmente el despliegue de los artefactos de lanzamiento en el entorno provisional. 8. Un aprobador aprueba manualmente el despliegu	

Tarea	Descripción	Habilidades requeridas
	e de los artefactos de lanzamiento en el entorno de producción.	

Solución de problemas

Problema	Solución
Conflictos de sucursales	Un problema común que puede producirse con el modelo troncal es cuando es necesario realizar una revisión en producción, pero el cambio correspondiente debe producirse en una `feature` rama, donde se modifican los mismos recursos. Le recomendamos que fusione con frecuencia los cambios de `main` las ramas inferiores para evitar conflictos important es al `main` fusionarlos.

Recursos relacionados

Esta guía no incluye formación sobre Git; sin embargo, hay muchos recursos de alta calidad disponibles en Internet si necesitas esta formación. Te recomendamos que comiences por el sitio de documentación de Git.

Los siguientes recursos pueden ayudarlo en su viaje hacia la ramificación de Trunk en el Nube de AWS.

AWS DevOps orientación

- AWS DevOps Orientación
- AWS Arquitectura de referencia para la canalización de despliegue
- ¿Qué es DevOps?
- DevOps recursos

Guía troncal

- Desarrollo basado en troncales

Otros recursos

- Metodología de aplicaciones de doce factores (12factor.net)

Detecta automáticamente los cambios e inicia diferentes CodePipeline canalizaciones para un monorepo en CodeCommit

Creado por Helton Ribeiro (AWS), Petrus Batalha (AWS) y Ricardo Morais (AWS)

Repositorio de código: activadores de canalización múltiple de AWS CodeCommit monorepo	Entorno: PoC o piloto	Tecnologías: infraestructura, DevOps sin servidor
Servicios de AWS: AWS CodeCommit CodePipeline; AWS Lambda		

Resumen

Este patrón le ayuda a detectar automáticamente los cambios en el código fuente de una aplicación basada en monorepo AWS CodeCommit y, a continuación, a iniciar una canalización AWS CodePipeline que ejecute la automatización de la integración continua y la entrega continua (CI/CD) para cada microservicio. Este enfoque significa que cada microservicio de su aplicación basada en monorepo puede tener una canalización de CI/CD dedicada, lo que garantiza una mejor visibilidad, un intercambio de código más sencillo y una mayor colaboración, estandarización y capacidad de descubrimiento.

La solución descrita en este patrón no realiza ningún análisis de dependencia entre los microservicios del monorepo. Solo detecta los cambios en el código fuente e inicia la canalización de CI/CD correspondiente.

El patrón AWS Cloud9 se utiliza como entorno de desarrollo integrado (IDE) y AWS Cloud Development Kit (AWS CDK) para definir una infraestructura mediante dos AWS CloudFormation pilas: y. `MonoRepoStack` `PipelinesStack` La `MonoRepoStack` pila crea la entrada monorepo AWS CodeCommit y la AWS Lambda función que inicia las canalizaciones de CI/CD. La pila `PipelinesStack` define su infraestructura de canalizaciones.

Importante: El flujo de trabajo de este patrón es una prueba de concepto (PoC). Le recomendamos que lo use solo en un entorno de prueba. Si desea utilizar el enfoque de este patrón en un entorno

de producción, consulte las prácticas recomendadas de seguridad en IAM en la documentación AWS Identity and Access Management (IAM) y realice los cambios necesarios en sus funciones de IAM y. Servicios de AWS

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta activa. AWS
- AWS Command Line Interface (AWS CLI), instalada y configurada. Para obtener más información, consulte Instalación, actualización y desinstalación de AWS CLI en la AWS CLI documentación.
- Python 3 y `pip` instalados en su equipo local. Para obtener más información, consulte la Documentación de Python.
- AWS CDK, instalado y configurado. Para obtener más información, consulte Primeros pasos con el AWS CDK en la AWS CDK documentación.
- Un AWS Cloud9 IDE, instalado y configurado. Para obtener más información, consulte Configuración AWS Cloud9 en la AWS Cloud9 documentación.
- El repositorio de activadores multicanalización de GitHub AWS CodeCommit monorepo, clonado en su máquina local.
- Un directorio existente que contiene el código de la aplicación con el que desea crear e implementar. CodePipeline
- Familiaridad y experiencia con las DevOps mejores prácticas en el Nube de AWS. Para aumentar su familiaridad DevOps, puede utilizar el patrón Construir una arquitectura de acoplamiento flexible con microservicios utilizando DevOps prácticas y AWS Cloud9 en el AWS sitio web de orientación prescriptiva.

Arquitectura

El siguiente diagrama muestra cómo usar el AWS CDK para definir una infraestructura con dos AWS CloudFormation pilas: y. `MonoRepoStack` `PipelinesStack`

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El proceso de arranque utiliza el AWS CDK para crear las AWS CloudFormation pilas `MonoRepoStack` y. `PipelinesStack`

2. La `MonoRepoStack` pila crea el CodeCommit repositorio para la aplicación y la función `monorepo-event-handler` Lambda que se inicia después de cada confirmación.
3. La `PipelinesStack` pila crea las canalizaciones CodePipeline iniciadas por la función Lambda. Cada microservicio debe tener una canalización de infraestructura definida.
4. La canalización para `microservice-n` la inicia la función Lambda e inicia sus etapas de CI/CD aisladas que se basan en el código fuente de. CodeCommit
5. La canalización para `microservice-1` la inicia la función Lambda e inicia sus etapas de CI/CD aisladas que se basan en el código fuente de. CodeCommit

En el siguiente diagrama, se muestra el despliegue de las AWS CloudFormation pilas `MonoRepoStack` y `PipelinesStack` en una cuenta.

1. Un usuario cambia el código de uno de los microservicios de la aplicación.
2. El usuario transfiere los cambios de un repositorio local a un CodeCommit repositorio.
3. La actividad de envío inicia la función Lambda que recibe todos los envíos al repositorio. CodeCommit
4. La función Lambda lee un parámetro del almacén de parámetros, una capacidad de AWS Systems Manager, para recuperar el ID de confirmación más reciente. El parámetro tiene el formato de denominación:`/MonoRepoTrigger/{repository}/{branch_name}/LastCommit`. Si no se encuentra el parámetro, la función Lambda lee el último ID de confirmación del CodeCommit repositorio y guarda el valor devuelto en el almacén de parámetros.
5. Tras identificar el ID de confirmación y los archivos modificados, la función Lambda identifica las canalizaciones de cada directorio de microservicios e inicia la canalización requerida. CodePipeline

Herramientas

- AWS Cloud Development Kit (AWS CDK)es un marco de desarrollo de software para definir la infraestructura de nube en código y aprovisionarla mediante ella. AWS CloudFormation
- Python es un lenguaje de programación que permite trabajar con rapidez e integrar sistemas de forma más eficaz.

Código

El código fuente y las plantillas de este patrón están disponibles en el repositorio de activadores multicanalización de GitHub AWS CodeCommit monorepo.

Prácticas recomendadas

- Este ejemplo de arquitectura no incluye una solución de monitoreo para la infraestructura implementada. Si desea implementar esta solución en un entorno de producción, le recomendamos que habilite la supervisión. Para obtener más información, consulte Supervise sus aplicaciones sin servidor con CloudWatch Application Insights en la documentación AWS Serverless Application Model (AWS SAM).
- Al editar el código de muestra que proporciona este patrón, siga las prácticas recomendadas para desarrollar e implementar la infraestructura de nube de la AWS CDK documentación.
- Al definir las canalizaciones de microservicios, revise las prácticas recomendadas de seguridad de la AWS CodePipeline documentación.
- También puede comprobar las prácticas recomendadas en su AWS CDK código mediante la utilidad cdk-nag. Esta herramienta utiliza un conjunto de reglas, agrupadas por paquetes, para evaluar el código. Los paquetes disponibles son:
  - AWS Biblioteca de soluciones
  - Seguridad de la Ley de Portabilidad y Responsabilidad de los Seguros de Salud (HIPAA)
  - Instituto Nacional de Estándares y Tecnología (NIST) 800-53 rev 4
  - NIST 800-53 rev. 5
  - La norma de seguridad de datos del sector de pagos con tarjeta (PCI DSS), versión 3.2.1

Epics

Configuración del entorno

Tarea	Descripción	Habilidades requeridas
Cree un entorno virtual de Python.	En su AWS Cloud9 IDE, cree un entorno virtual de Python e instale las dependencias necesarias ejecutando el siguiente comando:	Desarrollador

Tarea	Descripción	Habilidades requeridas
	`make install`	
Arranca el Cuenta de AWS y Región de AWS para. AWS CDK	Inicie la región Cuenta de AWS y requerida ejecutando el siguiente comando: `make bootstrap account-id=<your-AWS-account-ID> region=<required-region>`	Desarrollador

Cómo añadir una nueva canalización para un microservicio

Tarea	Descripción	Habilidades requeridas
Añada su código de muestra al directorio de su aplicación.	Añada el directorio que contiene el código de la aplicación de muestra al `monorepo-sample` directorio del repositorio clonado de GitHub AWS CodeCommit monorepo multi-pipeline triggers.	Desarrollador
Edite el archivo `monorepo-main.json` .	Agrega el nombre del directorio del código de tu aplicación y el nombre de la canalización al `monorepo-main.json` archivo del repositorio clonado.	Desarrollador
Cree la canalización.	En el `Pipelines` directorio del repositorio, agrega la canalización `class` de	Desarrollador

Tarea	Descripción	Habilidades requeridas
	tu aplicación. El directori o contiene dos archivos de ejemplo `pipeline_ hotsite.py ypipeline_ demo.py` . Cada archivo tiene tres etapas: origen, compilaci ón e implementación. Puede copiar uno de los archivos y modificarlo según los requisitos de su aplicació n.	

Tarea	Descripción	Habilidades requeridas
Edite el archivo `monorepo_config.py` .	En `service_map` , añada el nombre del directorio de su aplicación y la clase que creó para la canalización. Por ejemplo, en el siguiente código, se muestra una definición de canalización en el directorio `Pipelines` que usa un archivo llamado `pipeline_mysample.py` con una clase `MySampleP ipeline` : `...` `# Pipeline definition imports` `from pipelines.pipeline_demo import DemoPipeline` `from pipelines.pipeline_hotsite import HotsitePipeline` `from pipelines.pipeline_mysample import MySampleP ipeline` `### Add your pipeline configuration here` `service_map: Dict[str, ServicePipeline] = {` `# folder-name -> pipeline-class` `'demo': DemoPipel ine(),` `'hotsite': HotsitePipeline(),`	Desarrollador

Tarea	Descripción	Habilidades requeridas
	`'mysample': MySamplePipeline() }`	

Implemente la MonoRepoStack pila

Tarea	Descripción	Habilidades requeridas
Despliegue la AWS CloudFormation pila.	Ejecute el `make deploy-core` comando para implementar la AWS CloudFormation `MonoRepoStack` pila con los valores de los parámetros predeterminados en el directorio raíz del repositorio clonado. Puede cambiar el nombre del repositorio si ejecuta el comando `make deploy-core monorepo-name=<repo_name>` . Nota: Puede implementar ambas canalizaciones simultáneamente mediante el comando `make deploy monorepo-name=<repo_name>` .	Desarrollador
Valide el CodeCommit repositorio.	Valide si sus recursos se crearon mediante la ejecución del comando `aws codecommit get-repos`	Desarrollador

Tarea	Descripción	Habilidades requeridas
	`itory --repository-name <repo_name>` . Importante: dado que la AWS CloudFormation pila crea el CodeCommit repositor io en el que se almacena el monorepo, no ejecute el `cdk destroy MonoRepoS tack` comando si ha empezado a introducir modificaciones en él.	
Valide los resultados de la AWS CloudFormation pila.	Valide que la AWS CloudForm ation `MonoRepoStack` pila se haya creado y configurado correctamente ejecutando el siguiente comando: `aws cloudformation list-stacks --stack-status-filter CREATE_COMPLETE --query 'StackSummaries[?StackName == 'MonoRepoStack']'`	Desarrollador

Implemente la PipelinesStack pila

Tarea	Descripción	Habilidades requeridas
Despliegue la AWS CloudFormation pila.	La AWS CloudFormation `PipelinesStack` pila debe desplegarse después de `MonoRepoStack` desplegar la. La pila aumenta de tamaño	Desarrollador

Tarea	Descripción	Habilidades requeridas
	cuando se añaden nuevos microservicios al código base del monorepo y se vuelve a implementar cuando se incorpora un nuevo microserv icio. Implemente la Pipelines Stack pila ejecutando el `make deploy-pipelines` comando. Nota: También puede ejecutar el comando `make deploy monorepo-name=<rep o_name>` para implement ar simultáneamente ambas canalizaciones. En el siguiente ejemplo de resultado, se muestra cómo la implementación `Pipelines Stacks` imprime las URL de los microservicios al final de la implementación: `Outputs: PipelinesStack.dem ourl = .cloudfront.net PipelinesStack.hotsi teurl = .cloudfro nt.net`	

Tarea	Descripción	Habilidades requeridas
Valide los resultados de la AWS CloudFormation pila.	Valide que la AWS CloudFormation `PipelinesStacks` pila se haya creado y configurado correctamente ejecutando el siguiente comando: `aws cloudformation list-stacks --stack-status-filter CREATE_COMPLETE UPDATE_COMPLETE --query 'StackSummaries[?StackName == 'PipelinesStack']'`	Desarrollador

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Elimina tus AWS CloudFormation pilas.	Ejecute el comando `make destroy`.	Desarrollador
Elimine los buckets de S3 para sus canalizaciones.	1. Inicie sesión en la consola AWS Management Consolede Amazon Simple Storage Service (Amazon S3) y ábrala. 2. Elimine los buckets de S3 que están asociados a sus canalizaciones y utilice el siguiente nombre: `pipelinesstack-codepipeline*`	Desarrollador

Solución de problemas

Problema	Solución
He encontrado problemas AWS CDK .	Consulte Solución de AWS CDK problemas comunes en la documentación de AWS CDK.
Inserté mi código de microservicio, pero la canalización de microservicios no funcionó.	Validación de la configuración Verifique la configuración de la sucursal: • Asegúrese de enviar el código a la rama correcta. Esta canalización está configura da para ejecutarse solo cuando se realizan cambios en la `main` rama. Los envíos a otras ramas no inician la canalización a menos que estén configurados específicamente. • Después de insertar el código, comprueba si la confirmación está visible AWS CodeCommit para asegurarte de que la inserción se ha realizado correctamente y de que la conexión entre tu entorno local y el repositorio está intacta. Actualiza tus credenciales si hay problemas al insertar el código. Valide los archivos de configuración: • Confirme que la `service_map` variable refleja `monorepo_config.py` con precisión la estructura de directorios actual de sus microservicios. Esta variable desempeña un papel crucial a la hora de mapear el envío de código a la canalización correspondiente. • Asegúrese de que `monorepo-main.json` esté actualizado para incluir el nuevo

Problema	Solución
	mapeo para su microservicio. Este archivo es esencial para que la canalización reconozca y gestione correctamente los cambios en el microservicio. Solución de problemas en la consola AWS CodePipeline comprueba: • En el AWS Management Console, confirma que estás en el Región de AWS lugar donde está alojada tu canalización. Abre la CodePipeline consola y comprueba si se ha iniciado la canalización correspondiente a tu microservicio. Análisis de errores: si la canalización se inició pero falló, revise los mensajes de error o los registros proporcionados por usted CodePipeline para saber qué es lo que ha fallado. AWS Lambda solución de problemas: • En la AWS Lambda consola, abra la función `monorepo-event-handler` Lambda. Compruebe que la función se haya iniciado en respuesta a la inserción del código. Análisis de registros: examine los registros de la función Lambda para detectar cualquier problema. Los registros pueden proporcionar información detallada sobre lo que ocurrió cuando se ejecutó la función y ayudar a

Problema	Solución
	identificar si la función procesó el evento según lo esperado.

Problema	Solución
Necesito volver a implementar todos mis microservicios.	Existen dos enfoques para forzar la redistribución de todos los microservicios. Elija la opción que mejor se adapte a sus necesidades. Método 1: Eliminar un parámetro del almacén de parámetros Este método implica eliminar un parámetro específico del almacén de parámetros de Systems Manager que rastrea el último ID de confirmación utilizado para la implementación. Al eliminar este parámetro, el sistema se ve obligado a volver a implementar todos los microservicios en el siguiente activador, ya que lo percibe como un estado nuevo. Pasos: 1. Busca la entrada específica del almacén de parámetros que contiene el ID de confirmación o un marcador de despliegue relacionado con tu monorepo. El nombre del parámetro sigue el formato: `"/MonoRepoTrigger/{repository}/{branch_name}/LastCommit"` 2. Considere la posibilidad de hacer una copia de seguridad del valor del parámetro si es crítico o si desea mantener un registro del estado de despliegue antes de restablecerlo. 3. Usa los AWS Management Console AWS CLI, o los SDK para eliminar el parámetro identificado. Esta acción restablece el marcador de despliegue. 4. Tras la eliminación, la siguiente inserción en el repositorio debería provocar que el

Problema	Solución
	sistema despliegue todos los microservicios, ya que buscará la última confirmación que tenga en cuenta para el despliegue. Ventajas: • Sencillo y rápido de implementar con unos pasos mínimos. • No es necesario realizar cambios arbitrari os en el código para iniciar las implement aciones. Desventajas: • Control menos detallado sobre el proceso de implementación. • Potencialmente riesgoso si el almacén de parámetros se utiliza para gestionar otras configuraciones críticas. Método 2: Inserte una confirmación en cada subcarpeta de monorepo Este método implica realizar un cambio menor e insertarlo en cada subcarpeta de microserv icios del monorepo para iniciar sus canalizac iones individuales. Pasos: 1. Enumere todos los microservicios del monorepo que necesitan ser redistribuidos. 2. Para cada microservicio, realice un cambio mínimo y sin impacto en su subcarpeta. Esto puede consistir en actualizar un `README`

Problema	Solución
	archivo, añadir un comentario en un archivo de configuración o realizar cualquier cambio que no afecte a la funcionalidad del servicio. 3. Confirme estos cambios con un mensaje claro (como «Inicie la redistribución de los microservicios») y envíelos al repositorio. Asegúrese de enviar los cambios a la rama que inicia la implementación. 4. Supervise las canalizaciones de cada microservicio para confirmar que se han iniciado y completado correctamente. Ventajas: • Proporciona un control detallado sobre los microservicios que se vuelven a implement ar. • Es más seguro porque no implica eliminar los parámetros de configuración que podrían usarse para otros fines. Desventajas: • Consume más tiempo, especialmente con una gran cantidad de microservicios. • Requiere realizar cambios de código innecesarios que podrían saturar el historial de confirmaciones.

Recursos relacionados

- Integración y entrega continuas (CI/CD) mediante CDK Pipelines (documentación)AWS CDK
- módulo aws-cdk/pipelines (referencia de la API)AWS CDK

Integre un repositorio de Bitbucket con AWS Amplify mediante AWS CloudFormation

Creado por Alwin Abraham (AWS)

Entorno: producción	Tecnologías: DevOps	Servicios de AWS: AWS Amplify; AWS CloudFormation

Resumen

AWS Amplify le ayuda a implementar y probar sitios web estáticos rápidamente sin tener que configurar la infraestructura que normalmente se requiere. Puede implementar el enfoque de este patrón si su organización quiere usar Bitbucket como control de código fuente, ya sea para migrar el código de una aplicación existente o para crear una nueva aplicación. Al utilizar AWS CloudFormation para configurar Amplify automáticamente, proporciona visibilidad de las configuraciones que utiliza.

Este patrón describe cómo crear una canalización y un entorno de implementación de integración y despliegue continuos (CI/CD) front-end mediante AWS CloudFormation para integrar un repositorio de Bitbucket con AWS Amplify. El enfoque del patrón significa que puede crear una canalización de front-end de Amplify para implementaciones repetibles.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de Amazon Web Services (AWS)
- Una cuenta de Bitbucket activa con acceso de administrador
- Acceder a un terminal que usa cURL o la aplicación Postman
- Familiaridad con Amplify
- Familiaridad con AWS CloudFormation
- Familiaridad con los archivos con formato YAML

Arquitectura

Pila de tecnología

- Amplify
- AWS CloudFormation
- Bitbucket

Herramientas

- AWS Amplify: Amplify ayuda a los desarrolladores a desarrollar e implementar aplicaciones móviles y web impulsadas por la nube.
- AWS CloudFormation: AWS CloudFormation es un servicio que le ayuda a modelar y configurar sus recursos de AWS para que pueda dedicar menos tiempo a gestionarlos y más a centrarse en las aplicaciones que se ejecutan en AWS.
- Bitbucket: Bitbucket es una solución de gestión de repositorios de Git diseñada para equipos profesionales. Le brinda un lugar central para administrar los repositorios de Git, colaborar en tu código fuente y guiarte a través del flujo de desarrollo.

Código

El `bitbucket-amplify.yml` archivo (adjunto) contiene la CloudFormation plantilla de AWS para este patrón.

Epics

Configurar el repositorio de Bitbucket

Tarea	Descripción	Habilidades requeridas
(Opcional) Cree un repositorio de Bitbucket.	1. Inicie sesión en su cuenta de Bitbucket y crea un repositorio nuevo. Para obtener más informaci ón al respecto, consulte Crear un repositorio de Git	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	en la documentación de Bitbucket. 2. Registrar el nombre del espacio de trabajo. Nota: también puede utilizar un repositorio de Bitbucket ya existente.	
Abra la configuración del espacio de trabajo.	1. Abra el espacio de trabajo y seleccione la pestaña Repositorio. 2. Seleccione el repositorio que desee integrar con AmplifyAmplify. 3. Seleccione el nombre del espacio de trabajo que está por encima del nombre del repositorio. 4. En la barra lateral, seleccione Configuración.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Crear un consumidor de OAuth.	1. En la sección Aplicaciones y funciones, seleccione Consumidores de OAuth y, a continuación, Agregar consumidor. 2. Escriba un nombre para la secuencia, por ejemplo, `Amplify Integration .` 3. Introduzca una URL de devolución de llamada. Aunque este campo es obligatorio, no se utiliza para completar la integración, por lo que el valor podría ser `http://localhost:3000` 4. Marque la casilla Se trata de un consumidor privado. 5. Elija los siguientes permisos: • Proyecto – `Read` • Repositorios – `Admin` • Solicitudes de extracción – `Read` • Webhooks, y `Read Write` 6. Deje las opciones predeterminadas para todos los demás campos y elija Enviar. 7. Registra la clave y el secreto que se generan.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Obtenga el token de acceso de OAuth.	1. Abra una ventana del terminal y ejecute el siguiente comando: `curl -X POST -u "KEY:SECRET" https://bitbucket.org/site/oauth2/access_token -d grant_type=client_credentials` Importante: sustituya `KEY` y `SECRET` por la clave y el secreto que grabaste anteriormente. 2. Registre el token de acceso sin utilizar las comillas. El token solo es válido durante un tiempo limitado y el tiempo predeterminado es de dos horas. Debe ejecutar la CloudFormation plantilla de AWS en este período de tiempo.	DevOps ingeniero

Cree e implemente el CloudFormation stack de AWS

Tarea	Descripción	Habilidades requeridas
Descargue la CloudFormation plantilla de AWS.	Descargue la CloudFormation plantilla de `bitbucket-amplify.yml` AWS (adjunta). Esta plantilla crea	

Tarea	Descripción	Habilidades requeridas
	la canalización de CI/CD en Amplify, además del proyecto y la sucursal de Amplify.	

Tarea	Descripción	Habilidades requeridas
Cree e implemente la CloudFormation pila de AWS.	1. Inicie sesión en la consola de administración de AWS en la región de AWS en la que desee realizar la implementación y abra la CloudFormation consola de AWS. 2. Seleccione Crear pila (con nuevos recursos) y, a continuación, Cargar un archivo de plantilla. 3. Cargue el archivo `bitbucket-amplify.yml` . 4. Seleccione Siguiente, introduzca un nombre de pila y, a continuación, introduzca los siguientes parámetros: • Token de acceso: pegue el token de acceso de OAuth que creó anteriormente. • URL del repositorio: añada la URL del repositorio del proyecto de Bitbucket. La URL tiene el siguiente formato: `https://bitbucket.org/<WORKSPACE_NAME>/<REPO_NAME>`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	• Nombre de la sucursal: debe coincidir con el nombre de una rama de su repositor io de Bitbucket. No es necesario que esta rama exista cuando ejecute la CloudFormation pila de AWS, pero es necesaria para implementar el código en el entorno. • Nombre del proyecto: este es el nombre que se debe asociar al proyecto Amplify. 5. Seleccione Siguiente y después Crear pilas.	

Pruebe la canalización de CI/CD

Tarea	Descripción	Habilidades requeridas
Implementar el código en la rama de su repositorio.	1. Clona tu repositorio de Bitbucket ejecutando el siguiente comando: `git clone https://bitbucket.org/<WORKSPACE_NAME>/<REPO_NAME>` 2. Consulte el nombre de la rama que se utilizó al ejecutar el CloudFormation	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	script de AWS. Para crear y comprobar una nueva rama, ejecute el comando `git checkout -b <BRANCH_NAME>` . Para revisar una rama existente , ejecute el comando `git checkout <BRANCH_NAME>` 3. Introduzca el código en la rama y envíelo a la rama remota ejecutando los comandos `git commit` y `git push`. 4. Amplify luego crea e implementa la aplicación. Para obtener más información sobre esto, consulte Comandos básicos de Git en la documentación de Bitbucket .	

Recursos relacionados

Métodos de autenticación (documentación de Atlassian)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Lance un CodeBuild proyecto en todas las cuentas de AWS mediante Step Functions y una función de proxy Lambda

Creado por Richard Milner-Watts (AWS) y Amit Anjarlekar (AWS)

Repositorio de código CodeBuild : Cross-Account Proxy	Entorno: producción	Tecnologías: DevOps gestión y gobierno; operaciones; sin servidor
Servicios de AWS: AWS CodeBuild; AWS Lambda; AWS Step Functions; AWS X-Ray; AWS CloudFormation		

Resumen

Este patrón demuestra cómo lanzar de forma asíncrona un CodeBuild proyecto de AWS en varias cuentas de AWS mediante AWS Step Functions y una función de proxy de AWS Lambda. Puedes usar la máquina de estados Step Functions de muestra del patrón para probar el éxito de tu CodeBuild proyecto.

CodeBuild le ayuda a lanzar tareas operativas mediante la interfaz de línea de comandos de AWS (AWS CLI) desde un entorno de ejecución totalmente gestionado. Puede cambiar el comportamiento de su CodeBuild proyecto en tiempo de ejecución anulando las variables de entorno. Además, se puede utilizar CodeBuild para gestionar los flujos de trabajo. Para obtener más información, consulte las herramientas del catálogo de servicios en el sitio web de AWS Workshop y Programe trabajos en Amazon RDS para PostgreSQL con AWS y EventBridge Amazon en el blog de bases de datos de CodeBuild AWS.

Requisitos previos y limitaciones

Requisitos previos

- Dos cuentas de AWS activas: una cuenta de origen para invocar una función de proxy de Lambda con Step Functions y una cuenta de destino para crear un CodeBuild proyecto de muestra remoto

Limitaciones

- Este patrón no se puede utilizar para copiar artefactos entre cuentas.

Arquitectura

En el siguiente diagrama, se muestra la arquitectura que crea este patrón.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. La máquina de estados Step Functions analiza el mapa de entrada suministrado e invoca la función proxy Lambda (`codebuild-proxy-lambda`) para cada cuenta, región y proyecto que haya definido.
2. La función de proxy Lambda utiliza AWS Security Token Service (AWS STS) para asumir una función de proxy de IAM (`codebuild-proxy-role`), que está asociada a una política de IAM (`codebuild-proxy-policy`) en la cuenta de destino.
3. Con el rol asumido, la función Lambda lanza el CodeBuild proyecto y devuelve el identificador del CodeBuild trabajo. La máquina de estado Step Functions realiza un bucle y sondea el CodeBuild trabajo hasta recibir un estado de éxito o fracaso.

La lógica de la máquina de estados se muestra en la siguiente imagen.

Pila de tecnología

- AWS CloudFormation
- CodeBuild
- IAM
- Lambda
- Step Functions
- X-Ray

Herramientas

- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- AWS CloudFormation Designer proporciona un editor JSON y YAML integrado que le ayuda a ver y editar CloudFormation plantillas.
- AWS CodeBuild es un servicio de compilación totalmente gestionado que le ayuda a compilar código fuente, ejecutar pruebas unitarias y producir artefactos listos para su implementación.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Step Functions es un servicio de orquestación sin servidor que le permite combinar funciones de Lambda AWS y otros servicios de AWS para crear aplicaciones esenciales desde el punto de vista empresarial.
- AWS X-Ray le ayuda a recopilar datos sobre las solicitudes que atiende su aplicación y proporciona herramientas que puede utilizar para ver, filtrar y obtener información sobre esos datos para identificar problemas y oportunidades de optimización.

Código

El código de muestra para este patrón está disponible en el repositorio de GitHub Cross Account CodeBuild Proxy. Este patrón utiliza la biblioteca AWS Lambda Powertools para Python para proporcionar funciones de registro y rastreo. Para obtener más información sobre esta biblioteca y sus utilidades, consulte Powertools for AWS Lambda (Python).

Prácticas recomendadas

1. Ajuste los valores del tiempo de espera en la máquina de estados Step Function para minimizar las solicitudes de sondeo sobre el estado del trabajo. Utilice el tiempo de ejecución previsto para el CodeBuild proyecto.
2. Ajusta la `MaxConcurrency` propiedad del mapa en Step Functions para controlar cuántos CodeBuild proyectos se pueden ejecutar en paralelo.

3. Si es necesario, revise el código de muestra para ver si está listo para la producción. Considera qué datos podría registrar la solución y si el CloudWatch cifrado predeterminado de Amazon es suficiente.

Epics

Crear la función proxy Lambda y el rol de IAM asociado en la cuenta de origen

Tarea	Descripción	Habilidades requeridas
Registrar los ID de las cuentas de AWS.	Los ID de cuenta de AWS son necesarios para configurar el acceso a todas las cuentas. Registre el ID de cuenta de AWS de sus cuentas de origen y destino. Para obtener más información, consulte Cómo encontrar el ID de su cuenta de AWS en la documentación de IAM.	AWS DevOps
Descargue las CloudForm ation plantillas de AWS.	1. Descargue la CloudForm ation plantilla de `sample_target_code build_template.yam l` AWS del GitHub repositorio para este patrón. 2. Descargue la CloudForm ation plantilla de `codebuild_lambda_p roxy_template.yaml` AWS del GitHub repositor io para este patrón.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	Nota: En las CloudFormation plantillas de AWS, `<SourceAccountId>` es el ID de la cuenta de AWS de la cuenta de origen y `<TargetAccountId>` es el ID de la cuenta de AWS de la cuenta de destino.	

Tarea	Descripción	Habilidades requeridas
Cree e implemente la CloudFormation pila de AWS.	1. Inicie sesión en la consola de administración de AWS de su cuenta de origen, abra la CloudFormation consola de AWS y, a continuación, elija Stacks. 2. Seleccione Crear pila y, a continuación, Con nuevos recursos (estándar). 3. Para Origen de plantilla, elija Cargar un archivo de plantilla. 4. En Cargar un archivo de plantilla, seleccione un archivo y, a continuac ión, el archivo descargad `ocodebuild_lambda_p roxy_template.yaml` . Seleccione Siguiente. 5. En Nombre de pila, especifique un nombre para la pila (por ejemplo, `codebuild-lambda-p roxy`). 6. Reemplace el parámetro `crossAccountTarget RoleArn` con su `<TargetAccountId>` (por ejemplo, `<arn:aws: iam::123456789012: role/proxy-lambda- codebuild-role>`). Nota: No es necesario que	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	actualice el valor predeterminado del parámetro **`targetCodeBuildProject`** . 7. Seleccione Siguiente, acepte las opciones de creación de pilas predeterminadas y, a continuación, Siguiente. 8. Seleccione la casilla Acepto que AWS CloudFormation podría crear recursos de IAM con nombres personalizados y, a continuación, seleccione Crear pila. Nota: Debe crear la CloudFormation pila de AWS para la función de proxy Lambda antes de crear cualquier recurso en las cuentas de destino. Al crear una política de confianza en una cuenta de destino, el rol de IAM pasa del nombre del rol a un identificador interno. Es la razón por la que el rol de IAM debe existir previamente.	

Tarea	Descripción	Habilidades requeridas
Confirme la creación de la función proxy y la máquina de estado.	1. Espere a que la CloudFormation pila de AWS alcance el estado CREATE_COMPLETE. Este proceso no debería tardar más de un minuto. 2. Abra la consola de AWS Lambda, seleccione Funciones, y encuentre la función `lambda-proxy-ProxyLambda-<GUID>` . 3. Abra la consola AWS Step Functions, seleccione máquinas de estado y, a continuación, busque la máquina de estados `sample-crossaccount-codebuild-state-machine` .	AWS DevOps

Cree un rol de IAM en la cuenta de destino y lance un proyecto de muestra CodeBuild

Tarea	Descripción	Habilidades requeridas
Cree e implemente la CloudFormation pila de AWS.	1. Inicie sesión en la consola de administración de AWS de su cuenta de destino, abra la CloudFormation consola de AWS y, a continuación, elija Stacks.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	2. Seleccione Crear pila y, a continuación, Con nuevos recursos (estándar). 3. Para Origen de plantilla, elija Cargar un archivo de plantilla. 4. En Cargar un archivo de plantilla, seleccione Elegir archivo y, a continuación, seleccione el archivo `sample_target_codebuild_template.yaml` . Seleccione Siguiente. 5. En Nombre de pila, especifique un nombre para la pila (por ejemplo:`sample-codebuild-stack`). 6. Reemplace el parámetro `crossAccountSourceRoleArn` con su `<SourceAccountId>` (por ejemplo, `<arn:aws:iam::123456789012:role/codebuild-proxy-lambda-role>`). 7. Seleccione Siguiente, acepte las opciones de creación de pilas predeterminadas y, a continuación, seleccione Siguiente. 8. Seleccione la casilla Acepto que AWS CloudFormation	

Tarea	Descripción	Habilidades requeridas
	podría crear recursos de IAM con nombres personalizados y, a continuación, seleccione Crear pila.	
Verifique la creación del CodeBuild proyecto de muestra.	1. Espere a que la CloudFormation pila de AWS alcance el estado CREATE_COMPLETE. Este proceso no debería tardar más de un minuto. 2. Abra la CodeBuild consola de AWS y busque el `sample-codebuild-project` proyecto.	AWS DevOps

Prueba de la función de proxy de Lambda entre cuentas

Tarea	Descripción	Habilidades requeridas
Lance la máquina de estado.	1. Inicie sesión en la consola de administración de AWS de su cuenta de origen, abra la consola AWS Step Functions y, a continuación, seleccione Máquinas de estado. 2. Seleccione la máquina de estados `sample-crossaccount-codebuild-state-machine` y, a continuación, Iniciar ejecución.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	3. En el editor de entrada, introduzca el siguiente JSON y `<TargetAccountID>` sustitúyalo por el ID de cuenta de AWS de la cuenta que contiene el CodeBuild proyecto. `{ "crossAccountTargetRoleArns": [ { "arn": "arn:aws:iam::<TargetAccountID>:role/proxy-lambda-codebuild-role", "region": "eu-west-1", "codeBuildProject": "sample-codebuild-project", "SampleValue1": "Value1", "SampleValue2": "Value2" } ] }` Nota: Los pares clave-valor se pasan como variables de entorno desde la función de la cuenta de origen al CodeBuild proyecto de la cuenta de destino. 4. Seleccione Iniciar ejecución.	

Tarea	Descripción	Habilidades requeridas
	5. En la pestaña Detalles de la página de la máquina de estados, compruebe si el Estado de ejecución está establecido como Correcto. Esto confirma que la máquina de estado se está ejecutando. Nota: La máquina de estados puede tardar unos 30 segundos en alcanzar el estado Correcto. 6. Para ver la salida y la entrada de un paso en la máquina de estados, amplíe ese paso en la sección Historial de eventos de ejecución. Por ejemplo, amplíe el paso Lambda - CodeBuild Proxy — Start. El resultado incluye detalles sobre las variables de entorno anuladas, la carga útil original y el identificador del trabajo. CodeBuild	

Tarea	Descripción	Habilidades requeridas
Valide las variables de entorno.	1. Inicie sesión en la consola de administración de AWS usando su cuenta de AWS . 2. Abra la CodeBuild consola de AWS, expanda Crear y, a continuación, elija Crear proyectos. 3. Elija el `sample-co debuild-project` proyecto y, a continuación, elija Ver detalles. 4. En la pestaña Historial de compilaciones, seleccion a la compilación más reciente del proyecto y, a continuación, selecciona Ver registros. 5. En la salida del registro, compruebe que las variables de entorno impresas en STDOUT coincidan con las variables de entorno de la máquina de estados de ejemplo de Step Functions.	AWS DevOps

Solución de problemas

Problema	Solución
La ejecución de Step Functions está tardando más de lo esperado.	Ajuste la `MaxConcurrency` propiedad del mapa en la máquina de estados Step Function

Problema	Solución
	para controlar cuántos CodeBuild proyectos se pueden ejecutar en paralelo.
La ejecución de los CodeBuild trabajos está tardando más de lo esperado.	1. Ajuste los valores del tiempo de espera en la máquina de estados Step Functions para minimizar las solicitudes de sondeo sobre el estado del trabajo. Utilice el tiempo de ejecución previsto para el CodeBuild proyecto. 2. Considere si CodeBuild es la herramienta adecuada que debe utilizar. Por ejemplo, el tiempo necesario para inicializar un CodeBuild trabajo puede ser considera blemente superior al de AWS Lambda. Si se requiere un alto rendimiento y tiempos de finalización rápidos, considere la posibilid ad de migrar la lógica empresarial a AWS Lambda y utilizar una arquitectura desplegab le.

Gestione las implementaciones azul/verde de microservicios en varias cuentas y regiones mediante los servicios de código de AWS y las claves multirregionales de AWS KMS

Creado por Balaji Vedagiri (AWS), Ashish Kumar (AWS), Faisal Shahdad (AWS), Anand Krishna Varanasi (AWS), Vanitha Dontireddy (AWS) y Vivek Thangamuthu (AWS)

Repositorio de código: ecs-blue-green-global - -codepipeline deployment-with-multiregion-cmk	Entorno: PoC o piloto	Tecnologías: DevOps; Contenedores y microservicios
Servicios de AWS: AWS CloudFormation CodeBuild ; AWS CodeDeploy; AWS CodePipeline; Amazon ECS		

Resumen

En este patrón se describe cómo implementar una aplicación de microservicios global desde una cuenta central de AWS en varias cuentas de carga de trabajo y regiones de acuerdo con una estrategia de implementación azul/verde. El patrón es compatible con lo siguiente:

- El software se desarrolla en una cuenta central, mientras que las cargas de trabajo y las aplicaciones se distribuyen en varias cuentas y regiones de AWS.
- Se utiliza una única clave multirregional del Sistema de administración de claves de AWS (AWS KMS) para el cifrado y el descifrado a fin de permitir la recuperación de desastres.
- La clave KMS es específica de cada región y debe mantenerse o crearse en tres regiones diferentes para los artefactos del proyecto. Una clave KMS multirregional facilita poder conservar el mismo ID de clave en todas las regiones.
- El modelo de ramificación del flujo de trabajo de Git se implementa con dos ramas (de desarrollo y principal) y el código se fusiona mediante solicitudes de extracción (pull requests, PR). La función de Lambda de AWS que se implementa desde esta pila crea una PR desde la rama de desarrollo hacia la rama principal. La fusión de PR con la rama principal inicia una CodePipeline canalización

de AWS, que organiza el flujo de integración y entrega continuas (CI/CD) y despliega las pilas en todas las cuentas.

Este patrón proporciona un ejemplo de configuración de infraestructura como código (IaC) mediante CloudFormation pilas de AWS para demostrar este caso de uso. La implementación azul/verde de los microservicios se implementa mediante AWS. CodeDeploy

Requisitos previos y limitaciones

Requisitos previos

- Cuatro cuentas de AWS activas:
  - Una cuenta de herramientas para administrar la canalización de código y mantener el CodeCommit repositorio de AWS.
  - Tres cuentas de carga de trabajo (de prueba) para implementar la carga de trabajo de los microservicios.
- Este patrón utiliza las siguientes regiones. Si desea utilizar otras regiones, debe realizar las modificaciones adecuadas en las pilas multirregionales de AWS CodeDeploy y AWS KMS.
  - Cuenta Tools (AWS CodeCommit): `ap-south-1`
  - Cuenta de carga de trabajo (de prueba) 1: `ap-south-1`
  - Cuenta de carga de trabajo (de prueba) 2: `eu-central-1`
  - Cuenta de carga de trabajo (de prueba) 3: `us-east-1`
- Tres buckets de Amazon Simple Storage Service (Amazon S3) para las regiones de implementación de cada cuenta de carga de trabajo. (Se denominan `S3BUCKETNAMETESTACCOUNT1`, `S3BUCKETNAMETESTACCOUNT2` y `S3BUCKETNAMETESTACCOUNT3` más adelante en este patrón).

  A modo de ejemplo, se pueden crear estos buckets en cuentas y regiones específicas con nombres de bucket únicos de la siguiente manera (reemplazar xxxx por un número aleatorio):

```
##In Test Account 1
aws s3 mb s3://ecs-codepipeline-xxxx-ap-south-1 --region ap-south-1
##In Test Account 2
aws s3 mb s3://ecs-codepipeline-xxxx-eu-central-1 --region eu-central-1
##In Test Account 3
aws s3 mb s3://ecs-codepipeline-xxxx-us-east-1 --region us-east-1
```

```
#Example
##In Test Account 1
aws s3 mb s3://ecs-codepipeline-18903-ap-south-1 --region ap-south-1
##In Test Account 2
aws s3 mb s3://ecs-codepipeline-18903-eu-central-1 --region eu-central-1
##In Test Account 3
aws s3 mb s3://ecs-codepipeline-18903-us-east-1 --region us-east-1
```

Limitaciones

El patrón utiliza AWS CodeBuild y otros archivos de configuración para implementar un microservicio de muestra. Si tiene un tipo de carga de trabajo diferente (por ejemplo, sin servidor), debe actualizar todas las configuraciones pertinentes.

Arquitectura

Pila de tecnología de destino

- AWS CloudFormation
- AWS CodeCommit
- AWS CodeBuild
- AWS CodeDeploy
- AWS CodePipeline

Arquitectura de destino

Automatizar y escalar

La configuración se automatiza mediante plantillas de CloudFormation pila de AWS (IaC). Se puede escalar fácilmente para varios entornos y cuentas.

Herramientas

Servicios de AWS

- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.

- AWS CodeBuild es un servicio de compilación totalmente gestionado que le ayuda a compilar código fuente, ejecutar pruebas unitarias y producir artefactos listos para su implementación.
- AWS CodeCommit es un servicio de control de versiones que le ayuda a almacenar y gestionar repositorios de Git de forma privada, sin necesidad de gestionar su propio sistema de control de código fuente.
- AWS CodeDeploy automatiza las implementaciones en Amazon Elastic Compute Cloud (Amazon EC2) o en instancias locales, funciones de AWS Lambda o servicios de Amazon Elastic Container Service (Amazon ECS).
- AWS le CodePipeline ayuda a modelar y configurar rápidamente las diferentes etapas de una versión de software y a automatizar los pasos necesarios para publicar cambios de software de forma continua.
- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable.
- Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores escalable y rápido que ayuda a ejecutar, detener y administrar contenedores en un clúster.
- AWS Key Management Service (AWS KMS) facilita poder crear y controlar claves criptográficas para proteger los datos.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Herramientas adicionales

- Git es un sistema de control de versiones distribuido y de código abierto que funciona con el CodeCommit repositorio de AWS.
- Docker es un conjunto de productos de plataforma como servicio (PaaS) que utiliza la virtualización a nivel del sistema operativo para entregar software en contenedores. Este patrón utiliza Docker para crear y probar imágenes de contenedores de forma local.
- cfn-lint y cfn-nag son herramientas de código abierto que le ayudan a revisar CloudFormation las pilas para detectar cualquier error o problema de seguridad.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub Global Blue/Green de múltiples regiones y cuentas.

Epics

Configurar las variables de entorno

Tarea	Descripción	Habilidades requeridas
Exporte las variables de entorno para CloudFormation el despliegue de pilas.	Defina las variables de entorno que se utilizarán como entrada en las CloudForm ation pilas más adelante en este patrón. 1. Actualice los nombres de los buckets que creó en las tres cuentas y regiones, tal y como se explicó anteriorm ente en la sección Requisito s previos: `export S3BUCKETN AMETESTACCOUNT1=<S 3BUCKETACCOUNT1> export S3BUCKETN AMETESTACCOUNT2=<S 3BUCKETACCOUNT2> export S3BUCKETN AMETESTACCOUNT3=<S 3BUCKETACCOUNT3>` 2. Defina una cadena de asignación al azar para crear buckets de artefactos, ya que los nombres de los buckets deben ser únicos en todo el mundo: `export BUCKETSTA RTNAME=ecs-codepip`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`eline-artifacts-19992` 3. Defina y exporte los ID de las cuentas y las regiones: `export TOOLSACCOUNT=<TOOLSACCOUNT>` `export CODECOMMITACCOUNT=<CODECOMMITACCOUNT>` `export CODECOMMITREGION=ap-south-1` `export CODECOMMITREPONAME=Poc` `export TESTACCOUNT1=<TESTACCOUNT1>` `export TESTACCOUNT2=<TESTACCOUNT2>` `export TESTACCOUNT3=<TESTACCOUNT3>` `export TESTACCOUNT1REGION=ap-south-1` `export TESTACCOUNT2REGION=eu-central-1` `export TESTACCOUNT3REGION=us-east-1` `export TOOLSACCOUNTREGION=ap-south-1` `export ECRREPOSITORYNAME=web`	

Package e implemente las CloudFormation pilas para la infraestructura

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Clone el repositorio de muestras en un nuevo repositorio de su lugar de trabajo: `##In work location` `git clone https://github.com/aws-samples/ecs-blue-green-global-deployment-with-multiregion-cmk-codepipeline.git`	AWS DevOps
Empaquete los recursos de Cloudformation.	En este paso, empaqueta los artefactos locales a los que hacen referencia las CloudFormation plantillas para crear los recursos de infraestructura necesarios para servicios como Amazon Virtual Private Cloud (Amazon VPC) y Application Load Balancer. Las plantillas están disponibles en la carpeta `Infra` del repositorio de código. `##In TestAccount1##` `aws cloudformation package \` `--template-file mainInfraStack.yaml \`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	--s3-bucket $S3BUCKETNAMETESTACCOUNT1 \ --s3-prefix infraStack \ --region $TESTACCOUNT1REGION \ --output-template-file infrastructure_${TESTACCOUNT1}.template ##In TestAccount2## aws cloudformation package \ --template-file mainInfraStack.yaml \ --s3-bucket $S3BUCKETNAMETESTACCOUNT2 \ --s3-prefix infraStack \ --region $TESTACCOUNT2REGION \ --output-template-file infrastructure_${TESTACCOUNT2}.template ##In TestAccount3## aws cloudformation package \ --template-file mainInfraStack.yaml \ --s3-bucket $S3BUCKETNAMETESTACCOUNT3 \ --s3-prefix infraStack \	

Tarea	Descripción	Habilidades requeridas
	`--region $TESTACCOUNT3REGION \` `--output-template-file infrastructure_${TESTACCOUNT3}.template`	
Valide las plantillas de paquetes.	Valide las plantillas de paquetes: `aws cloudformation validate-template \` `--template-body file://infrastructure_${TESTACCOUNT1}.template` `aws cloudformation validate-template \` `--template-body file://infrastructure_${TESTACCOUNT2}.template` `aws cloudformation validate-template \` `--template-body file://infrastructure_${TESTACCOUNT3}.template`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Implemente los archivos del paquete en las cuentas de carga de trabajo,	1. Actualice los valores de los marcadores de posición y los nombres de las cuentas en el script `infraParameters.json` según su configuración. 2. Implemente las plantillas de paquetes en sus tres cuentas de carga de trabajo. `##In TestAccount1##` `aws cloudformation deploy \` `--template-file infrastructure_${TESTACCOUNT1}.template \` `--stack-name mainInfrastack \` `--parameter-overrides file://infraParameters.json \` `--region $TESTACCOUNT1REGION \` `--capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM` `##In TestAccount2##` `aws cloudformation deploy \` `--template-file infrastructure_${TESTACCOUNT2}.template \` `--stack-name mainInfrastack \`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`--parameter-overrides file://infraParameters.json \` `--region $TESTACCOUNT2REGION \` `--capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM` `##In TestAccount3##` `aws cloudformation deploy \` `--template-file infrastructure_${TESTACCOUNT3}.template \` `--stack-name mainInfrastack \` `--parameter-overrides file://infraParameters.json \` `--region $TESTACCOUNT3REGION \` `--capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM`	

Insertar una imagen de muestra y escalar Amazon ECS

Tarea	Descripción	Habilidades requeridas
Pase una imagen de muestra a un repositorio de Amazon ECR.	Pase una imagen de muestra (NGINX) al repositorio Amazon Elastic Container Registry (Amazon ECR) denominado `web` (tal y como	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	se establece en los parámetros). Puede personalizar la imagen según sea necesario. Para iniciar sesión y configurar las credenciales para enviar una imagen a Amazon ECR, siga las instrucciones de la documentación de Amazon ECR. Los comandos son: `docker pull nginx` `docker images` `docker tag <imageid> aws_account_id.dkr.ecr.region.amazonaws.com/<web>:latest` `docker push <aws_account_id>.dkr.ecr.<region>.amazonaws.com/<web>:tag`	

Tarea	Descripción	Habilidades requeridas
Escale Amazon ECS y verifique el acceso.	1. Escale Amazon ECS para crear dos réplicas: `aws ecs update-service --cluster QA-Cluster --service Poc-Service --desired-count 2` donde `Poc-Service` se refiere a la aplicación de muestra. 2. Compruebe que se pueda acceder a los servicios desde el equilibrador de carga de aplicación mediante un nombre de dominio completo (FQDN) o un DNS desde un navegador o mediante el comando curl.	AWS DevOps

Configurar los servicios y recursos de código

Tarea	Descripción	Habilidades requeridas
Cree un CodeCommit repositorio en la cuenta de herramientas.	Cree un CodeCommit repositorio en la cuenta de herramientas mediante la `codecommit.yaml` plantilla, que se encuentra en la `code` carpeta del GitHub repositorio. Debe crear este repositorio solo en la única región en	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	la que planea desarrollar el código. `aws cloudformation deploy --stack-name codecommitrepoStack --parameter-overrides CodeCommitReponame=$CODECOMMITREPONAME \ ToolsAccount=$TOOLSACCOUNT --template-file codecommit.yaml --region $TOOLSACCOUNTREGION \ --capabilities CAPABILITY_NAMED_IAM`	

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3 para gestionar los artefactos generados por CodePipeline.	Cree un depósito de S3 para gestionar los artefactos generados CodePipeline mediante la `pre-reqs-bucket.yaml` plantilla, que se encuentra en la `code` carpeta del GitHub repositorio. Las pilas se deben implementar en las tres regiones y cuentas de carga de trabajo (prueba) y de herramientas. `aws cloudformation deploy --stack-name pre-reqs-artifacts-bucket --parameter-overrides BucketStartName=$BUCKETSTARTNAME \ TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT \ --template-file pre-reqs_bucket.yaml --region $TESTACCOUNT1REGION --capabilities CAPABILITY_NAMED_IAM`  `aws cloudformation deploy --stack-name pre-reqs-artifacts-bucket --parameter-overrides BucketSta`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	rtName=$BUCKETSTAR TNAME \ TestAccount1=$TE STACCOUNT1 TestAccou nt2=$TESTACCOUNT2 \ TestAccount3=$TE STACCOUNT3 CodeCommi tAccount=$CODECOMM ITACCOUNT ToolsAcco unt=$TOOLSACCOUNT \ --template-file pre- reqs_bucket.yaml --region $TESTACCO UNT2REGION --capabil ities CAPABILIT Y_NAMED_IAM aws cloudformation deploy --stack-name pre-reqs-artifacts -bucket --parameter- overrides BucketSta rtName=$BUCKETSTAR TNAME \ TestAccount1=$TE STACCOUNT1 TestAccou nt2=$TESTACCOUNT2 \ TestAccount3=$TE STACCOUNT3 CodeCommi tAccount=$CODECOMM ITACCOUNT ToolsAcco unt=$TOOLSACCOUNT \ --template-file pre- reqs_bucket.yaml --region $TESTACCO UNT3REGION --capabil ities CAPABILIT Y_NAMED_IAM aws cloudformation deploy --stack-name pre-reqs-artifacts	

Tarea	Descripción	Habilidades requeridas
	`-bucket --parameter-overrides BucketStartName=$BUCKETSTARTNAME \ TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT \ --template-file pre-reqs_bucket.yaml --region $TOOLSACCOUNTREGION --capabilities CAPABILITY_NAMED_IAM`	

Tarea	Descripción	Habilidades requeridas
Configure una clave KMS multirregional.	1. Cree una clave KMS multirregional con las claves principales y de réplica que CodePipeline utilizará. En nuestro ejemplo, `ToolsAccount1region - ap-south-1` será la región principal. `aws cloudformation deploy --stack-name ecs-codepipeline-pre-reqs-KMS \ --template-file pre-reqs_KMS.yaml --parameter-overrides \ TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT --region $TOOLSACCOUNTREGION` 2. Configure las variables CMKARN para transferirlas a los proyectos. CodeBuild Los valores están disponibles en la salida de la pila de plantillas ecs-codepipeline-pre-reqs -KMS (el ID de clave será el mismo en todas las regiones	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	y empezará por). `mrk-` Alternativamente, puede obtener los valores de CMKARN de la cuenta de herramientas. Expórtelos en todas las sesiones de la cuenta: `export CMKARN1=arn:aws:kms:ap-south-1:<TOOLSACCOUNTID>:key/mrk-xxx` `export CMKARN2=arn:aws:kms:eu-central-1:<TOOLSACCOUNTID>:key/mrk-xxx` `export CMKARN3=arn:aws:kms:us-east-1:<TOOLSACCOUNTID>:key/mrk-xxx` `export CMARNTOOLS=arn:aws:kms:ap-south-1:<TOOLSACCOUNTID>:key/mrk-xxx`	

Tarea	Descripción	Habilidades requeridas
Configure el CodeBuild proyecto en la cuenta de herramientas.	1. Utilice la `codebuild_IAM.yaml` plantilla de la `code` carpeta del GitHub repositorio para configurar AWS Identity and Access Management (IAM) para AWS CodeBuild en una sola región de la cuenta de herramientas: `#In ToolsAccount` `aws cloudformation deploy --stack-name ecs-codebuild-iam \` `--template-file codebuild_IAM.yaml --region $TOOLSACCOUNTREGION \` `--capabilities CAPABILITY_NAMED_IAM` 2. Utilice la `codebuild.yaml` plantilla CodeBuild para configurar su proyecto de compilación. Implemente esta plantilla en las tres regiones de la manera siguiente: `aws cloudformation deploy --stack-name ecscodebuildstack --parameter-overrides ToolsAccount=$TOOLSACCOUNT \` `CodeCommitRepoName=$CODECOMMITREPONAME`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	ECRRepositoryName= $ECRREPOSITORYNAME APPACCOUNTID=$TEST ACCOUNT1 \ TestAccount3=$TE STACCOUNT3 CodeCommi tRegion=$CODECOMMI TREGION CMKARN=$C MKARN1 \ --template-file codebuild.yaml --region $TESTACCO UNT1REGION --capabil ities CAPABILIT Y_NAMED_IAM aws cloudformation deploy --stack-name ecscodebuildstack -- parameter-overrides ToolsAccount=$TOOL SACCOUNT \ CodeCommitRepoName= $CODECOMMITREPONAME ECRRepositoryName= $ECRREPOSITORYNAME APPACCOUNTID=$TEST ACCOUNT2 \ TestAccount3=$TE STACCOUNT3 CodeCommi tRegion=$CODECOMMI TREGION CMKARN=$C MKARN2 \ --template-file codebuild.yaml --region $TESTACCO UNT2REGION --capabil ities CAPABILIT Y_NAMED_IAM aws cloudformation deploy --stack-name	

Tarea	Descripción	Habilidades requeridas
	ecscodebuildstack --parameter-overrides ToolsAccount=$TOOLSACCOUNT \ CodeCommitRepoName=$CODECOMMITREPONAME ECRRepositoryName=$ECRREPOSITORYNAME APPACCOUNTID=$TESTACCOUNT3 \ CodeCommitRegion=$CODECOMMITREGION CMKARN=$CMKARN3 \ --template-file codebuild.yaml --region $TESTACCOUNT3REGION --capabilities CAPABILITY_NAMED_IAM	

Tarea	Descripción	Habilidades requeridas
Configúrelo CodeDeploy en cuentas de carga de trabajo.	Utilice la `codedeploy.yaml` plantilla de la `code` carpeta del GitHub repositorio para configurar las tres cuentas CodeDeploy de carga de trabajo. La salida de `mainInfraStack` incluye los nombres de recursos de Amazon (ARN) del clúster Amazon ECS y el oyente del equilibrador de carga de aplicación. Nota: Los valores de las pilas de infraestructura ya se han exportado, por lo que las plantillas de CodeDeploy pilas los importan. `##WorkloadAccount1## aws cloudformation deploy --stack-name ecscodedeploystack \ --parameter-overrides ToolsAccount=$TOOLSACCOUNT mainInfrastackname=mainInfrastack \ --template-file codedeploy.yaml --region $TESTACCOUNT1REGION --capabilities CAPABILITY_NAMED_IAM` `##WorkloadAccount2##`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`aws cloudformation deploy --stack-name ecscodedeploystack \ --parameter-overrides ToolsAccount=$TOOLSACCOUNT mainInfrastackname=mainInfrastack \ --template-file codedeploy.yaml --region $TESTACCOUNT2REGION --capabilities CAPABILITY_NAMED_IAM` `##WorkloadAccount3## aws cloudformation deploy --stack-name ecscodedeploystack \ --parameter-overrides ToolsAccount=$TOOLSACCOUNT mainInfrastackname=mainInfrastack \ --template-file codedeploy.yaml --region $TESTACCOUNT3REGION --capabilities CAPABILITY_NAMED_IAM`	

Configúrelo CodePipeline en la cuenta de herramientas

Tarea	Descripción	Habilidades requeridas
Cree un proyecto de código en la cuenta de herramientas.	En la cuenta de herramientas, ejecute el comando:	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`aws cloudformation deploy --stack-name ecscodepipelinestack --parameter-overrides \ TestAccount1=$TESTACCOUNT1 TestAccount1Region=$TESTACCOUNT1REGION \ TestAccount2=$TESTACCOUNT2 TestAccount2Region=$TESTACCOUNT2REGION \ TestAccount3=$TESTACCOUNT3 TestAccount3Region=$TESTACCOUNT3REGION \ CMKARNTools=$CMKTROOLSARN CMKARN1=$CMKARN1 CMKARN2=$CMKARN2 CMKARN3=$CMKARN3 \ CodeCommitRepoName=$CODECOMMITREPONAME BucketStartName=$BUCKETSTARTNAME \ --template-file codepipeline.yaml --capabilities CAPABILITY_NAMED_IAM`	

Tarea	Descripción	Habilidades requeridas
Proporcione acceso CodePipeline y CodeBuild funciones en la política de claves de AWS KMS y en la política de bucket de S3.	1. Proporcione acceso CodePipeline y CodeBuild funciones en la política clave de AWS KMS: `aws cloudformation deploy --stack-name ecs-codepipeline-pre-reqs-KMS \ --template-file pre-reqs_KMS.yaml --parameter-overrides \ CodeBuildCondition=true TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT --region $TOOLSACCOUNTREGION` 2. Actualice la política de buckets de S3 para permitir el acceso a los CodeDeplo y roles CodePipeline y las funciones: `aws cloudformation deploy --stack-name pre-reqs-artifacts-bucket --parameter-overrides BucketStartName=$BUCKETSTARTNAME \`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	PutS3BucketPolicy=true TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT \ --template-file pre-reqs_bucket.yaml --region $TESTACCOUNT1REGION --capabilities CAPABILITY_NAMED_IAM aws cloudformation deploy --stack-name pre-reqs-artifacts-bucket --parameter-overrides BucketStartName=$BUCKETSTARTNAME \ PutS3BucketPolicy=true TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT \ --template-file pre-reqs_bucket.yaml --region $TESTACCOUNT2REGION --capabilities CAPABILITY_NAMED_IAM	

Tarea	Descripción	Habilidades requeridas
	aws cloudformation deploy --stack-name pre-reqs-artifacts-bucket --parameter-overrides BucketStartName=$BUCKETSTARTNAME \ PutS3BucketPolicy=true TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT \ --template-file pre-reqs_bucket.yaml --region $TESTACCOUNT3REGION --capabilities CAPABILITY_NAMED_IAM aws cloudformation deploy --stack-name pre-reqs-artifacts-bucket --parameter-overrides BucketStartName=$BUCKETSTARTNAME \ PutS3BucketPolicy=true TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT \	

Tarea	Descripción	Habilidades requeridas
	`--template-file pre-reqs_bucket.yaml --region $TOOLSACCOUNTREGION --capabilities CAPABILITY_NAMED_IAM`	

Llamar y probar el proyecto

Tarea	Descripción	Habilidades requeridas
Envía los cambios al CodeCommit repositorio.	1. Clone el CodeCommit repositorio que se creó en el `codecommitrepoStack` mediante el `git clone` comando, tal y como se describe en la CodeCommit documentación de AWS. 2. Actualice los artefactos de entrada con los detalles necesarios: • Archivo JSON: actualice `AccountID` en el archivo en tres lugares de este archivo. Cambie el nombre de los tres archivos para incluir los ID de las cuentas. • Archivos YAML: actualiza el ARN y la versión de la definición de la tarea. Cambie el nombre de los tres archivos para incluir los ID de las cuentas.	

Tarea	Descripción	Habilidades requeridas
	3. Modifique el archivo `index.html` para realizar algunos cambios menores en la página de inicio. 4. Copie los siguientes archivos en el repositorio y confirme: `index.html` `Dockerfile` `buildspec.yaml` `appspec_<accountid>.yaml (3 files - one per account )` `taskdef<accountid>.json (3 files - one per account)` 5. Inicie o reinicie el proyecto y verifique los resultados. 6. Acceda al servicio desde el equilibrador de carga de aplicación mediante un FQDN o un DNS y compruebe que se hayan implementado las actualizaciones.	

Limpieza

Tarea	Descripción	Habilidades requeridas
Limpie todos los recursos implementados.	1. Reduzca verticalmente Amazon ECS a cero instancias:	

Tarea	Descripción	Habilidades requeridas
	`aws ecs update-service --cluster QA-Cluster --service Poc-Service --desired-count 0` 2. Elimine las CloudFormation pilas de cada cuenta y región: `##In Tools Account##` `aws cloudformation delete-stack --stack-name ecscodepipelinestack --region $TOOLSACCOUNTREGION` `aws cloudformation delete-stack --stack-name ecscodebuildstack --region $TESTACCOUNT1REGION` `aws cloudformation delete-stack --stack-name ecscodebuildstack --region $TESTACCOUNT2REGION` `aws cloudformation delete-stack --stack-name ecscodebuildstack --region $TESTACCOUNT3REGION` `aws cloudformation delete-stack --stack-name ecs-codepipeline-pre-reqs-KMS --region $TOOLSACCOUNTREGION` `aws cloudformation delete-stack --stack-name codecommi`	

Tarea	Descripción	Habilidades requeridas
	trepoStack --region $TOOLSACCOUNTREGION aws cloudformation delete-stack -- stack-name pre-reqs- artifacts-bucket --region $TESTACCO UNT1REGION aws cloudformation delete-stack -- stack-name pre-reqs- artifacts-bucket --region $TESTACCO UNT2REGION aws cloudformation delete-stack -- stack-name pre-reqs- artifacts-bucket --region $TESTACCO UNT3REGION aws cloudformation delete-stack -- stack-name pre-reqs- artifacts-bucket --region $TOOLSACC OUNTREGION aws cloudformation delete-stack -- stack-name ecs-codeb uild-iam --region $TOOLSACCOUNTREGION ##NOTE: Artifact buckets will not get deleted if there are artifacts so it has to be emptied manually before deleting.##	

Tarea	Descripción	Habilidades requeridas
	`` ##In Workload / Test Accounts## ##Account:1## aws cloudformation delete-stack -- stack-name ecscodede ploystack --region $TESTACCOUNT1REGION aws cloudformation delete-stack -- stack-name mainInfra stack --region $TESTACCOUNT1REGION ##Account:2## aws cloudformation delete-stack -- stack-name ecscodede ploystack --region $TESTACCOUNT2REGION aws cloudformation delete-stack -- stack-name mainInfra stack --region $TESTACCOUNT2REGION ##Account:3## aws cloudformation delete-stack -- stack-name ecscodede ploystack --region $TESTACCOUNT3REGION aws cloudformation delete-stack -- stack-name mainInfra stack --region $TESTACCOUNT3REGION ##NOTE: Amazon ECR (web) will not get deleted if the registry still includes images. It can be manually ```	

Tarea	Descripción	Habilidades requeridas
	`cleaned up if not required.`	

Solución de problemas

Problema	Solución
Los cambios realizados en el repositorio no se están implementando.	• Comprueba los CodeBuild registros para ver si hay errores en la acción de compilación de Docker. Para obtener más información, consulta la CodeBuild documentación. • Compruebe la CodeDeploy implement ación para ver si hay algún problema con la implementación de Amazon ECS.

Recursos relacionados

- Insertar una imagen de Docker (documentación de Amazon ECR)
- Conectarse a un CodeCommit repositorio de AWS (CodeCommit documentación de AWS)
- Solución de problemas de AWS CodeBuild (CodeBuild documentación de AWS)

Supervise los repositorios de Amazon ECR en busca de permisos comodín mediante AWS y AWS Config CloudFormation

Creado por Vikrant Telkar (AWS), Sajid Momin (AWS) y Wassim Benhallam (AWS)

Entorno: producción	Tecnologías: DevOps contenedores y microservicios	Servicios de AWS: AWS CloudFormation; AWS Config; Amazon ECR; Amazon SNS; AWS Lambda

Resumen

En la nube de Amazon Web Services (AWS), Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedores administrado que admite repositorios privados con permisos basados en recursos mediante AWS Identity and Access Management (IAM).

IAM admite el comodín "*" en los atributos tanto de recurso como de acción, lo que facilita la selección automática de varios elementos coincidentes. En su entorno de pruebas, puede permitir que todos los usuarios autenticados de AWS accedan a un repositorio de Amazon ECR utilizando el permiso comodín `ecr:*` en un elemento de entidad principal de la declaración de política del repositorio. El permiso comodín `ecr:*` puede resultar útil a la hora de desarrollar y realizar pruebas en cuentas de desarrollo que no pueden acceder a sus datos de producción.

Sin embargo, debe asegurarse de que el permiso comodín `ecr:*` no se utilice en sus entornos de producción, ya que puede provocar graves vulnerabilidades de seguridad. El enfoque de este patrón le ayuda a identificar los repositorios de Amazon ECR que contienen el permiso comodín `ecr:*` en las declaraciones de política de repositorios. El patrón proporciona los pasos y una CloudFormation plantilla de AWS para crear una regla personalizada en AWS Config. A continuación, una función de Lambda de AWS supervisa las declaraciones de política del repositorio de Amazon ECR para detectar los permisos comodín `ecr:*`. Si encuentra declaraciones de política de repositorios no conformes, Lambda notifica a AWS Config que envíe un evento a EventBridge Amazon y, a continuación, inicia un tema del EventBridge Amazon Simple Notification Service (Amazon SNS). El tema SNS le notifica por correo electrónico sobre las declaraciones no conformes con la política de repositorios.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada. Para obtener más información, consulte Instalar, actualizar y desinstalar la CLI de AWS en la documentación de AWS CLI.
- Un repositorio de Amazon ECR existente con una declaración de política adjunta, instalado y configurado en su entorno de pruebas. Para obtener más información al respecto, consulte Creación de un repositorio privado y Configuración de una declaración de política de repositorio en la documentación de Amazon ECR.
- AWS Config, configurado en la región de AWS que prefiera. Para obtener más información al respecto, consulte Introducción a AWS Config en la documentación de AWS Config.
- El archivo `aws-config-cloudformation.template` (adjunto), descargado en su equipo local.

Limitaciones

- La solución de este patrón es regional y sus recursos se deben crear en la misma región.

Arquitectura

El siguiente diagrama muestra cómo AWS Config evalúa las declaraciones de política de repositorios de Amazon ECR.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. AWS Config inicia una regla personalizada.
2. La regla personalizada invoca una función de Lambda para evaluar el cumplimiento de las declaraciones de política del repositorio de Amazon ECR. A continuación, la función de Lambda identifica las declaraciones no conformes con la política del repositorio.
3. La función de Lambda envía el estado de no conformidad a AWS Config.
4. AWS Config envía un evento a EventBridge.

5. EventBridge publica las notificaciones de incumplimiento en un tema de SNS.
6. Amazon SNS le envía una alerta por correo electrónico a usted o a un usuario autorizado.

Automatizar y escalar

La solución de este patrón puede supervisar cualquier número de declaraciones de política del repositorio de Amazon ECR, pero todos los recursos que desee evaluar deben ser creados en la misma región.

Herramientas

- AWS CloudFormation: AWS le CloudFormation ayuda a modelar y configurar sus recursos de AWS, a aprovisionarlos de forma rápida y coherente y a gestionarlos durante todo su ciclo de vida. Facilita poder usar una plantilla para describir los recursos y sus dependencias, y lanzarlos y configurarlos juntos como una pila, en lugar de administrarlos de forma individual. Puede administrar y aprovisionar pilas en varias cuentas y regiones de AWS.
- AWS Config: AWS Config proporciona una visión detallada de la configuración de los recursos de AWS de su cuenta de AWS. Esto incluye cómo se relacionan los recursos entre sí y cómo se han configurado en el pasado, para que pueda ver cómo las configuraciones y las relaciones cambian a lo largo del tiempo.
- Amazon ECR: Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado por AWS que es seguro, escalable y fiable. Amazon ECR admite repositorios privados con permisos basados en recursos mediante IAM.

- Amazon EventBridge: Amazon EventBridge es un servicio de bus de eventos sin servidor que puede utilizar para conectar sus aplicaciones con datos de diversas fuentes. EventBridge ofrece un flujo de datos en tiempo real desde sus aplicaciones, aplicaciones de software como servicio (SaaS) y servicios de AWS a objetivos como las funciones de AWS Lambda, los puntos de enlace de invocación HTTP que utilizan destinos de API o los buses de eventos de otras cuentas.
- AWS Lambda es un servicio informático que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo. Solo pagará por el tiempo de computación que consuma, no se aplican cargos cuando el código no se está ejecutando.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) coordina y gestiona la entrega o el envío de mensajes entre publicadores y clientes, incluyendo los servidores web y las direcciones

de correo electrónico. Los suscriptores reciben todos los mensajes publicados de los temas a los que están suscritos y todos los suscriptores de un tema reciben los mismos mensajes.

Código

El código de este patrón está disponible en el archivo `aws-config-cloudformation.template` (adjunto).

Epics

Cree la CloudFormation pila de AWS

Tarea	Descripción	Habilidades requeridas
Cree la CloudFormation pila de AWS.	Cree una CloudFormation pila de AWS ejecutando el siguiente comando en la CLI de AWS: `$ aws cloudformation create-stack --stack-name=AWSConfigECR \ --template-body file://aws-config-cloudformation.template \ --parameters ParameterKey=<email>,ParameterValue=<myemail@example.com> \ --capabilities CAPABILITY_NAMED_IAM`	AWS DevOps

Probar la regla personalizada de AWS Config

Tarea	Descripción	Habilidades requeridas
Pruebe la regla personalizada de AWS Config.	1. Inicie sesión en la consola de administración de AWS, abra la consola de AWS Config y, a continuación, seleccione Recursos. 2. En la página de Inventari o de recursos, puede filtrar por categoría de recurso, tipo de recurso y estado de conformidad. 3. Un repositorio de Amazon ECR que contiene `ecr:*` es `NON-COMPLIANT?` y un repositorio de Amazon ECR que no contiene `ecr:*` es `COMPLIANT` . 4. La dirección de correo electrónico suscrita al tema de SNS recibe notificac iones si un repositorio de Amazon ECR contiene declaraciones de políticas no conformes.	AWS DevOps

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Realice acciones personalizadas a partir de CodeCommit eventos de AWS

Creado por Abdullahi Olaoye (AWS)

Entorno: PoC o piloto	Tecnologías: DevOps Gestión y gobierno	Servicios de AWS: AWS CodeCommit; Amazon SNS

Resumen

Cuando utiliza un CodeCommit repositorio de AWS para almacenar código, es posible que desee monitorizar el repositorio e iniciar un flujo de trabajo de acciones cuando se produzcan eventos específicos. Por ejemplo, es posible que desee enviar una notificación por correo electrónico cuando un usuario comente una línea de código en una confirmación, o iniciar una función de AWS Lambda para realizar escaneos de seguridad del contenido del repositorio tras una confirmación. Este patrón describe los pasos para configurar un CodeCommit repositorio para acciones personalizadas. El patrón utiliza las reglas de CodeCommit notificación de AWS para capturar los eventos de interés y, a continuación, los envía a un destino configurado.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Familiaridad con los comandos de Git.
- AWS CodeCommit, configúrelo. Para obtener instrucciones, consulte Configuración de AWS CodeCommit.
- (Recomendado) Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada. Consulte Introducción a AWS CLI para obtener instrucciones.

Arquitectura

Herramientas

Servicios de AWS

- AWS CodeCommit es un servicio de control de código fuente totalmente gestionado que aloja repositorios seguros basados en Git. Facilita a los equipos la colaboración en el código en un ecosistema seguro y altamente escalable. CodeCommit elimina la necesidad de operar su propio sistema de control de código fuente o preocuparse por escalar su infraestructura
- Amazon Simple Notification Service (Amazon SNS) es un servicio web que permite a las aplicaciones, los usuarios finales y los dispositivos enviar y recibir al instante notificaciones desde la nube. Amazon SNS proporciona temas (canales de comunicación) para mensajes push de alto rendimiento. many-to-many Al utilizar los temas de Amazon SNS, los publicadores pueden distribuir mensajes a un gran número de suscriptores para su procesamiento en paralelo, incluidas las colas de Amazon Simple Queue Service (Amazon SQS), las funciones de AWS Lambda y los webhooks HTTP/S. También puede utilizar Amazon SNS para enviar notificaciones a usuarios finales mediante notificaciones push para móvil, SMS y correo electrónico.

Epics

Configure un repositorio CodeCommit

Tarea	Descripción	Habilidades requeridas
Crea un CodeCommit repositorio.	Utilice la CodeCommit consola o la AWS CLI para crear un CodeCommit repositorio. Para obtener instrucciones, consulte Crear un CodeCommit repositorio.	DevOps ingeniero
Envía el contenido al CodeCommit repositorio.	Después de crear el repositorio, añada contenido mediante comandos de Git. Puede migrar el contenido de un repositorio de Git existente, o bien contenido local sin control de versiones desde su	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	computadora. Para obtener instrucciones, consulte Añadir archivos a su repositorio o Migrar a AWS CodeCommit.	

Configurar Amazon SNS

Tarea	Descripción	Habilidades requeridas
Cree un tema de SNS.	Este tema de SNS recibe los eventos de CodeCommit. Para obtener instrucciones, consulte Crear un tema de Amazon SNS.	Arquitecto e ingeniero de nube DevOps
Cree un recurso para llevar a cabo una acción personali zada.	Para que se lleve a cabo la acción personalizada, debe crear el recurso correspon diente. Por ejemplo, si su acción personalizada es ejecutar código de Lambda y enviar mensajes a una cola de SQS, debe crear la función de Lambda y la cola de SQS. Ciertas acciones, como las notificaciones por correo electrónico y SMS, no requieren recursos. Para obtener más información, consulte la documentación de AWS correspondiente al tipo de recurso que va a crear.	Arquitecto de nube, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Suscriba el recurso de acción personalizada al tema de SNS.	En función de la acción personalizada, se creará una suscripción para el protocolo correspondiente. Por ejemplo, suscribirá una dirección de correo electrónico para recibir notificaciones por correo electrónico, una función de Lambda para ejecutar código personalizado o una cola de SQS para enviar eventos a Amazon SQS. En protocolos de suscripción como correo electrónico y SMS, deberá confirmar la suscripción desde el enlace que se envía al correo electrónico o al número de teléfono, respectivamente. Para obtener más instrucciones, consulte Suscribirse a un tema de Amazon SNS.	Arquitecto de nube, DevOps ingeniero

Configuración de las reglas de notificación

Tarea	Descripción	Habilidades requeridas
Cree la regla de notificación para el CodeCommit repositorio.	Para crear la regla de notificación, seleccione los eventos de Git que deben iniciar la notificación, seleccione el tema de SNS como tipo de destino y, a continuación, seleccione el tema de SNS que creó anteriormente.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	También puede configura r varios destinos para el repositorio. Para obtener más instrucciones, consulte Crear una regla de notificación.	
Pruebe las acciones personali zadas.	Realice uno de los eventos que ha configurado para iniciar la notificación. Por ejemplo, crea una solicitud de extracción si seleccionó ese evento como desencade nante. Debería ver su acción personalizada en ejecución . Por ejemplo, si se suscribió para recibir el tema SNS por correo electrónico, debería recibir una notificación por correo electrónico.	DevOps ingeniero

Recursos relacionados

- CodeCommit Documentación de AWS
- Documentación de Amazon SNS
- Documentación de Git

Publica CloudWatch las métricas de Amazon en un archivo CSV

Creado por Abdullahi Olaoye (AWS)

Entorno: PoC o piloto	Tecnologías: DevOps	Servicios de AWS: Amazon CloudWatch

Resumen

Este patrón utiliza un script de Python para recuperar CloudWatch las métricas de Amazon y convertir la información de las métricas en un archivo de valores separados por comas (CSV) para mejorar la legibilidad. El script toma como argumento obligatorio el servicio de AWS cuyas métricas deben recuperarse. Puede especificar la región de AWS y el perfil de credenciales de AWS como argumentos opcionales. Si no especifica esos argumentos, el script utilizará la región y el perfil predeterminados configurados para la estación de trabajo en la que se ejecuta el script. Una vez ejecutado, el script genera y almacena un archivo CSV en el mismo directorio.

Consulte la sección Adjuntos para ver el script y los archivos asociados que se proporcionan con este patrón.

Requisitos previos y limitaciones

Requisitos previos

- Python 3.x
- Interfaz de la línea de comandos de AWS (AWS CLI)

Limitaciones

El script en estos momentos admite los siguientes servicios de AWS:

- AWS Lambda
- Amazon Elastic Compute Cloud (Amazon EC2)
  - De forma predeterminada, el script no recopila métricas de volúmenes de Amazon Elastic Block Store (Amazon EBS). Para recopilar las métricas de Amazon EBS, debe modificar el archivo adjunto `metrics.yaml`.

- Amazon Relational Database Service (Amazon RDS)
  - Sin embargo, el script no es compatible con Amazon Aurora.
- Equilibrador de carga de aplicación
- Equilibrador de carga de red
- Amazon API Gateway

Herramientas

- Amazon CloudWatch es un servicio de monitoreo creado para DevOps ingenieros, desarrolladores, ingenieros de confiabilidad de sitios (SRE) y administradores de TI. CloudWatch proporciona datos e información procesable para ayudarlo a monitorear sus aplicaciones, responder a los cambios de rendimiento en todo el sistema, optimizar la utilización de los recursos y obtener una visión unificada del estado operativo. CloudWatch recopila datos operativos y de supervisión en forma de registros, métricas y eventos, y proporciona una vista unificada de los recursos, las aplicaciones y los servicios de AWS que se ejecutan en AWS y en servidores locales.

Epics

Instalar y configurar los requisitos previos

Tarea	Descripción	Habilidades requeridas
Instalar los requisitos previos.	Ejecute el siguiente comando: `$ pip3 install -r requirements.txt`	Desarrollador
Configure la CLI de AWS.	Ejecute el siguiente comando: `$ aws configure`	Desarrollador

Configurar el script de Python

Tarea	Descripción	Habilidades requeridas
Abra el script.	Para cambiar la configuración predeterminada del script, abra `metrics.yaml` .	Desarrollador
Defina el período del script.	Este es el período de tiempo para realizar la búsqueda. El período predeterminado es de 5 minutos (300 segundos) . Puede cambiar el período de tiempo, pero tenga en cuenta las siguientes limitaciones: • Si el valor de horas que especificó es de entre 3 horas y 15 días atrás, utilice un múltiplo de 60 segundos (1 minuto) para el período. • Si el valor de horas que especificó es de entre 15 horas y 63 días atrás, utilice un múltiplo de 300 segundos (5 minutos) para el período. • Si el valor de horas que especificó es mayor que 63 días atrás, utilice un múltiplo de 3.600 segundos (1 hora) para el período. De lo contrario, la operación de la API no devolverá ningún punto de datos.	Desarrollador

Tarea	Descripción	Habilidades requeridas
Defina las horas del script.	Este valor especifica cuántas horas de métricas desea obtener. El valor predeterm inado es una hora. Para recuperar métricas de varios días, proporcione el valor en horas. Por ejemplo, para 2 días, especifique 48.	Desarrollador
Cambie los valores de las estadísticas del script.	(Opcional) El valor de las estadísticas globales es `Average`, que se utiliza al buscar métricas que no tienen asignado un valor estadístico específico. El script admite los valores estadísticos `Maximum`, `SampleCount` y `Sum`.	Desarrollador

Ejecute el script de Python

Tarea	Descripción	Habilidades requeridas
Ejecute el script.	Utilice el siguiente comando: `$ python3 cwreport.py <service>` Para ver una lista de los valores del servicio y los `region` opcionales y parámetros `profile`, ejecute el siguiente comando:	Desarrollador

Tarea	Descripción	Habilidades requeridas
	`$ python3 cwreport.py -h` Para más información sobre los parámetros opcionales, consulte la sección Informaci ón adicional.	

Recursos relacionados

- Configuración de la CLI de AWS
- Uso de CloudWatch las métricas de Amazon
- CloudWatch Documentación de Amazon
- Métricas de EC2 CloudWatch
- Métricas de AWS Lambda
- Métricas de Amazon RDS
- Métricas del Equilibrador de carga de aplicación
- Métricas del Equilibrador de carga de red
- Métricas de Amazon API Gateway

Información adicional

Uso de scripts

```
$ python3 cwreport.py -h
```

Ejemplo de sintaxis

```
python3 cwreport.py <service> <--region=Optional Region> <--profile=Optional credential
 profile>
```

Parámetros

- servicio (obligatorio): el servicio en el que desea ejecutar el script. El script admite actualmente los siguientes servicios: AWS Lambda, Amazon EC2, Amazon RDS, Equilibrador de carga de aplicación, Equilibrador de carga de red y API Gateway.
- región (opcional): la región de AWS de la que se van a obtener las métricas. La región predeterminada es `ap-southeast-1`.
- perfil (opcional): el perfil con nombre de la CLI de AWS que se va a utilizar. Si no se especifica este parámetro, se utiliza el perfil de credenciales configurado por defecto.

Ejemplos

- Para utilizar la región predeterminada `ap-southeast-1` y las credenciales configuradas de forma predeterminada para obtener las métricas de Amazon EC2: `$ python3 cwreport.py ec2`
- Para especificar una región y obtener las métricas de API Gateway: `$ python3 cwreport.py apigateway --region us-east-1`
- Para especificar un perfil de AWS y obtener las métricas de Amazon EC2: `$ python3 cwreport.py ec2 --profile testprofile`
- Para especificar región y perfil para obtener las métricas de Amazon EC2: `$ python3 cwreport.py ec2 --region us-east-1 --profile testprofile`

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Ejecutar pruebas unitarias para trabajos ETL de Python en AWS Glue con el marco pytest

Repositorio de código: aws-glue-jobs-unit-testing	Entorno: producción	Tecnologías: macrodatos; desarrollo y pruebas DevOps de software
Servicios de AWS: AWS CloudFormation CodeBuild ; AWS CodeCommit; AWS CodePipeline; AWS Glue		

Resumen

Puede ejecutar pruebas unitarias para trabajos de extracción, transformación y carga (ETL) de Python para AWS Glue en un entorno de desarrollo local, pero replicar esas pruebas en una DevOps canalización puede resultar difícil y llevar mucho tiempo. Las pruebas unitarias pueden resultar especialmente difíciles cuando se moderniza el proceso de ETL de unidad central en las pilas de tecnología de AWS. Este patrón le muestra cómo simplificar las pruebas unitarias y, al mismo tiempo, mantener intacta la funcionalidad existente, evitar interrupciones de funcionalidad de la aplicaciones clave cuando se lanzan nuevas características y mantener un software de alta calidad. Puede usar los pasos y los ejemplos de código de este patrón para ejecutar pruebas unitarias para trabajos ETL de Python en AWS Glue mediante el marco pytest de AWS CodePipeline. También puede usar este patrón para probar e implementar varios trabajos de AWS Glue.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- URI de imagen de Amazon Elastic Container Registry (Amazon ECR) para su biblioteca de AWS Glue, descargada de la galería pública de Amazon ECR
- Terminal Bash (en cualquier sistema operativo) con un perfil para la cuenta de AWS y la región de AWS de destino

- Python 3.10 o posterior
- Pytest
- Biblioteca Moto Python para probar los servicios de AWS

Arquitectura

Pila de tecnología

- Amazon Elastic Container Registry (Amazon ECR)
- AWS CodeBuild
- AWS CodeCommit
- AWS CodePipeline
- AWS Glue
- Pytest
- Python
- Biblioteca ETL de Python para AWS Glue

Arquitectura de destino

En el siguiente diagrama se describe cómo incorporar las pruebas unitarias para los procesos ETL de AWS Glue basados en Python en una canalización típica de AWS DevOps a escala empresarial.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. En la fase de código fuente, CodePipeline utiliza un CodeCommit repositorio para el código fuente, que incluye un ejemplo de trabajo ETL de Python (`sample.py`), un archivo de prueba unitaria (`test_sample.py`) y una CloudFormation plantilla de AWS. A continuación, CodePipeline transfiere el código más reciente de la rama principal al CodeBuild proyecto para su posterior procesamiento.
2. En la etapa de creación y publicación, el código más reciente de la etapa de origen anterior se somete a pruebas unitarias con la ayuda de una imagen de Amazon ECR pública de AWS Glue. A continuación, el informe de la prueba se publica en los grupos de CodeBuild informes. La imagen del contenedor en el repositorio público de Amazon ECR para las bibliotecas de AWS Glue incluye

todos los binarios necesarios para ejecutar tareas de ETL PySparkbasadas en pruebas unitarias en AWS Glue de forma local. El repositorio de contenedores público tiene tres etiquetas de imagen, una para cada versión compatible con AWS Glue. Con fines de demostración, este patrón usa la etiqueta de imagen `glue_libs_4.0.0_image_01`. Para usar esta imagen de contenedor como imagen en tiempo de ejecución CodeBuild, copie el URI de la imagen que corresponda a la etiqueta de imagen que pretende usar y, a continuación, actualice el `pipeline.yml` archivo en el GitHub repositorio del recurso. `TestBuild`

3. En la fase de despliegue, el CodeBuild proyecto se lanza y publica el código en un bucket de Amazon Simple Storage Service (Amazon S3) si se aprueban todas las pruebas.
4. El usuario implementa la tarea AWS Glue mediante la CloudFormation plantilla de la `deploy` carpeta.

Herramientas

Herramientas de AWS

- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable.
- AWS CodeBuild es un servicio de compilación totalmente gestionado que le ayuda a compilar código fuente, ejecutar pruebas unitarias y producir artefactos listos para su implementación.
- AWS CodeCommit es un servicio de control de versiones que le ayuda a almacenar y gestionar repositorios de Git de forma privada, sin necesidad de gestionar su propio sistema de control de código fuente.
- AWS le CodePipeline ayuda a modelar y configurar rápidamente las diferentes etapas de una versión de software y a automatizar los pasos necesarios para publicar cambios de software de forma continua.
- AWS Glue es un servicio ETL completamente administrado. Ayuda a clasificar, limpiar, enriquecer y mover datos de forma fiable entre almacenes de datos y flujos de datos.

Otras herramientas

- Python es un lenguaje de programación de uso general interpretado de alto nivel.
- Moto es una biblioteca de Python para probar los servicios de AWS.
- Pytest es un marco para escribir pruebas unitarias pequeñas que se escalan para permitir pruebas funcionales complejas para aplicaciones y bibliotecas.

- La biblioteca ETL de Python para AWS Glue es un repositorio de bibliotecas de Python que se utilizan en el desarrollo local de trabajos PySpark por lotes para AWS Glue.

Código

El código de este patrón está disponible en el repositorio GitHub aws-glue-jobs-unit-testing. El repositorio incluye los siguientes recursos:

- Un ejemplo de trabajo de AWS Glue basado en Python en la carpeta `src`
- Los casos de pruebas unitarias asociados (creados con el marco pytest) están en la carpeta `tests`
- Una CloudFormation plantilla (escrita en YAML) en la carpeta `deploy`

Prácticas recomendadas

Seguridad de los recursos CodePipeline

Se recomienda utilizar el cifrado y la autenticación en los repositorios de origen que se conectan a tus canalizaciones. CodePipeline Para obtener más información, consulta las prácticas recomendadas de seguridad en la CodePipeline documentación.

Supervisión y registro de los CodePipeline recursos

Se recomienda utilizar las funciones de registro de AWS para determinar qué acciones realizan los usuarios en su cuenta y qué recursos utilizan. Los archivos de registro muestran lo siguiente:

- La fecha y la hora de las acciones
- Dirección IP de origen de las acciones
- Las acciones que han fallado debido a permisos inadecuados

Las funciones de registro están disponibles en AWS CloudTrail y Amazon CloudWatch Events. Puede utilizarlo CloudTrail para registrar las llamadas a las API de AWS y los eventos relacionados realizados por su cuenta de AWS o en su nombre. Para obtener más información, consulte Registrar llamadas a la CodePipeline API con AWS CloudTrail en la CodePipeline documentación.

Puede usar CloudWatch Events para monitorear los recursos y las aplicaciones de la nube de AWS que se ejecutan en AWS. También puede crear alertas en CloudWatch Events. Para obtener más información, consulte Supervisión de CodePipeline eventos en la CodePipeline documentación.

Epics

Implementar el código fuente

Tarea	Descripción	Habilidades requeridas
Prepare el archivo de códigos para su implementación.	1. `code.zip`Descárguelo desde el repositorio GitHub aws-glue-jobs-unit-testing o cree usted mismo el archivo.zip mediante una herramienta de línea de comandos. Por ejemplo, puede crear el archivo .zip en Linux o Mac ejecutando los siguientes comandos en la terminal: `git clone https://github.com/aws-samples/aws-glue-jobs-unit-testing.git` `cd aws-glue-jobs-unit-testing` `git checkout master` `zip -r code.zip src/ tests/ deploy/` 2. Inicie sesión en la consola de administración de AWS y elija la región de AWS que prefiera. 3. Cree un bucket de S3 y, a continuación, cargue el paquete .zip y el archivo `code.zip` (descargados anteriormente) en el bucket de S3 creado.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Crea la CloudFormation pila.	1. Inicie sesión en la consola de administración de AWS y, a continuación, abra la CloudFormation consola. 2. Elija Create stack (Crear pila) y, a continuación, seleccione With existing resources (import resources) (Con recursos existentes (importar recursos)). 3. En la sección Especific ar la plantilla de la página Crear pila, elija Cargar un archivo de plantilla y, a continuación, elija la plantilla pipeline.yml (descargada del repositor io). GitHub A continuación, haga clic en Next (Siguient e). 4. En Stack name (Nombre de pila), escriba glue-unit -testing-pipeline o elija el nombre de pila que prefiera. 5. En ApplicationStackNo mbre, usa el nombre glue-codepipeline-app rellenado previamente. Este es el nombre de la CloudForm ation pila que crea la canalización. 6. Para BranchName, usa el nombre maestro rellenado	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	previamente. Es el nombre de la rama creada en el CodeCommit repositorio para incluir el código del archivo.zip del bucket de S3. 7. Para BucketName, utilice el nombre del bucket aws-glue-artifacts-us-east-1 rellenado previamente. Este es el nombre del bucket de S3 que contiene el archivo .zip y que la canalización utiliza para almacenar artefactos de código. 8. CodeZipEn Archivo, utilice el valor code.zip rellenado previamente. Este es el nombre de la clave del objeto S3 de código de ejemplo. El objeto debe ser un archivo .zip. 9. Para RepositoryName, utilice el nombre aws-glue-unit-testing rellenado previamente. Este es el nombre del CodeCommi t repositorio creado por la pila. 10. Para ello TestRepor tGroupName, usa el nombre glue-unittest-repo rt rellenado previamente.	

Tarea	Descripción	Habilidades requeridas
	Es el nombre del grupo de informes de CodeBuild pruebas que se creó para almacenar los informes de las pruebas unitarias. 11. Seleccione Next (Siguiente) y, a continuación, vuelva a seleccionar Next (Siguiente) en la página Configure stack options (Configurar opciones de pila). 12. En la página de revisión, en Capacidades, elija la opción Reconozco que CloudFormation podría crear recursos de IAM con nombres personalizados. 13. Elija Submit (Enviar). Una vez finalizada la creación de la pila, podrá ver los recursos creados en la pestaña Resources (Recursos). Las pilas tardan aproximadamente entre 5 y 7 minutos en crearse. La pila crea automáticamente un CodeCommit repositorio con el código inicial que se registró en el archivo.zip y se cargó en el depósito de S3. Además, la pila crea una CodePipeline vista utilizando el CodeCommit repositor	

Tarea	Descripción	Habilidades requeridas
	io como fuente. En los pasos anteriores, el CodeCommit repositorio es aws-glue-unit-test y la canalización es aws-glue-unit-test-pipeline.	
Limpie los recursos del entorno.	Para evitar costos de infraestructura adicionales, asegúrese de eliminar la pila después de experimentar con los ejemplos que se proporcionan en este patrón. 1. Abra la CloudFormation consola y, a continuación, seleccione la pila que ha creado. 2. Elija Eliminar. Esto elimina todos los recursos que creó su pila, incluidos los CodeCommit repositorios, las funciones o políticas de AWS Identity and Access Management (IAM) y los proyectos. CodeBuild	AWS DevOps, DevOps ingeniero

Ejecute las pruebas unitarias

Tarea	Descripción	Habilidades requeridas
Ejecute las pruebas unitarias en la canalización.	1. Para probar la canalización implementada, inicie sesión en la consola de administración de AWS	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	y, a continuación, abra la CodePipeline consola. 2. Seleccione la canalización creada por la CloudFormation pila y, a continuación, elija Release change. La canalización comienza a ejecutarse (utilizando el código más reciente del CodeCommit repositorio). 3. Una vez finalizada la etapa de Test_and_build, seleccione la pestaña Details (Detalles) y, a continuación, examine los registros. 4. Seleccione la pestaña Reports (Informes) y, a continuación, elija el informe de prueba en el Report history (Historial de informes) para ver los resultados de las pruebas unitarias. 5. Una vez finalizada la etapa de implementación, ejecute y supervise el trabajo de AWS Glue implementado en la consola de AWS Glue. Para obtener más información, consulte Monitoreo de AWS Glue en la documentación de AWS Glue.	

Resolución de problemas

Problema	Solución
Una canalización con Amazon S3, Amazon ECR o una CodeCommit fuente ya no se inicia automáticamente	Si cambia los ajustes de configuración de una acción que utiliza reglas de CloudWatch eventos en Amazon EventBridge o Events para la detección de cambios, es posible que la consola de administración de AWS no detecte ningún cambio en el que los identificadores de origen sean similares y tengan caracteres iniciales idénticos. Como la consola no crea la nueva regla de eventos, la canalización ya no se inicia automáticamente. Por ejemplo, cambiar el nombre de una CodeCommit sucursal de `MyTestBranch-1` a `MyTestBranch-2` es un cambio menor. Como el cambio se produce al final del nombre de la rama, es posible que la regla de eventos de la acción de origen no actualice ni cree una regla para la nueva configuración del origen. Esto se aplica a las siguientes acciones de origen que utilizan eventos de CloudWatch Events para la detección de cambios: • El nombre del bucket de S3 y los parámetros clave de objeto de S3 o los identificadores de consola cuando la acción de origen se encuentra en Amazon S3 • El nombre del repositorio y los parámetros de etiqueta de imagen o los identificadores de consola cuando la acción de origen se encuentra en Amazon ECR • El nombre del repositorio y el nombre de la rama, los parámetros o los identificadores de

Problema	Solución
	la consola cuando la acción de origen está activa CodeCommit Para resolver este problema, siga uno de estos pasos: • Cambie los ajustes de configuración en Amazon S3, Amazon ECR o CodeCommit, para que los cambios se realicen en la parte inicial del valor del parámetro. Por ejemplo, cambie el nombre de la ramificación de `release-branch` a `2nd-release-branch`. Evite un cambio al final del nombre, por ejemplo `release-branch-2`. • Cambie los ajustes de configuración en Amazon S3, Amazon ECR o CodeCommit en cada canalización. Por ejemplo, cambie el nombre de la ramificación de `myRepo/myBranch` a `myDeployRepo/myDeployBranch`. Evite un cambio al final del nombre, por ejemplo `myRepo/myBranch2`. • En lugar de utilizar la consola de administración de AWS, utilice la interfaz de línea de comandos de AWS (AWS CLI) o CloudFormation AWS para crear y actualizar las reglas de los eventos de detección de cambios. Para obtener instrucciones sobre cómo crear reglas de eventos para una acción de origen de Amazon S3, consulte Acciones y CloudWatch eventos de origen de Amazon S3. Para obtener instrucciones sobre cómo crear reglas de eventos para una acción de Amazon ECR, consulte Amazon ECR source actions and CloudWatch Events.

Problema	Solución
	Para obtener instrucciones sobre cómo crear reglas de eventos para una CodeCommit acción, consulte la CodeCommit fuente de acciones y CloudWatch eventos. Tras editar la configuración de acción en la consola, acepte los recursos de detección de cambios actualizados creados por la consola.

Recursos relacionados

- AWS Glue
- Desarrollo y pruebas de trabajos de AWS Glue a nivel local
- AWS CloudFormation para AWS Glue

Información adicional

Además, puede implementar las CloudFormation plantillas de AWS mediante la CLI de AWS. Para obtener más información, consulte Implementación rápida de plantillas con transformaciones en la CloudFormation documentación.

Configure un repositorio de gráficos de Helm v3 en Amazon S3

Entorno: PoC o piloto	Tecnologías: contenedores y microservicios DevOps; Modernización	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon S3		

Resumen

Este patrón le ayuda a administrar los gráficos de Helm v3 de forma eficiente integrando el repositorio de Helm v3 en Amazon Simple Storage Service (Amazon S3) en la nube de Amazon Web Services (AWS). Para usar este patrón, debe estar familiarizado con Kubernetes y con el administrador de paquetes de Kubernetes Helm. El uso de repositorios de Helm para almacenar gráficos y controlar sus versiones puede mejorar el tiempo medio de restauración (MTTR) durante las interrupciones.

Este patrón usa AWS CodeCommit para la creación de repositorios de Helm y usa un bucket de S3 como repositorio de gráficos de Helm, de modo que los desarrolladores de toda la organización puedan administrar los gráficos de forma centralizada y acceder a ellos.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Python, versión 2.7.12 o posterior.
- pip
- Una nube privada virtual (VPC) con subredes y una instancia de Amazon Elastic Compute Cloud (Amazon EC2)
- Git instalado en la instancia EC2
- Acceso a AWS Identity and Access Management (IAM) para crear el bucket de S3
- Acceso de IAM (mediante programación o de rol) a Amazon S3 desde la máquina cliente
- CodeCommit Repositorio de AWS

- Interfaz de la línea de comandos de AWS (AWS CLI)

Versiones de producto

- Helm v3
- Python, versión 2.7.12 o posterior.

Arquitectura

Pila de tecnología de destino

- Amazon S3
- AWS CodeCommit
- Helm
- Kubectl
- Python y pip
- Git
- complemento helm-s3

Arquitectura de destino

Automatizar y escalar

- Puede incorporar Helm a su herramienta existente de automatización de integración y entrega continuas (CI/CD) para automatizar el empaquetado y el control de versiones de los gráficos de Helm (fuera del alcance de este patrón).
- GitVersion Los números de compilación de Jenkins o Jenkins se pueden utilizar para automatizar el control de versiones de los gráficos.

Herramientas

- Helm: Helm es un administrador de paquetes para Kubernetes que le ayuda a instalar y administrar aplicaciones en su clúster de Kubernetes.

- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet. Puede utilizar Amazon S3 para almacenar y recuperar cualquier cantidad de datos en cualquier momento y desde cualquier parte de la web.
- Complemento helm-s3: el complemento helm-s3 respalda la interacción con Amazon S3. Se puede usar con Helm v2 o Helm v3.

Epics

Instale y valide Helm v3

Tarea	Descripción	Habilidades requeridas
Instale el cliente Helm v3.	Para descargar e instalar el cliente de Helm en su sistema local, ejecute el siguiente comando: `sudo curl https://raw.githubusercontent.com/helm/helm/main/scripts/get-helm-3 | bash`	Administrador de nube, ingeniero DevOps
Valide la instalación de Helm.	Para validar el cliente de Helm, ejecute el siguiente comando: `helm version --short`	Administrador de nube, DevOps ingeniero

Inicializar un bucket de S3 como repositorio de Helm

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3 para gráficos de Helm.	Cree un bucket de S3 único. En el bucket, cree una carpeta llamada `stable/myapp` . El ejemplo de este patrón usa `s3://my-helm-charts/stable/myapp` como	Administrador de nube, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	repositorio de gráficos de destino.	
Instale el complemento helm-s3 para Amazon S3.	Para instalar el plugin helm-s3 en su máquina cliente, ejecute el siguiente comando: `helm plugin install https://github.com/hypnoglow/helm-s3.git`	Administrador de nube, DevOps ingeniero
Inicialice el repositorio Helm de Amazon S3.	Para inicializar la carpeta de destino como repositorio de Helm, ejecute el siguiente comando: `helm s3 init s3://my-helm-charts/stable/myapp` El comando crea un archivo `index.yaml` en el destino para rastrear toda la información del gráfico almacenada en esa ubicación.	Administrador de nube, DevOps ingeniero
Verifique el repositorio de Helm recién creado.	Para comprobar que se ha creado el archivo `index.yaml`, ejecute el siguiente comando: `aws s3 ls s3://my-helm-charts/stable/myapp/`	Administrador de nube, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Añada el repositorio de Amazon S3 a Helm en la máquina cliente.	Para añadir el alias del repositorio de destino a la máquina cliente de Helm, ejecute el siguiente comando: `helm repo add stable-myapp s3://my-helm-charts/stable/myapp/`	Administrador de nube, DevOps ingeniero

Empaquete y publique gráficos en el repositorio Helm de Amazon S3

Tarea	Descripción	Habilidades requeridas
Clone sus gráficos de Helm.	Si no hay gráficos de Helm locales en tu CodeCommit repositorio, clónalos desde tu GitHub repositorio ejecutando el siguiente comando: `git clone <url_of_your_helm_source_code>.git`	Administrador de nube, ingeniero DevOps
Empaquete el gráfico de Helm local.	Para empaquetar el gráfico que ha creado o clonado, ejecute el siguiente comando: `helm package ./my-app` Como ejemplo, este patrón usa el gráfico `my-app`. El comando empaqueta todo el contenido de la carpeta de gráficos `my-app` en un archivo de almacenamiento. Este archivo toma su nombre del	Administrador de nube, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	número de versión mencionado en el archivo `Chart.yaml` .	
Almacene el paquete local en el repositorio Helm de Amazon S3.	Para cargar el paquete local en el repositorio de Helm en Amazon S3, ejecute el siguiente comando: `helm s3 push ./my-app-0.1.0.tgz stable-myapp` En el comando, `my-app` es el nombre de la carpeta de gráficos, `0.1.0` es la versión del gráfico mencionada en `Chart.yaml` y `stable-myapp` es el alias del repositorio de destino.	Administrador de nube, DevOps ingeniero
Busque el gráfico de Helm.	Para confirmar que el gráfico aparece tanto localmente como en el repositorio de Helm de Amazon S3, ejecute el siguiente comando: `helm search repo stable-myapp`	Administrador de nube, DevOps ingeniero

Actualice su repositorio de Helm

Tarea	Descripción	Habilidades requeridas
Modifique y empaquete el gráfico.	En `values.yaml` , establezca el valor `replicaCount` en 1 y, a continuación, empaquete el gráfico, esta	Administrador de nube, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
	vez cambiando la versión de `Chart.yaml` a `0.1.1`. Lo ideal es que el control de versiones se logre mediante la automatización mediante el uso de herramientas como GitVersion los números de compilación de Jenkins en una canalización de CI/CD. La automatización del número de versión está fuera del alcance de este patrón. Para agrupar la tabla, ejecute el siguiente comando: `helm package ./my-app/`	
Introduzca la nueva versión en el repositorio de Helm en Amazon S3.	Para enviar el nuevo paquete, versión 0.1.1, al repositor io Helm my-helm-charts de Amazon S3, ejecute el siguiente comando: `helm s3 push ./my-app-0.1.1.tgz stable-myapp`	Administrador de nube, DevOps ingeniero
Compruebe el gráfico de Helm actualizado.	Para confirmar que el gráfico actualizado aparece tanto localmente como en el repositorio Helm de Amazon S3, ejecute los siguientes comandos. `helm repo update` `helm search repo stable-myapp`	Administrador de nube, DevOps ingeniero

Busque e instale un gráfico en el repositorio de Helm de Amazon S3

Tarea	Descripción	Habilidades requeridas
Busque todas las versiones del gráfico my-app.	Para ver todas las versiones disponibles de un gráfico, ejecute el siguiente comando con la marca `--versions` : `helm search repo my-app --versions` Sin la marca, Helm mostrará de forma predeterminada la última versión cargada de un gráfico.	DevOps Ingeniero
Instale una tabla desde el repositorio Helm de Amazon S3.	La instalación automatizada está fuera del alcance de este patrón, pero puede realizar una instalación manual. Los resultados de la búsqueda de la tarea anterior mostrarán las múltiples versiones del gráfico `my-app`. Para instalar la nueva versión (0.1.1) desde el repositorio de Helm de Amazon S3, ejecute el siguiente comando: `helm upgrade --install my-app-release stable-my app/my-app --version 0.1.1 --namespace dev`	DevOps Ingeniero

Restaure una versión anterior con Helm

Tarea	Descripción	Habilidades requeridas
Compruebe los detalles de una revisión específica.	La reversión automática está fuera del alcance de este patrón, pero puede restaurar manualmente una versión anterior. Antes de cambiar o revertir a una versión funcional , y para obtener un nivel adicional de validación antes de instalar una revisión, compruebe qué valores se han pasado a cada una de las revisiones mediante el siguiente comando: `helm get values --revisio n=2 my-app-release`	DevOps Ingeniero
Vuelva a una versión anterior.	La reversión automática está fuera del alcance de este patrón. Para restaurar manualmente una revisión anterior, ejecute el siguiente comando: `helm rollback my-app-release 1` Este ejemplo restaura la revisión número 1.	DevOps Ingeniero

Recursos relacionados

- Documentación de HELM
- Complemento helm-s3 (licencia MIT)
- Amazon S3

Configure una canalización de CI/CD mediante AWS y CodePipeline AWS CDK

Repositorio de código: AWS CodePipeline con CI/CD	Entorno: PoC o piloto	Tecnologías: DevOps
Carga de trabajo: código abierto	Servicios de AWS: AWS CodePipeline	

Inicio

Automatizar el proceso de creación y publicación del software mediante la integración y entrega continuas (CI/CD) facilita las compilaciones repetibles y la entrega rápida de nuevas funciones a los usuarios. Puede probar rápida y fácilmente cada cambio de código, así como detectar y corregir errores antes de lanzar su software. Al ejecutar cada cambio en los procesos de preparación y publicación, puede verificar la calidad del código de su aplicación o infraestructura. La CI/CD abarca una cultura, un conjunto de principios operativos y un conjunto de prácticas que ayudan a los equipos de desarrollo de aplicaciones a realizar cambios de código con mayor frecuencia y fiabilidad. Esta implementación también se conoce como proceso de CI/CD.

Este patrón define un proceso reutilizable de integración y entrega continuas (CI/CD) en Amazon Web Services (AWS). La CodePipeline canalización de AWS se ha escrito con el AWS Cloud Development Kit (AWS CDK) v2.

Con CodePipeline él, puede modelar las diferentes etapas del proceso de lanzamiento de software a través de la interfaz de la consola de administración de AWS, la interfaz de línea de comandos de AWS (AWS CLI), CloudFormation AWS o los SDK de AWS. Este patrón demuestra la implementación CodePipeline y sus componentes mediante AWS CDK. Además de crear bibliotecas, AWS CDK incluye un kit de herramientas (el comando de CLI `cdk`). Es la herramienta principal para interactuar con la aplicación de AWS CDK. Entre otras funciones, el kit de herramientas ofrece la posibilidad de convertir una o más pilas en CloudFormation plantillas e implementarlas en una cuenta de AWS.

El proceso incluye pruebas para validar la seguridad de sus bibliotecas de terceros, y ayuda a garantizar una publicación rápida y automatizada en los entornos especificados. Puede aumentar la seguridad general de sus aplicaciones sometiéndolas a un proceso de validación.

El objetivo de este patrón es acelerar el uso de las canalizaciones de CI/CD para implementar el código y, al mismo tiempo, garantizar que los recursos que se implementen se ajusten a las mejores prácticas. DevOps Tras implementar el código de ejemplo, dispondrá de un AWS CodePipeline con procesos de linting, pruebas, controles de seguridad y procesos de implementación y posteriores a la implementación. Este patrón también incluye pasos para Makefile. Con Makefile, los desarrolladores pueden reproducir los pasos de CI/CD localmente y aumentar la velocidad del proceso de desarrollo.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una comprensión básica de lo siguiente:
  - AWS CDK
  - AWS CloudFormation
  - AWS CodePipeline
  - TypeScript

Limitaciones

Este patrón utiliza AWS CDK TypeScript únicamente para. No abarca otros lenguajes compatibles con AWS CDK.

Versiones de producto

Utilice las versiones más recientes de las siguientes herramientas:

- Interfaz de la línea de comandos de AWS (AWS CLI)
- cfn_nag
- git-remote-codecommit
- Node.js

Arquitectura

Pila de tecnología de destino

- AWS CDK

- AWS CloudFormation
- AWS CodeCommit
- AWS CodePipeline

Arquitectura de destino

La canalización se desencadena por un cambio en el CodeCommit repositorio de AWS (`SampleRepository`). Al principio, CodePipeline crea artefactos, se actualiza automáticamente e inicia el proceso de implementación. El proceso resultante implementa una solución en tres entornos independientes:

- Desarrollo: verificación del código en tres pasos en el entorno de desarrollo activo
- Prueba: entorno de pruebas de integración y regresión
- Prod: entorno de producción

Los tres pasos incluidos en la etapa de desarrollo son el linting, la seguridad y las pruebas unitarias. Estos pasos se ejecutan en paralelo para acelerar el proceso. Para garantizar que el proceso solo proporcione artefactos funcionales, dejará de funcionar cada vez que falle un paso del proceso. Tras la implementación en la fase de desarrollo, el proceso ejecuta pruebas de validación para verificar los resultados. En caso de éxito, el proceso implementará los artefactos en el entorno de prueba, que contiene la validación posterior a la implementación. El paso final consiste en implementar los artefactos en el entorno de producción.

El siguiente diagrama muestra el flujo de trabajo desde el CodeCommit repositorio hasta los procesos de creación y actualización que se llevan a cabo en el entorno de desarrollo, así como el despliegue y la validación posteriores en cada uno de los tres entornos. CodePipeline

Herramientas

Servicios de AWS

- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura de la nube de AWS en código.
- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de

AWS. En este patrón, CloudFormation las plantillas se pueden utilizar para crear un CodeCommit repositorio y una canalización de CodePipeline CI/CD.

- AWS CodeCommit es un servicio de control de versiones que le ayuda a almacenar y gestionar repositorios de Git de forma privada, sin necesidad de gestionar su propio sistema de control de código fuente.
- AWS CodePipeline es un servicio de CI/CD que le ayuda a modelar y configurar rápidamente las diferentes etapas de una versión de software y a automatizar los pasos necesarios para publicar cambios de software de forma continua.
- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.

Otras herramientas

- cfn_nag es una herramienta de código abierto que busca patrones en CloudFormation las plantillas para identificar posibles problemas de seguridad.
- git-remote-codecommit es una utilidad para insertar y extraer código de los repositorios CodeCommit mediante la extensión de Git.
- Node.js es un entorno de JavaScript ejecución basado en eventos diseñado para crear aplicaciones de red escalables.

Código

El código de este patrón está disponible en el repositorio de prácticas de GitHub AWS CodePipeline with CI/CD.

Prácticas recomendadas

Revise los recursos, como las políticas de AWS Identity and Access Management (IAM), para asegurarse de que se ajusten a las prácticas recomendadas de su organización.

Epics

Instalar herramientas

Tarea	Descripción	Habilidades requeridas
Instalar herramientas en macOS o Linux.	Si usa macOS o Linux, puede instalar las herramien tas ejecutando el siguiente comando en su terminal preferido o usando Homebrew para Linux. `brew install` `brew install git-remot e-codecommit` `brew install ruby brew- gem` `brew-gem install cfn- nag`	DevOps ingeniero
Instale herramientas con AWS Cloud9.	Si usa AWS Cloud9, instale las herramientas ejecutando el siguiente comando. `gem install cfn-nag` Nota: AWS Cloud9 debe tener Node.js y npm instalados. Para comprobar la instalaci ón o la versión, ejecute el siguiente comando. `node -v` `npm -v`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Configure AWS CLI.	Para configurar la CLI de AWS, consulte las instrucciones del sistema operativo: • Windows: pasos de configuración para las conexiones HTTPS a los CodeCommit repositorios de AWS en Windows con el asistente de credenciales de la CLI de AWS • Linux, macOS y Unix: pasos de configuración para las conexiones HTTPS a los CodeCommit repositorios de AWS en Linux, macOS o Unix con el asistente de credenciales de la CLI de AWS	DevOps ingeniero

Configurar la implementación inicial

Tarea	Descripción	Habilidades requeridas
Descargue o clone el código.	Para obtener el código que utiliza este patrón, realice una de las siguientes acciones: • Descarga el código fuente más reciente de las versiones del GitHub repositorio y descomprime el archivo descargado en una carpeta.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	• Clone el proyecto ejecutando el siguiente comando. `git clone --depth 1 https://github.com/aws-samples/aws-codepipeline-cicd.git` Elimine el directorio `.git` del repositorio clonado. `cd ./aws-codepipeline-cicd` `rm -rf ./.git` Más adelante, utilizará un CodeCommit repositorio de AWS recién creado como origen remoto.	
Conéctese a la cuenta de AWS.	Puede conectarse mediante un token de seguridad temporal o una autenticación de zona de aterrizaje. Para confirmar que está utilizando la cuenta y región de AWS correctas, ejecute los siguientes comandos. `AWS_REGION="eu-west-1"` `ACCOUNT_NUMBER=$(aws sts get-caller-identity --query Account --output text)` `echo "${ACCOUNT_NUMBER}"`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Inicie el entorno.	Para arrancar un entorno AWS CDK, ejecute los siguientes comandos. `npm install` `npm run cdk bootstrap "aws://${ACCOUNT_NUMBER}/${AWS_REGION}"` Tras arrancar correctamente el entorno, debería aparecer el siguiente resultado. `# Bootstrapping environment aws://{account}/{region}...` `# Environment aws://{account}/{region} bootstrapped` Para más información sobre el proceso de arranque de AWS CDK, consulte la documentación de AWS CDK.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Sintetice una plantilla.	Para sintetizar una aplicación de AWS CDK, ejecute el comando `cdk synth`. `npm run cdk synth` Debería ver la siguiente salida. `Successfully synthesized to <path-to-directory>/aws-codepipeline-cicd/cdk.out` `Supply a stack id (CodePipeline, Dev-MainStack) to display its template.`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Despliega la CodePipeline pila.	Ahora que ha iniciado y sintetizado la CloudFormation plantilla, puede desplegarla. La implementación creará la CodePipeline canalización y un CodeCommit repositor io, que serán la fuente y el desencadenante de la canalización. `npm run cdk -- deploy CodePipeline --require-approval never` Tras ejecutar el comando, debería ver una implement ación correcta de la CodePipel ine pila y la información de salida. `CodePipel ine.RepositoryName` Le da el nombre del CodeCommit repositorio de la cuenta de AWS. `CodePipeline: deploying ... CodePipeline: creating CloudFormation changeset... # CodePipeline Outputs: CodePipeline.R epositoryName = SampleRepository Stack ARN: arn:aws:cloudformation :REGION:ACCOUNT-ID`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`:stack/CodePipeline/STACK-ID`	

Tarea	Descripción	Habilidades requeridas
Configure el CodeCommit repositorio y la sucursal remotos.	Tras una implementación correcta, CodePipeline iniciará la primera ejecución de la canalización, que puede encontrar en la CodePipeline consola de AWS. Como AWS CDK y CodeCommit no inician una rama predeterminada, esta canalización inicial fallará y devolverá el siguiente mensaje de error. `The action failed because no branch named main was found in the selected AWS CodeCommit repository SampleRepository. Make sure you are using the correct branch name, and then try again. Error: null` Para corregir este error, configure un origen remoto como `SampleRepository` y cree la ramificación `main` requerida. `RepoName=$(aws cloudformation describe-stacks --stack-name CodePipeline --query "Stacks[0].Outputs[?OutputKey=='RepositoryName'].OutputValue" --output text)`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`echo "${RepoName}"` `#` `git init` `git branch -m master main` `git remote add origin codecommit://${RepoName}` `git add .` `git commit -m "Initial commit"` `git push -u origin main`	

Pruebe la CodePipeline canalización desplegada

Tarea	Descripción	Habilidades requeridas
Realice un cambio para activar el proceso.	Tras la implementación inicial satisfactoria, debería disponer de un proceso de CI/CD completo con una ramificación `main` con `SampleRepository` como ramificación de origen. En cuanto realice los cambios en la ramificación `main`, se iniciará el proceso y se ejecutará la siguiente secuencia de acciones: 1. Obtenga el código del CodeCommit repositorio. 2. Compila el código. 3. Actualiza el proceso (`UpdatePipeline`).	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	4. Ejecuta tres trabajos paralelos para comprobar el linting, la seguridad y las pruebas unitarias. 5. En caso de éxito, el proceso implementará la pila `Main` de `./lib/main-stack.ts` en el entorno de desarrollo. 6. Realice una comprobación de los recursos tras la implementación. Puedes seguir todos los CodePipeline pasos y resultados en la CodePipeline consola. 7. En caso de éxito, el proceso repetirá la implementación y la validación en los entornos de prueba y producción.	

Realice pruebas locales mediante Makefile

Tarea	Descripción	Habilidades requeridas
Ejecute el proceso de desarrollo mediante Makefile.	Puede ejecutar todo el proceso de forma local mediante el comando `make`, o bien ejecutar un paso individual (por ejemplo, `make linting`).	Desarrollador de aplicaciones, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Para probar el uso de `make`, realice las siguientes acciones: • Implemente el proceso local: `make` • Ejecute solo pruebas unitarias: `make unittest` • Implemente en la cuenta actual: `make deploy` • Limpie el entorno: `make clean`	

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Elimine los recursos de la aplicación AWS CDK.	Para limpiar su aplicación AWS CDK, ejecute el siguiente comando. `cdk destroy --all` Tenga en cuenta que los buckets de Amazon Simple Storage Service (Amazon S3) creados durante el arranque no se eliminan automáticamente. Necesitará una política de retención que permita su eliminación, o bien tendrá que eliminarlos manualmente en su cuenta de AWS.	DevOps ingeniero

Resolución de problemas

Problema	Solución
La plantilla no funciona como se esperaba.	Si algo sale mal y la plantilla no funciona, asegúrese de que dispone de lo siguiente: • Las versiones adecuadas de las herramien tas. • Acceso a la cuenta de AWS de destino (conectividad de red). • Permisos suficientes para la cuenta de AWS de destino.

Recursos relacionados

- Comience con las tareas habituales en IAM Identity Center
- CodePipeline Documentación de AWS
- AWS CDK

Configure el end-to-end cifrado para aplicaciones en Amazon EKS mediante cert-manager y Let's Encrypt

Creado por Mahendra Siddappa (AWS) y Vasanth Jeyaraj (AWS)

Repositorio de código: nd-to-end cifrado electrónico en Amazon EKS	Entorno: PoC o piloto	Tecnologías: DevOps contenedores y microservicios; seguridad, identidad y conformidad
Carga de trabajo: todas las demás cargas de trabajo	Servicios de AWS: Amazon EKS; Amazon Route 53	

Resumen

La implementación del end-to-end cifrado puede resultar compleja y es necesario gestionar los certificados de cada activo de la arquitectura de microservicios. Si bien puede finalizar la conexión de Transport Layer Security (TLS) en el extremo de la red de Amazon Web Services (AWS) con un Network Load Balancer o Amazon API Gateway, algunas organizaciones end-to-end requieren el cifrado.

Este patrón utiliza el controlador de entrada NGINX para la entrada. Esto se debe a que cuando se crea una entrada de Kubernetes, el recurso de entrada utiliza un equilibrador de carga de red. El equilibrador de carga de red no permite cargar certificados de cliente. Por lo tanto, no puede lograr el TLS mutuo con el ingreso de Kubernetes.

Este patrón está pensado para las organizaciones que requieren la autenticación mutua entre todos los microservicios de sus aplicaciones. El TLS mutuo reduce la carga que supone mantener los nombres de usuario o las contraseñas y, además, puede utilizar un marco de seguridad listo para usar. El enfoque de este patrón es compatible si su organización tiene una gran cantidad de dispositivos conectados o si debe cumplir con estrictas pautas de seguridad.

Este patrón ayuda a aumentar la postura de seguridad de su organización al implementar el end-to-end cifrado para las aplicaciones que se ejecutan en Amazon Elastic Kubernetes Service (Amazon EKS). Este patrón proporciona una aplicación y un código de muestra en el repositorio de nd-to-end cifrado GitHub E en Amazon EKS para mostrar cómo se ejecuta un microservicio con el end-

to-end cifrado en Amazon EKS. El enfoque del patrón utiliza cert-manager, un complemento de Kubernetes, con Let's Encrypt como autoridad de certificación (CA). Let's Encrypt es una solución rentable para administrar certificados y proporciona certificados gratuitos con una validez de 90 días. Cert-Manager automatiza el aprovisionamiento bajo demanda y la rotación de los certificados cuando se implementa un nuevo microservicio en Amazon EKS.

Destinatarios previstos

Este patrón se recomienda para los usuarios que tengan experiencia con Kubernetes, TLS, Amazon Route 53 y el Sistema de nombres de dominio (DNS).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Un clúster existente de Amazon EKS.
- Interfaz de la línea de comandos de AWS (AWS CLI) versión 1.7, instalada y configurada en macOS, Linux o Windows
- La utilidad de línea de comandos `kubectl`, instalada y configurada para acceder al clúster de Amazon EKS. Para obtener más información, consulte Installing kubectl (Instalación de kubectl) en la documentación de Amazon EKS.
- Un nombre DNS existente para probar una aplicación. Para obtener más información, consulte Registrar nombres de dominio mediante Amazon Route 53 en la documentación de Amazon Route 53.
- La última versión de Helm, instalada en su máquina local. Para obtener más información al respecto, consulte Uso de Helm con Amazon EKS en la documentación de Amazon EKS y en el repositorio de GitHub Helm.
- El nd-to-end cifrado GitHub E del repositorio EKS de Amazon, clonado en su máquina local.
- Sustituya los siguientes valores en los `trustpolicy.json` archivos `policy.json` y del repositorio de nd-to-end cifrado GitHub E clonado en Amazon EKS:
  - `<account number>`: sustitúyalo por el ID de cuenta de AWS de la cuenta en la que desea implementar la solución.
  - `<zone id>`: sustitúyalo por el ID de zona de Route 53 del nombre de dominio.
  - `<node_group_role>`: sustitúyalo por el nombre de la función de AWS Identity and Access Management del rol de IAM asociada a los nodos de Amazon EKS.

- `<namespace>`: sustitúyalo por el espacio de nombres de Kubernetes en el que se despliega el controlador de entrada NGINX y la aplicación de ejemplo.
- `<application-domain-name>`: sustitúyalo por el nombre de dominio DNS de Route 53

Limitaciones

- Este patrón no describe cómo rotar los certificados y solo muestra cómo usar los certificados con microservicios en Amazon EKS.

Arquitectura

En el siguiente diagrama se muestran los componentes de la arquitectura y el flujo de trabajo de esta aplicación.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un cliente envía una solicitud de acceso a la aplicación al nombre DNS.
2. El registro de Route 53 es un CNAME para el equilibrador de carga de red.
3. El equilibrador de carga de red reenvía la solicitud al controlador de entrada NGINX que está configurado con un agente oyente TLS. La comunicación entre el controlador de entrada NGINX y el equilibrador de carga de red sigue el protocolo HTTPS.
4. El controlador de entrada NGINX realiza un enrutamiento basado en rutas en función de la solicitud del cliente al servicio de la aplicación.
5. El servicio de aplicaciones reenvía la solicitud al pod de la aplicación. La aplicación está diseñada para utilizar el mismo certificado al llamar a secretos.
6. Los pods ejecutan la aplicación de ejemplo con los certificados del administrador de certificados. La comunicación entre el controlador de entrada de NGINX y los pods utiliza HTTPS.

Nota: Cert-Manager se ejecuta en su propio espacio de nombres. Utiliza un rol de clúster de Kubernetes para aprovisionar certificados como secretos en espacios de nombres específic os. Puede adjuntar esos espacios de nombres a los pods de aplicaciones y al NGINX Ingress Controller.

Herramientas

Servicios de AWS

- Amazon Elastic Kubernetes Service (Amazon EKS) es un servicio administrado que puede utilizar para ejecutar Kubernetes en AWS sin necesidad de instalar, operar ni mantener su propio plano de control o nodos de Kubernetes.
- Elastic Load Balancing distribuye automáticamente el tráfico entrante entre varios destinos, por ejemplo, instancias EC2, contenedores y direcciones IP en una o varias zonas de disponibilidad.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad.

Otras herramientas

- cert-manager es un complemento de Kubernetes que solicita certificados, los distribuye a los contenedores de Kubernetes y automatiza la renovación de los certificados.
- NGINX Ingress Controller es una solución de gestión del tráfico para aplicaciones nativas en la nube en Kubernetes y entornos contenerizados.

Epics

Cree y configure una zona alojada pública con Route 53

Tarea	Descripción	Habilidades requeridas
Cree una zona alojada pública para Route 53.	Inicie sesión en la consola de administración de AWS, abra la consola Amazon Route 53, elija Zonas alojadas y, a continuación, elija Crear zona alojada. Cree una zona alojada pública y registre el ID de la zona. Para obtener más información, consulte Crear	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	una zona alojada pública en la documentación de Amazon Route 53. Nota: ACME DNS01 utiliza el proveedor de DNS para solicitar al administrador de certificados que emita el certificado. Este desafío le pide que demuestre que controla el DNS de su nombre de dominio poniendo un valor específico en un registro TXT situado debajo de ese nombre de dominio. Cuando Let's Encrypt proporciona un token a su cliente ACME, este crea un registro TXT derivado de ese token y de su clave de cuenta, y coloca ese registro en `_acme-challenge.<YOURDOMAIN>` . Luego, Let's Encrypt consulta el DNS de ese registro. Si encuentra una coincidencia, puede proceder a emitir un certificado.	

Configure un rol de IAM para permitir que el administrador de certificados acceda a la zona alojada pública

Tarea	Descripción	Habilidades requeridas
Cree la política de IAM para cert-manager.	Se requiere una política de IAM para proporcionar a cert-manager permiso para	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	validar que usted es propietario del dominio de Route 53. El `policy.json` ejemplo de política de IAM se proporciona en el `1-IAMRole` directorio del repositorio de nd-to-end cifrado GitHub E clonado en Amazon EKS. Escriba el siguiente comando en la CLI de AWS para crear la política de IAM: `aws iam create-policy \` `  --policy-name PolicyForCertManager \` `  --policy-document file://policy.json`	

Tarea	Descripción	Habilidades requeridas
Cree el rol de IAM para cert-manager.	Después de crear la política de IAM, debe crear un rol de IAM. El ejemplo del rol de IAM `trustpolicy.json` se proporciona en el directorio `1-IAMRole`. Escriba el siguiente comando en la CLI de AWS para crear el rol de IAM: `aws iam create-role \` `  --role-name RoleForCertManager \` `  --assume-role-policy-document file://trustpolicy.json`	AWS DevOps
Asocie la política al rol.	Escriba el siguiente comando en la CLI de AWS para adjuntar la política de IAM al rol de IAM: Sustituya `AWS_ACCOUNT_ID` por el ID de la cuenta de AWS. `aws iam attach-role-policy \` `  --policy-arn arn:aws:iam::AWS_ACCOUNT_ID:policy/PolicyForCertManager \` `  --role-name RoleForCertManager`	AWS DevOps

Configure el controlador de entrada NGINX en Amazon EKS

Tarea	Descripción	Habilidades requeridas
Implemente el controlador de entrada NGINX.	Instale la versión más reciente de `nginx-ingress` mediante Helm. Puede modificar la configuración `nginx-ingress` según sus requisitos antes de implementarla. Este patrón utiliza un equilibrador de carga de red anotado e interno que está disponible en el directorio `5-Nginx-Ingress-Controller`. Instale el controlador de entrada NGINX ejecutando el siguiente comando Helm desde el directorio `5-Nginx-Ingress-Controller`. `helm install test-nginx nginx-stable/nginx-ingress -f 5-Nginx-Ingress-Controller/values_internal_nlb.yaml`	AWS DevOps
Verifique que el controlador de entrada NGINX se encuentre instalado.	Escriba el comando `helm list`. El resultado debería mostrar que el controlador de entrada NGINX está instalado.	AWS DevOps
Cree un registro A de Route 53.	El registro A apunta al equilibrador de carga de red	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	creado por el controlador de entrada de NGINX. 1. Obtener el nombre del DNS del equilibrador de carga de red. Para más instrucciones, consulte Obtener el nombre del DNS para un equilibrador de carga ELB. 2. En la consola de Amazon Route 53, elija Hosted Zones (Zonas alojadas). 3. Seleccione la zona alojada pública en la que desee crear el registro y, a continuación, elija Crear registro. 4. Ingrese un nombre para el registro. 5. En Record type, (Tipo de registro) elija A - Routes traffic to an IPv4 address and some AWS resources (A - Enruta el tráfico a una dirección IPv4 y algunos recursos de AWS). 6. Habilite el Alias. 7. En Enrutar el tráfico a, haga lo siguiente: a. Elija Alias para el equilibrador de carga de red.	

Tarea	Descripción	Habilidades requeridas
	b. Elija la región de AWS en la que se implementa el equilibrador de carga de red. c. Introduzca el nombre DNS del equilibrador de carga de red. 8. Elija Crear registros.	

Configurar NGINX en VirtualServer Amazon EKS

Tarea	Descripción	Habilidades requeridas
Implemente NGINX. VirtualServer	El VirtualServer recurso NGINX es una configuración de equilibrio de carga que es una alternativa al recurso de entrada. La configuración para crear el VirtualServer recurso NGINX está disponible en el archivo del `nginx_virtualserver.yaml` directorio. `6-Nginx-Virtual-Server` Introduzca el siguiente comando `kubectl` para crear el recurso VirtualServer NGINX. `kubectl apply -f nginx_virtualserver.yaml`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	Importante: asegúrese de actualizar el nombre de dominio de la aplicación, el secreto del certificado y el nombre del servicio de la aplicación en el archivo `nginx_virtualserver.yaml` .	
Compruebe que se ha creado NGINX VirtualServer .	Introduzca el siguiente comando `kubectl` para comprobar que el VirtualServer recurso NGINX se creó correctamente. `kubectl get virtualserver` Nota: Compruebe que la columna `Host` coincida con el nombre de dominio de su aplicación.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Implemente el servidor web NGINX con TLS habilitado.	Este patrón utiliza un servidor web NGINX con TLS habilitad o como aplicación para probar el cifrado. end-to-end Los archivos de configuración necesarios para implementar la aplicación de prueba están disponibles en el directorio `demo-webserver` . Para implementar la aplicación de prueba, ejecute el siguiente comando en `kubectl`: `kubectl apply -f nginx-tls-ap.yaml`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Compruebe que se hayan creado los recursos de la aplicación de prueba.	Introduzca los siguientes comandos en `kubectl` para comprobar que se han creado los recursos necesarios para la aplicación de prueba: • `kubectl get deployments` Nota: Valide la columna`Ready` y la columna `Available` . • `kubectl get pods | grep -i example-deploy` Nota: Los pods deben estar en un estado `running`. • `kubectl get configmap` • `kubectl get svc`	AWS DevOps
Validación de la solicitud.	1. Introduzca el siguiente comando sustituyendo `<application-domain-name>` por el nombre DNS de Route53 que creó anteriormente. `curl --verbose https://<application-domain-name>` 2. Compruebe que puede acceder a la aplicación.	AWS DevOps

Recursos relacionados

Recursos de AWS

- Creación de registros con la consola de Amazon Route 53 (documentación de Amazon Route 53)
- Uso de un equilibrador de carga de red con el controlador de entrada de NGINX en Amazon EKS en el blog de AWS

Otros recursos

- Route 53 (documentación del administrador de certificados)
- Configuración del proveedor de desafíos DNS01 (documentación sobre el administrador de certificados)
- El desafío Let's Encrypt DNS (documentación de Let's Encrypt)

Simplifique la implementación de aplicaciones multiusuario de Amazon EKS mediante Flux

Creado por Nadeem Rahaman (AWS), Aditya Ambati (AWS), Aniket Dekate (AWS) y Shrikant Patil (AWS)

Repositorio de código: aws-eks-multitenancy-deployment	Entorno: PoC o piloto	Tecnologías: DevOps contenedores y microservicios
Servicios de AWS: AWS CodeBuild; AWS CodeCommit CodePipeline; Amazon EKS; Amazon VPC		

Resumen

Muchas empresas que ofrecen productos y servicios son sectores regulados por los datos que deben mantener las barreras de datos entre sus funciones empresariales internas. Este patrón describe cómo puede utilizar la función de tenencia múltiple de Amazon Elastic Kubernetes Service (Amazon EKS) para crear una plataforma de datos que logre el aislamiento lógico y físico entre los inquilinos o usuarios que comparten un único clúster de Amazon EKS. El patrón proporciona aislamiento mediante los siguientes enfoques:

- Aislamiento del espacio de nombres de Kubernetes
- Control de acceso basado en roles (RBAC)
- Políticas de red
- Cuotas de recursos
- AWS Identity and Access Management Funciones (IAM) para cuentas de servicio (IRSA)

Además, esta solución utiliza Flux para mantener inmutable la configuración del inquilino al implementar aplicaciones. Puede implementar sus aplicaciones arrendatarias especificando el repositorio arrendatario que contiene el `kustomization.yaml` archivo Flux en su configuración.

Este patrón implementa lo siguiente:

- Un AWS CodeCommit repositorio, AWS CodeBuild proyectos y una AWS CodePipeline canalización, que se crean mediante la implementación manual de los scripts de Terraform.
- Componentes de red y cómputo necesarios para alojar a los inquilinos. Estos se crean a través de Terraform CodePipeline y CodeBuild utilizando Terraform.
- Espacios de nombres de inquilinos, políticas de red y cuotas de recursos, que se configuran mediante un diagrama de Helm.
- Aplicaciones que pertenecen a diferentes inquilinos, implementadas mediante Flux.

Le recomendamos que planifique y construya cuidadosamente su propia arquitectura para múltiples inquilinos en función de sus requisitos únicos y sus consideraciones de seguridad. Este patrón proporciona un punto de partida para la implementación.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- AWS Command Line Interface (AWS CLI) versión 2.11.4 o posterior, instalada y configurada
- La versión 0.12 o posterior de Terraform está instalada en su máquina local
- Terraform AWS Provider versión 3.0.0 o posterior
- Kubernetes Provider, versión 2.10 o posterior
- Helm Provider, versión 2.8.0 o posterior
- Kubectl Provider versión 1.14 o posterior

Limitaciones

- Dependencia de las implementaciones manuales de Terraform: la configuración inicial del flujo de trabajo, que incluye la creación de CodeCommit repositorios, CodeBuild proyectos y CodePipeline canalizaciones, se basa en las implementaciones manuales de Terraform. Esto introduce una posible limitación en términos de automatización y escalabilidad, ya que requiere una intervención manual para los cambios en la infraestructura.
- CodeCommit dependencia de los repositorios: el flujo de trabajo se basa en CodeCommit los repositorios como solución de gestión del código fuente y está estrechamente AWS vinculado a los servicios.

Arquitectura

Arquitecturas de destino

Este patrón implementa tres módulos para crear la infraestructura de canalización, red e informática de una plataforma de datos, como se ilustra en los siguientes diagramas.

Arquitectura de canalización:

Arquitectura de red:

Arquitectura de cómputo:

Herramientas

Servicios de AWS

- AWS CodeBuildes un servicio de compilación totalmente gestionado que le ayuda a compilar el código fuente, ejecutar pruebas unitarias y producir artefactos listos para su implementación.
- AWS CodeCommites un servicio de control de versiones que te ayuda a almacenar y gestionar de forma privada los repositorios de Git, sin necesidad de gestionar tu propio sistema de control de código fuente.
- AWS CodePipelinete ayuda a modelar y configurar rápidamente las diferentes etapas de una versión de software y a automatizar los pasos necesarios para publicar cambios de software de forma continua.
- Amazon Elastic Kubernetes Service (Amazon EKS) le ayuda a ejecutar AWS Kubernetes sin necesidad de instalar ni mantener su propio plano de control o nodos de Kubernetes.
- AWS Transit Gateway es un núcleo central que conecta las nubes privadas virtuales (VPC) y las redes en las instalaciones.
- Amazon Virtual Private Cloud (Amazon VPC) le ayuda a lanzar AWS recursos en una red virtual que haya definido. Esa red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Otras herramientas

- Las políticas de red de Cilium son compatibles con las políticas de red L3 y L4 de Kubernetes. Se pueden ampliar con políticas L7 para proporcionar seguridad a nivel de API para HTTP, Kafka y gRPC, y otros protocolos similares.
- Flux es una herramienta de entrega continua (CD) basada en Git que automatiza las implementaciones de aplicaciones en Kubernetes.
- Helm es un administrador de paquetes de código abierto para Kubernetes que le ayuda a instalar y administrar aplicaciones en su clúster de Kubernetes.
- Terraform es una herramienta de infraestructura como código (IaC) HashiCorp que le ayuda a crear y administrar recursos locales y en la nube.

Repositorio de código

El código de este patrón está disponible en el repositorio de soluciones Terraform Multi-Tenancy de GitHub EKS.

Prácticas recomendadas

Para ver las directrices y las mejores prácticas para el uso de esta implementación, consulte lo siguiente:

- Prácticas recomendadas de tenencia múltiple de Amazon EKS
- Documentación de Flux

Epics

Cree canalizaciones para las etapas de construcción, prueba e implementación de Terraform

Tarea	Descripción	Habilidades requeridas
Clona el repositorio del proyecto.	Clone el repositorio de la solución Terraform Multi-Tenancy de GitHub EKS ejecutando el siguiente comando en una ventana de terminal:	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`git clone https://github.com/aws-samples/aws-eks-multitenancy-deployment.git`	
Inicie el bucket Terraform S3 y Amazon DynamoDB.	1. En la `bootstrap` carpeta, abra el `bootstrap.sh` archivo y actualice los valores de las variables para el nombre del bucket de S3, el nombre de la tabla de DynamoDB y: Región de AWS `S3_BUCKET_NAME="<S3_BUCKET_NAME>" DYNAMODB_TABLE_NAME="<DYNAMODB_NAME>" REGION="<AWS_REGION>"` 2. Ejecute el script `bootstrap.sh` . El script requiere el AWS CLI, que ha instalado como parte de los requisitos previos. `cd bootstrap ./bootstrap.sh`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Actualice los `locals.tf` archivos `run.sh` y.	1. Cuando el proceso de arranque se complete correctamente, copie el bucket de S3 y el nombre de la tabla de DynamoDB de la sección `variables` del script: `bootstrap.sh` `# Variables S3_BUCKET_NAME="< S3_BUCKET_NAME>" DYNAMODB_TABLE_NAME ="<DYNAMODB_NAME"` 2. Pegue esos valores en el `run.sh` script, que se encuentra en el directorio raíz del proyecto: `BACKEND_BUCKET_ID= "<SAME_NAME_AS_S3_ BUCKET_NAME>" DYNAMODB_ID=" <SAME_NAME_AS_DYNA MODB_NAME>"` 3. Sube el código del proyecto a un CodeCommit repositor io. Puedes crear este repositorio automátic amente a través de Terraform configurando la siguiente variable `true` en el `demo/pipeline/loca ls.tf` archivo:	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`create_new_repo = true` 4. Actualice el `locals.tf` archivo de acuerdo con sus requisitos para crear recursos de canalización.	
Implemente el módulo Pipeline.	Para crear recursos de canalización, ejecuta los siguientes comandos de Terraform de forma manual. No hay ninguna organización para ejecutar estos comandos automáticamente. `./run.sh -m pipeline -e demo -r <AWS_REGION> -t init` `./run.sh -m pipeline -e demo -r <AWS_REGION> -t plan` `./run.sh -m pipeline -e demo -r <AWS_REGION> -t apply`	AWS DevOps

Cree la infraestructura de red

Tarea	Descripción	Habilidades requeridas
Iniciar la canalización.	1. En la `templates` carpeta, asegúrese de que los `buildspec` archivos tengan la siguiente variable establecida en`network`:	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`TF_MODULE_TO_BUILD: "network"` 2. En la CodePipeline consola, en la página de detalles de la canalización, inicia la canalización seleccionando Release change. Tras esta primera ejecución , la canalización se iniciará automáticamente cada vez que realices un cambio en la rama principal del CodeCommit repositorio. La canalización incluye las siguientes etapas: • `validate`inicializa Terraform, ejecuta los escaneos de seguridad de Terraform mediante las herramientas checkov y tfsec y carga los informes de escaneo en el bucket de S3. • `plan` muestra el plan de Terraform y lo carga en el depósito de S3. • `apply`aplica el resultado del plan Terraform del depósito de S3 y crea recursos. AWS	

Tarea	Descripción	Habilidades requeridas
	• `destroy`elimina los AWS recursos creados durante la `apply` etapa. Para habilitar esta etapa opcional, defina la siguiente variable `true` en el `demo/pipeline/locals.tf` archivo: `enable_destroy_stage = true`	

Tarea	Descripción	Habilidades requeridas
Valide los recursos creados a través del módulo de red.	Confirme que los siguiente s AWS recursos se crearon después de que la canalizac ión se implementara correctamente: • Una VPC de salida con tres subredes públicas y tres privadas, una puerta de enlace a Internet y una puerta de enlace NAT. • Una VPC de Amazon EKS con tres subredes privadas. • VPC de arrendatario 1 y arrendatario 2 con tres subredes privadas cada una. • Una puerta de enlace de tránsito con todos los adjuntos de la VPC y las rutas a cada subred privada. • Una ruta de puerta de enlace de tránsito estática para la VPC de salida de Amazon EKS con un bloque CIDR de destino de. `0.0.0.0/0` Esto es necesario para permitir que todas las VPC tengan acceso saliente a Internet a través de la VPC de salida de Amazon EKS.	AWS DevOps

Cree la infraestructura de cómputo

Tarea	Descripción	Habilidades requeridas
Actualice `locals.tf` para permitir el acceso del CodeBuild proyecto a la VPC.	Para implementar los complementos para el clúster privado de Amazon EKS, el CodeBuild proyecto debe estar adjunto a la VPC de Amazon EKS. 1. En la `demo/pipeline` carpeta, abra el `locals.tf` archivo y defina `true` la `vpc_enabled` variable en. 2. Ejecute el `run.sh` script para aplicar los cambios al módulo de canalización: `demo/pipeline/locals.tf` `./run.sh -m pipeline -env demo -region <AWS_REGION> -tfcmd init` `./run.sh -m pipeline -env demo -region <AWS_REGION> -tfcmd plan` `./run.sh -m pipeline -env demo -region <AWS_REGION> -tfcmd apply`	AWS DevOps
Actualice los `buildspec` archivos para crear el módulo de cómputo.	En la `templates` carpeta, en todos los archivos `buildspec` YAML, establece el valor de la	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`TF_MODULE_TO_BUILD` variable entrenetwork: `compute` `TF_MODULE_TO_BUILD: "compute"`	

Tarea	Descripción	Habilidades requeridas
Actualice el `values` archivo del diagrama Helm de administración de inquilinos.	1. Abra el `values.yaml` archivo en la siguiente ubicación: `cd cfg-terraform/demo/compute/cfg-tenant-mgmt` El archivo tiene este aspecto: `---` `global:` `  clusterRoles:` `  operator: platform-tenant` `  flux: flux-tenant-applier` `  flux:` `  tenantCloneBaseUrl: ${TEANT_BASE_URL}` `  repoSecret: ${TENANT_REPO_SECRET}` `tenants:` `  tenant-1:` `  quotas:` `  limits:` `  cpu: 1` `  memory: 1Gi` `  flux:` `  path: overlays/tenant-1` `  tenant-2:` `  quotas:` `  limits:` `  cpu: 1` `  memory: 2Gi` `  flux:`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`path: overlays/tenant-2` 2. En las `tenants` secciones `global` y, actualice la configuración en función de sus requisitos: • `tenantCloneBaseUrl` — Ruta al repositorio que aloja el código para todos los inquilinos (utilizamos el mismo repositorio de Git para todos los inquilinos) • `repoSecret` — El secreto de Kubernetes que contiene las claves SSH y los hosts conocidos para autenticarse en el repositorio Git de inquilinos global • `quotas`— Cuotas de recursos de Kubernetes que quieres aplicar a cada inquilino • `flux path`— Ruta a los archivos YAML de la aplicación de inquilinos en el repositorio global de inquilinos	

Tarea	Descripción	Habilidades requeridas
Valide los recursos informáticos.	Tras actualizar los archivos en los pasos anteriores, se CodePipeline inicia automáticamente. Confirme que creó los siguientes AWS recursos para la infraestructura informática: • Clúster Amazon EKS con punto final privado • Nodos de trabajadores de Amazon EKS • Complementos de Amazon EKS: secretos externos y `aws-loadbalancer-controller` `metrics-server` • GitOps módulo, gráfico de Flux Helm, gráfico de Cilium Helm y gráfico de Helm de gestión de inquilinos	AWS DevOps

Consulte la gestión de inquilinos y otros recursos

Tarea	Descripción	Habilidades requeridas
Valide los recursos de administración de inquilinos en Kubernetes.	Ejecuta los siguientes comandos para comprobar que los recursos de gestión de inquilinos se crearon correctamente con la ayuda de Helm. 1. Se crearon los espacios de nombres de inquilinos, tal	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	y como se especifica en: `values.yaml` `kubectl get ns -A` 2. Las cuotas se asignan a cada espacio de nombres de inquilinos, tal y como se especifica en: `values.yaml` `kubectl get quota --namespace=<tenant_namespace>` 3. Los detalles de las cuotas son correctos para cada espacio de nombres de inquilinos: `kubectl describe quota cpu-memory-resource-quota-limit -n <tenant_namespace>` 4. Las políticas de Cilium Network se aplicaron a cada espacio de nombres de inquilinos: `kubectl get CiliumNetworkPolicy -A`	

Tarea	Descripción	Habilidades requeridas
Verifique las implement aciones de las aplicaciones arrendatarias.	Ejecute los siguientes comandos para verificar que se hayan implementado las aplicaciones arrendatarias. 1. Flux puede conectarse al CodeCommit repositorio especificado en el GitOps módulo: `kubectl get gitreposi tories -A` 2. El controlador de personali zación de Flux ha desplegado los archivos YAML en el repositorio: CodeCommit `kubectl get kustomiza tions -A` 3. Todos los recursos de la aplicación se implement an en sus espacios de nombres de inquilinos: `kubectl get all -n <tenant_namespace>` 4. Se ha creado una entrada para cada inquilino: `kubectl get ingress -n <tenant_namespace>`	

Solución de problemas

Problema	Solución
Aparece un mensaje de error similar al siguiente: `Failed to checkout and determine revision: unable to clone unknown error: You have successfully authenticated over SSH. You can use Git to interact with AWS CodeCommit.`	Sigue estos pasos para solucionar el problema: 1. Compruebe el repositorio de aplicaciones arrendatario: es posible que el error se deba a un repositorio vacío o mal configura do. Asegúrese de que el repositorio de aplicaciones arrendatarias contenga el código necesario. 2. Vuelva a implementar el `tenant_mgmt` módulo: en el archivo de configuración del `tenant_mgmt` módulo, localice el `app` bloque y, a continuación, defina el `deploy` parámetro en: `0` `deploy = 0` Tras ejecutar el `apply` comando Terraform , vuelva a cambiar el valor del `deploy` parámetro a: 1 `deploy = 1` 3. Vuelva a comprobar el estado: tras ejecutar los pasos anteriores, utilice el siguiente comando para comprobar si el problema persiste: `kubectl get gitrepositories -A` Si persiste, considere la posibilidad de profundizar en los registros de Flux para obtener más detalles o consulte la guía general de solución de problemas de Flux.

Recursos relacionados

- Planos de Amazon EKS para Terraform
- Guías de prácticas recomendadas de Amazon EKS, sección sobre tenencia múltiple
- Sitio web de Flux
- Sitio web de Helm

Información adicional

A continuación, se muestra un ejemplo de estructura de repositorios para implementar aplicaciones arrendatarias:

```
applications
sample_tenant_app
### README.md
### base
#   ### configmap.yaml
#   ### deployment.yaml
#   ### ingress.yaml
#   ### kustomization.yaml
#   ### service.yaml
### overlays
    ### tenant-1
    #   ### configmap.yaml
    #   ### deployment.yaml
    #   ### kustomization.yaml
    ### tenant-2
        ### configmap.yaml
        ### kustomization.yaml
```

Suscriba varios puntos de conexión de correo electrónico a un tema de SNS mediante un recurso personalizado

Creado por Ricardo Morais (AWS)

Entorno: producción	Tecnologías: DevOps	Servicios de AWS: Amazon SNS CloudFormation; AWS Lambda

Resumen

Nota, agosto de 2022: AWS CloudFormation ahora admite la suscripción de varios recursos a través del AWS::SNS::Topicobjeto y su atributo de suscripción.

Este patrón describe cómo suscribirse a varias direcciones de correo electrónico para recibir notificaciones de un tema de Amazon Simple Notification Service (Amazon SNS). Utiliza una función de AWS Lambda como recurso personalizado en una plantilla de AWS CloudFormation . La función de Lambda está asociada a un parámetro de entrada que especifica los puntos de conexión de correo electrónico del tema de SNS.

Actualmente, puede utilizar los objetos de CloudFormation plantilla de AWS AWS::SNS::Topicy AWS::SNS::Subscriptionsuscribir puntos de enlace únicos a temas de SNS. Para suscribir varios puntos de conexión, debe invocar el objeto varias veces. Al utilizar la función de Lambda como recurso personalizado, puede suscribir varios puntos de conexión mediante un parámetro de entrada. Puede utilizar esta función de Lambda como recurso personalizado en cualquier plantilla de AWS CloudFormation .

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Un perfil de AWS configurado en su entorno local con una clave de acceso y una clave secreta. También puede ejecutar este código desde AWS Cloud9.
- Permisos para lo siguiente:
  - Rol y política de AWS Identity and Access Management (IAM)

- Función de AWS Lambda
- Amazon Simple Storage Service (Amazon S3) para cargar la función de Lambda.
- Tema y política de Amazon SNS
- Pilas CloudFormation de AWS

Limitaciones

- El código es compatible con estaciones de trabajo Linux y macOS.

Versiones de producto

- Interfaz de la línea de comandos de AWS (AWS CLI) versión 2 o posterior.

Arquitectura

Pila de tecnología de destino

- AWS CloudFormation
- Amazon SNS
- AWS Lambda

Herramientas

Herramientas

- CLI de AWS versión 2

Código

El adjunto incluye los siguientes archivos:

- Función de Lambda: `lambda_function.py`
- CloudFormation Plantilla de AWS: `template.yaml`
- Dos archivos de parámetros para gestionar las suscripciones de puntos de conexión de correo electrónico múltiples o únicas: `parameters-multiple-values.json` (se utilizan de forma predeterminada) y `parameters-one-value.json`

Para implementar la pila, puede usar cualquiera de los dos archivos de parámetros. Para especificar varios puntos de conexión de correo electrónico:

```
./deploy.sh -p <YOUR_AWS_PROFILE_NAME> -r <YOUR_AWS_PROFILE_REGION>
```

Para especificar un único punto de conexión de correo electrónico:

```
./deploy.sh -p <YOUR_AWS_PROFILE_NAME> -r <YOUR_AWS_PROFILE_REGION> -f parameters-one-value.json
```

Epics

Opción 1: implementar un tema de SNS con una suscripción de correo electrónico

Tarea	Descripción	Habilidades requeridas
Configure el punto de conexión de correo electrónico para las suscripciones a temas de SNS.	Edite el archivo `parameters-one-value.json` (adjunto) y cambie el valor del parámetro `pSNSNotificationsEmail` para que refleje la dirección de correo electrónico que desea usar, por ejemplo `someone@example.com` .	
Implemente la CloudFormation pila de AWS que crea los recursos y la suscripción.	Ejecute el comando deploy.sh con el nombre de su perfil de AWS, la región de AWS y el archivo `parameters-one-value.json` . `./deploy.sh -p <YOUR_AWS_PROFILE_NAME> -r <YOUR_AWS_PROFILE_REGION> -f parameters-one-value.json`	Rol de IAM con permisos adecuados

Opción 2: implementar un tema SNS con dos o más suscripciones de correo electrónico

Tarea	Descripción	Habilidades requeridas
Configure los puntos de conexión de correo electrónico para las suscripciones a temas de SNS.	Edite el archivo `parameters-multiple-values.json` (adjunto), y cambie el valor del parámetro `pSNSNotificationsEmail` para reflejar las direcciones de correo electrónico que desea utilizar, separadas por comas, de la siguiente manera: `someone1@example.com,someone2@example.com` .	
Implemente la CloudFormation pila de AWS que crea los recursos y la suscripción.	Ejecute el comando deploy.sh con su nombre de perfil de AWS y su región de AWS. No es necesario que especifique el archivo `parameters-multiple-values.json` porque se usa de forma predeterminada. `./deploy.sh -p <YOUR_AWS_PROFILE_NAME> -r <YOUR_AWS_PROFILE_REGION>`	Rol de IAM con permisos adecuados

Opción 3: Implementar un tema de SNS a través de una plantilla de AWS CloudFormation

Tarea	Descripción	Habilidades requeridas
Cree un tema de SNS.	Cree un tema de SNS a través de una CloudFormation	Rol de IAM con permisos adecuados

Tarea	Descripción	Habilidades requeridas
	plantilla de AWS, sin especificar los puntos de enlace de la suscripción en el objeto de `AWS::SNS::Topic` plantilla. Puede utilizar `template.yaml` en el adjunto como punto de partida.	
Crear política de tema de SNS.	Cree una política temática de SNS en la CloudFormation plantilla de AWS.	Rol de IAM con permisos adecuados
Suscriba la lista de puntos de conexión de correo electrónico al tema de SNS.	Según la lista de puntos de conexión de correo electrónico (uno o más), suscriba los puntos de conexión al tema de SNS que creó.	Rol de IAM con permisos adecuados

Recursos relacionados

Referencias

- Recursos CloudFormation personalizados de AWS (documentación de AWS)
- Creación de recursos CloudFormation personalizados de AWS con Python, AWS Lambda y crhelper (entrada del blog)

Herramientas necesarias

- CLI de AWS versión 2

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Use Serverspec para desarrollar código de infraestructura basado en pruebas

Creado por Sushant Jagdale (AWS)

Entorno: PoC o piloto	Tecnologías: Infraestructura DevOps; Nube híbrida	Servicios de AWS: Amazon EC2; AWS; AWS CodeBuild CodeDeploy

Resumen

Este patrón muestra cómo usar Serverspec para escribir código de infraestructura mediante desarrollo basado en pruebas en la nube de Amazon Web Services (AWS). El patrón también cubre la automatización con AWS CodePipeline. El TDD centra su atención en lo que debe hacer el código de infraestructura, y establece una definición clara del trabajo realizado. Puede usar Serverspec para probar la infraestructura creada por herramientas como AWS CloudFormation, Terraform by HashiCorp y Ansible.

Serverspec ayuda a refactorizar el código de infraestructura. Serverspec le permite escribir pruebas de RSpec para comprobar la instalación de distintos paquetes y software, ejecutar comandos, comprobar procesos y puertos en ejecución, comprobar la configuración de permisos de los archivos, etc. Serverspec comprueba si sus servidores están configurados correctamente. Solo tiene que instalar Ruby en sus servidores. No es necesario instalar ningún software de agente.

La infraestructura basada en pruebas proporciona los siguientes beneficios:

- Actualizaciones entre plataformas
- Validación de las expectativas
- Confianza en su automatización
- Coherencia y estabilidad de la infraestructura
- Errores tempranos

Puede usar este patrón para ejecutar pruebas unitarias de Serverspec en el software Apache y comprobar la configuración de permisos de los archivos durante la creación de imágenes de

máquina de Amazon (AMI). Solo se creará la AMI si se superan todos los casos de prueba. Serverspec realizará las siguientes pruebas:

- El proceso de Apache se está ejecutando.
- El puerto de Apache se está ejecutando.
- Los archivos y directorios de configuración de Apache existen en sus ubicaciones, etc.
- Los permisos de los archivos están configurados correctamente.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- AWS CodeBuild
- AWS CodeCommit
- AWS CodePipeline
- Una nube privada virtual (VPC) con una subred pública
- Instalación de Interfaz de la línea de comandos de AWS (AWS CLI) y Git

Versiones de producto

- HashiCorp Versión Packer: 1.6.6
- Versión 2.5.1 y posteriores
- AWS CLI versión 1.18.185

Arquitectura

Arquitectura de destino

1. Cuando insertas el código en el CodeCommit repositorio, un evento de Amazon CloudWatch Events activa el CodePipeline. En la primera etapa de la canalización, se obtiene el código de. CodeCommit
2. Se ejecuta la segunda etapa de canalización CodeBuild, que valida y crea la plantilla de Packer.

3. Como parte del aprovisionador de compilaciones de Packer, Packer instala el software Ruby y Apache. A continuación, el aprovisionador llama a un script de intérprete de comandos que usa Serverspec para realizar pruebas unitarias del proceso, el puerto, los archivos y los directorios de Apache. El postprocesador Packer escribe un archivo de notación de JavaScript objetos (JSON) con una lista de todos los artefactos producidos por Packer durante una ejecución
4. Por último, se crea una instancia de Amazon Elastic Compute Cloud (Amazon EC2) con el ID de AMI producido por Packer.

Herramientas

- AWS CLIla linterfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.
- Amazon CloudWatch Events: Amazon CloudWatch Events ofrece una near-real-time secuencia de eventos del sistema que describen los cambios en los recursos de Amazon Web Services (AWS).
- AWS CodeBuild: AWS CodeBuild es un servicio de compilación en la nube totalmente gestionado. CodeBuild compila su código fuente, ejecuta pruebas unitarias y produce artefactos listos para su implementación.
- AWS CodeCommit: AWS CodeCommit es un servicio de control de versiones hospedado por Amazon Web Services. Puede utilizarlo CodeCommit para almacenar y gestionar de forma privada activos (como documentos, código fuente y archivos binarios) en la nube.
- AWS CodePipeline: AWS CodePipeline es un servicio de entrega continua que puede utilizar para modelar, visualizar y automatizar los pasos necesarios para lanzar su software. Puede diseñar y configurar rápidamente las diferentes etapas de un proceso de lanzamiento de software.
- HashiCorp Packer: HashiCorp Packer es una herramienta para automatizar la creación de imágenes de máquinas idénticas a partir de una configuración de fuente única.
- Serverspec: Serverspec ejecuta pruebas de RSpec para comprobar la configuración del servidor. Serverspec usa Ruby, y no es necesario instalar el software del agente.

Código

El código está adjunto. El código emplea la siguiente estructura, con tres directorios y ocho archivos.

```
### amazon-linux_packer-template.json (Packer template)
### buildspec.yaml (CodeBuild .yaml file)
```

```
### pipeline.yaml (AWS CloudFormation template to automate CodePipeline)
### rspec_tests (RSpec required files and spec)
#   ### Gem-file
#   ### Rakefile
#   ### spec
#       ### apache_spec.rb
#       ### spec_helper.rb
### scripts
    ### rspec.sh (Installation of Ruby and initiation of RSpec)
```

Epics

Configurar credenciales de AWS

Tarea	Descripción	Habilidades requeridas
Cree un usuario de IAM.	Cree un usuario de AWS Identity and Access Management (usuario de IAM) con acceso de consola y programático. Para obtener más información, consulte la documentación de AWS.	Desarrollador, administrador de sistemas, ingeniero DevOps
Configurar credenciales de AWS.	En su ordenador local o en su entorno, configure las credenciales de AWS para el usuario de IAM. Para obtener instrucciones, consulte la documentación de AWS.	Desarrollador, administrador de sistemas, DevOps ingeniero
Pruebe sus credenciales.	Para validar las credencia les configuradas, ejecute el siguiente comando. `aws sts get-caller-identity --profile <profile>`	Desarrollador, administrador de sistemas, DevOps ingeniero

AWS CodePipeline

Tarea	Descripción	Habilidades requeridas
Cree un CodeCommit repositorio.	Para crear un CodeCommit repositorio, ejecute el siguiente comando. `aws codecommit create-repository --repository-name "<provide repository-name>" --repository-description "repository to unit test the infrastructure code"`	Desarrollador, administrador de sistemas, DevOps ingeniero
Escriba pruebas de RSpec.	Cree casos de prueba de RSpec para su infraestructura. Para obtener más información, consulte la sección Información adicional.	Desarrollador, DevOps ingeniero
Envía el código al CodeCommit repositorio.	Para enviar el código adjunto al CodeCommit repositorio, ejecuta los siguientes comandos. `git clone <repository url>` `cp -R /tmp/<code folder>/ <repository_folder>/` `git add .` `git commit -m"initial commit"` `git push`	Desarrollador, administrador de sistemas, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Crear la canalización.	Para crear el proceso, ejecute en la CLI de AWS el comando que encontrará en la sección Información adicional.	Desarrollador, administrador de sistemas, DevOps ingeniero
Iniciar la canalización.	Envíe el código al CodeCommit repositorio. La confirmación en el repositorio iniciará el proceso.	Desarrollador, administrador de sistemas, DevOps ingeniero
Pruebe la URL de Apache.	Para probar la instalación de la AMI, use la siguiente URL. `http://<your instance public ip>/hello.html` La página mostrará un mensaje de “Hola desde Apache”.	Desarrollador, administrador de sistemas, DevOps ingeniero

Recursos relacionados

- HashiCorp
- HashiCorp Empacador
- Serverspec
- Introducción a ServerSpec: ¿Qué es Serverspec y cómo lo utilizamos en Stelligent? (entrada de blog externa)
- Desarrollo de código de infraestructura basado en pruebas (publicación de blog externa)
- Creación y prueba de imágenes con HashiCorp Packer y ServerSpec (artículo externo)

Información adicional

Escriba pruebas de RSpec

La prueba RSpec para este patrón se encuentra en `<repository folder>/rspec_tests/spec/apache_spec.rb`.

```
require 'spec_helper'


describe service('httpd') do
  it { should be_enabled }
  it { should be_running }
end


describe port(80) do
  it { should be_listening }
end


describe file('/etc/httpd/conf/httpd.conf') do
  it { should exist }
  it { should be_owned_by 'root' }
  it { should contain 'ServerName www.example.com' }
end


describe file('/etc/httpd/conf/httpd.conf') do
  its(:content) { should match /ServerName www.example.com/ }
end


describe file('/var/www/html/hello.html') do
  it { should exist }
  it { should be_owned_by 'ec2-user' }
end


describe file('/var/log/httpd') do
  it { should be_directory }
end


describe file('/etc/sudoers') do
  it { should be_mode 440 }
end
```

```
describe group('root') do
  it { should have_gid 0 }
end
```

Puede añadir sus propias pruebas al directorio `/spec`.

Crear la canalización

```
aws cloudformation create-stack --stack-name myteststack --template-body file://
pipeline.yaml --parameters ParameterKey=RepositoryName,ParameterValue=<provide
 repository-name> ParameterKey=ApplicationName,ParameterValue=<provide
 application-name> ParameterKey=SecurityGroupId,ParameterValue=<provide
 SecurityGroupId> ParameterKey=VpcId,ParameterValue=<provide VpcId>
 ParameterKey=SubnetId,ParameterValue=<provide SubnetId> ParameterKey=Region,ParameterValue=<pr
 AccountId> --capabilities CAPABILITY_NAMED_IAM
```

Detalles de los parámetros

`repository-name`— El nombre del CodeCommit repositorio de AWS

`application-name`: Los nombres de recurso de Amazon (ARN) están vinculados con `ApplicationName`; proporcione cualquier nombre

`SecurityGroupId`: Cualquier ID de grupo de seguridad de su cuenta de AWS que tenga el puerto 80 abierto

`VpcId`: ID de su VPC

`SubnetId`: ID de una subred pública de su VPC

`Region`: Región de AWS en la que se ejecuta este patrón

`Keypair`: Nombre de la clave de Secure Shell (SSH) para iniciar sesión en la instancia de EC2

`AccountId`: Su ID de cuenta de AWS

También puede crear una CodePipeline canalización mediante la consola de administración de AWS y pasar los mismos parámetros que estaban en la línea de comandos anterior.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Utilice repositorios de código fuente de Git de terceros en AWS CodePipeline

Entorno: PoC o piloto	Tecnologías: DevOps	Carga de trabajo: código abierto
Servicios de AWS: AWS CodeBuild CodePipeline; AWS Lambda		

Resumen

Este patrón describe cómo usar AWS CodePipeline con repositorios de código fuente de Git de terceros.

AWS CodePipeline es un servicio de entrega continua que automatiza las tareas de creación, prueba e implementación del software. Actualmente, el servicio es compatible con los repositorios de Git gestionados por GitHub AWS CodeCommit y Atlassian Bitbucket. Sin embargo, algunas empresas utilizan repositorios Git de terceros que están integrados con su servicio de inicio de sesión único (SSO) y Microsoft Active Directory para la autenticación. Puedes usar estos repositorios de Git de terceros como fuentes CodePipeline creando acciones personalizadas y webhooks.

Un webhook es una notificación HTTP que detecta eventos en otra herramienta, como un GitHub repositorio, y conecta esos eventos externos a una canalización. Cuando creas un webhook en CodePipeline, el servicio devuelve una URL que puedes usar en el webhook de tu repositorio de Git. Si insertas código en una rama específica del repositorio de Git, el webhook de Git inicia el CodePipeline webhook a través de esta URL y establece la etapa de origen de la canalización como En progreso. Cuando la canalización se encuentra en este estado, el trabajador CodePipeline busca el trabajo personalizado, lo ejecuta y envía un estado de éxito o fracaso a. CodePipeline En este caso, dado que la canalización se encuentra en la fase de origen, el trabajador obtiene el contenido del repositorio de Git, lo comprime y lo carga en el depósito de Amazon Simple Storage Service (Amazon S3), donde se almacenan los artefactos de la canalización, utilizando la clave de objeto proporcionada por el trabajo sondeado. También puedes asociar una transición para la acción personalizada a un evento en Amazon CloudWatch e iniciar el trabajo en función del evento. Esta

configuración te permite usar repositorios Git de terceros que el servicio no admite de forma nativa como fuentes. CodePipeline

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un repositorio de Git que admite webhooks y puede conectarse a una URL de CodePipeline webhook a través de Internet
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada con la cuenta de AWS

Arquitectura

El patrón incluye los siguientes pasos:

1. El usuario confirma el código en un repositorio de Git.
2. Se llama el webhook de Git.
3. Se llama CodePipeline webhook.
4. La canalización está configurada En curso y la etapa de origen está configurada en el estado En curso.
5. La acción de la etapa de origen inicia una regla de CloudWatch eventos, lo que indica que se ha iniciado.
6. El CloudWatch evento inicia una función Lambda.
7. La función de Lambda obtiene los detalles del trabajo de acción personalizado.
8. La función Lambda inicia CodeBuild AWS y le pasa toda la información relacionada con el trabajo.
9. CodeBuild obtiene la clave SSH pública o las credenciales de usuario para el acceso a HTTPS Git desde Secrets Manager.
10. CodeBuild clona el repositorio de Git para una rama específica.
11. CodeBuild comprime el archivo y lo carga en el depósito de S3 que sirve como almacén de CodePipeline artefactos.

Herramientas

- AWS CodePipeline: AWS CodePipeline es un servicio de entrega continua totalmente gestionado que le ayuda a automatizar sus procesos de lanzamiento para obtener actualizaciones rápidas y fiables de las aplicaciones y la infraestructura. CodePipeline automatiza las fases de creación, prueba e implementación del proceso de publicación para cada cambio de código, en función del modelo de publicación que defina. Le permite entregar características y actualizaciones de forma rápida y de confianza. Puede integrar AWS CodePipeline con servicios de terceros, como GitHub su propio complemento personalizado.
- AWS Lambda: AWS Lambda le permite ejecutar código sin aprovisionar ni administrar servidores. Con Lambda, puede ejecutar código para prácticamente cualquier tipo de aplicación o servicio backend sin necesidad de administración. Sólo tiene que cargar su código y Lambda se encarga de todo lo necesario para ejecutar y escalar su código con alta disponibilidad. Puede configurar el código para que se active automáticamente desde otros servicios de AWS o puede llamarlo directamente desde cualquier aplicación web o móvil.
- AWS CodeBuild: AWS CodeBuild es un servicio de integración continua totalmente gestionado que compila el código fuente, ejecuta pruebas y produce paquetes de software listos para su implementación. Con CodeBuild, no necesita aprovisionar, administrar ni escalar sus propios servidores de compilación. CodeBuild escala de forma continua y procesa varias compilaciones de forma simultánea, para que sus compilaciones no se queden esperando en una cola. Puede comenzar con rapidez usando entornos de compilación preempaquetados, o crear sus propios entornos de compilación personalizados que utilicen sus propias herramientas de compilación.
- AWS Secrets Manager: AWS Secrets Manager le ayuda a proteger los secretos necesarios para acceder a sus aplicaciones, servicios y recursos de TI. El servicio le permite rotar, administrar y recuperar fácilmente credenciales de bases de datos, claves de API y otros datos confidenciales durante todo su ciclo de vida. Los usuarios y las aplicaciones recuperan los secretos llamando a las API de Secrets Manager, sin tener que codificar información confidencial en texto plano. Secrets Manager ofrece rotación secreta con integración integrada para Amazon Relational Database Service (Amazon RDS), Amazon Redshift y Amazon DocumentDB. El servicio se puede ampliar para admitir otros tipos de secretos, incluidas las claves de API y los tokens de OAuth. Además, Secrets Manager le permite controlar el acceso a los datos secretos mediante permisos detallados y auditar la rotación de secretos de forma centralizada para los recursos de la nube de AWS, los servicios de terceros y los entornos locales.
- Amazon CloudWatch: Amazon CloudWatch es un servicio de monitoreo y observación creado para DevOps ingenieros, desarrolladores, ingenieros de confiabilidad de sitios (SRE) y administradores de TI. CloudWatch le proporciona datos e información útil para supervisar sus aplicaciones,

responder a los cambios en el rendimiento de todo el sistema, optimizar la utilización de los recursos y obtener una visión unificada del estado de las operaciones. CloudWatch recopila datos operativos y de supervisión en forma de registros, métricas y eventos, lo que le proporciona una visión unificada de los recursos, las aplicaciones y los servicios de AWS que se ejecutan en AWS y en servidores locales. Puede utilizarlos CloudWatch para detectar comportamientos anómalos en sus entornos, configurar alarmas, visualizar registros y métricas uno al lado del otro, tomar medidas automatizadas, solucionar problemas y descubrir información para que sus aplicaciones sigan funcionando sin problemas.

- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos que le permite almacenar y proteger cualquier cantidad de datos para diversos casos de uso, tales como sitios web, aplicaciones móviles, copia de seguridad y restauración, archivado, aplicaciones empresariales, dispositivos IoT y análisis de macrodatos. Amazon S3 ofrece funciones easy-to-use de administración que le ayudan a organizar sus datos y configurar controles de acceso ajustados con precisión para cumplir con sus requisitos empresariales, organizativos y de conformidad específicos.

Epics

Cree una acción personalizada en CodePipeline

Tarea	Descripción	Habilidades requeridas
Cree una acción personalizada mediante AWS CLI o AWS CloudFormation.	Este paso implica la creación de una acción de origen personalizada que se pueda utilizar en la fase de origen de una canalización en su cuenta de AWS en una región concreta. Debe usar AWS CLI o AWS CloudFormation (no la consola) para crear la acción de origen personalizada. Para obtener más información sobre los comandos y los pasos descritos en esta y otras	AWS general

Tarea	Descripción	Habilidades requeridas
	epics, consulte la sección «Recursos relacionados» al final de este patrón. En AWS CLI, utilice el create-custom-action-type comando. Utilice --configuration-properties para proporcionar todos los parámetros necesarios para que el trabajador del trabajo los procese cuando busca un trabajo CodePipeline . Asegúrese de anotar los valores proporcionados a las opciones --provider y --action-version, de modo que puedas usar los mismos valores al crear la canalización con esta etapa fuente personalizada. También puede crear la acción de origen personalizada en AWS CloudFormation mediante el tipo de recurso AWS::CodePipeline::CustomAction Type.	

Configuración de la autenticación

Tarea	Descripción	Habilidades requeridas
Cree un par de claves SSH.	Cree un par de claves Secure Shell (SSH). Para obtener instrucciones, consulte la GitHub documentación.	Ingeniero de sistemas/DevOps

Tarea	Descripción	Habilidades requeridas
Crear un secreto en AWS Secrets Manager.	Copie el contenido de la clave privada del par de claves SSH y cree un secreto en AWS Secrets Manager. Este secreto se utiliza para la autenticación al acceder al repositorio de Git.	AWS general
Añada la clave pública al repositorio de Git.	Añada la clave pública del par de claves SSH a la configuración de la cuenta del repositorio de Git para autenticarte con la clave privada.	Ingeniero de sistemas/ DevOps

Crear una canalización y un webhook

Tarea	Descripción	Habilidades requeridas
Crear una canalización que incluya la acción de origen personalizada.	Crea una canalización en CodePipeline. Al configurar la etapa de origen, elija la acción de origen personalizada que creó anteriormente. Puede hacerlo en la CodePipeline consola de AWS o en la CLI de AWS. CodePipeline le solicita las propiedades de configuración que ha establecido en la acción personalizada. Esta información es necesaria para que el trabajador procese el trabajo para la acción personalizada. Siga las instrucciones del	AWS general

Tarea	Descripción	Habilidades requeridas
	asistente y cree la siguiente etapa para la canalización.	
Crea un CodePipeline webhook.	Cree un webhook para la canalización que creócon la acción de origen personalizada. Debe usar AWS CLI o AWS CloudFormation (no la consola) para crear el webhook. En AWS CLI, ejecute el comando put-webhook y proporcione los valores adecuados para las opciones de webhook. Anote la URL del webhook que devuelve el comando. Si utiliza AWS CloudFormation para crear el webhook, utilice el tipo AWS::CodePipeline::Webhook de recurso. Asegúrese de generar la URL del webhook del recurso creado y anotarla.	AWS general

Tarea	Descripción	Habilidades requeridas
Cree una función y CodeBuild un proyecto de Lambda.	En este paso, utilizará Lambda y CodeBuild creará un trabajador laboral que sondeará las solicitudes de trabajo CodePipeline para la acción personali zada, ejecutará el trabajo y devolverá el resultado de estado al. CodePipeline Cree una función Lambda que se inicie mediante una regla de Amazon CloudWatch Events cuando la etapa de acción de origen personali zada de la canalización pase a «En curso». Cuando se inicia la funciónde Lambda, debe obtener los detalles del trabajo de acción personali zado consultando los trabajos. Puede utilizar la PollForJo bs API para devolver esta información. Una vez obtenida la información del trabajo sondeada, la función de Lambda debe devolver un acuse de recibo y, a continuac ión, procesar la información con los datos que obtiene de las propiedades de configura ción de la acción personali zada. Cuando el trabajado r esté listo para comunicar se con el repositorio de Git,	AWS general, desarrollador de código

Tarea	Descripción	Habilidades requeridas
	puedes iniciar un CodeBuild proyecto, ya que es conveniente gestionar las tareas de Git mediante el cliente SSH.	

Crea un evento en CloudWatch

Tarea	Descripción	Habilidades requeridas
Crea una regla de CloudWatch eventos.	Cree una regla de CloudWatch eventos que inicie la función Lambda como objetivo siempre que la etapa de acción personalizada de la canalización pase a «En curso».	AWS general

Recursos relacionados

Crear una acción personalizada en CodePipeline

- Cree y añada una acción personalizada en CodePipeline
- AWS::CodePipeline::CustomActionEscriba un recurso

Configurar la autenticación

- Creación y administración de secretos con AWS Secrets Manager

Crear una canalización y un webhook

- Cree una canalización en CodePipeline
- Referencia del comando put-webhook
- AWS::CodePipeline::Webhook recurso

- PollForJobs Referencia de la API
- Cree y añada una acción personalizada en CodePipeline
- Cree un proyecto de compilación en AWS CodeBuild

Creación de un evento

- Detecte los cambios en el estado de la canalización y reaccione ante ellos con Amazon CloudWatch Events

Referencias adicionales

- Trabajando con canalizaciones en CodePipeline
- Guía para desarrolladores de AWS Lambda

Cree una canalización de CI/CD para validar las configuraciones de Terraform mediante AWS CodePipeline

Creado por Aromal Raj Jayarajan (AWS) y Vijesh Vijayakumaran Nair (AWS)

Repositorio de código: aws-codepipeline-terraform-cicd - samples	Entorno: PoC o piloto	Tecnologías: DevOps
Carga de trabajo: todas las demás cargas de trabajo	Servicios de AWS: AWS CodeBuild CodeCommit; AWS CodePipeline; Amazon S3; AWS Identity and Access Management	

Resumen

Este patrón muestra cómo probar las configuraciones de HashiCorp Terraform mediante una canalización de integración y entrega continuas (CI/CD) implementada por AWS. CodePipeline

Terraform es una aplicación de interfaz de la línea de comandos que le ayuda a usar código para aprovisionar y administrar la infraestructura y los recursos de la nube. La solución que se proporciona en este patrón crea una canalización de CI/CD que le ayuda a validar la integridad de las configuraciones de Terraform mediante cinco etapas: CodePipeline

1. `"checkout"`extrae la configuración de Terraform que está probando de un repositorio de AWS CodeCommit .
2. `"validate"`ejecuta herramientas de validación infrastructure-as-cod (iAC), incluidas tfsec, tFlint y checkov. La etapa también ejecuta los siguientes comandos de validación de Terraform IaC: `terraform validate` y `terraform fmt`.
3. `"plan"` muestra qué cambios se aplicarán a la infraestructura si se aplica la configuración de Terraform.
4. `"apply"` utiliza el plan generado para aprovisionar la infraestructura requerida en un entorno de prueba.
5. `"destroy"` elimina la infraestructura de prueba que se creó durante la `"apply"` etapa.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Interfaz de la línea de comandos de AWS (AWS CLI)instalada y configurada
- Git, instalado y configurado en su equipo local
- Terraform, instalado y configurado en su equipo local

Limitaciones

- El enfoque de este patrón implementa AWS CodePipeline en una sola cuenta de AWS y solo en una región de AWS. Se requieren cambios de configuración para las implementaciones de varias cuentas y regiones.
- El rol de AWS Identity and Access Management (IAM) que proporciona este patrón (codepipeline_iam_role) sigue el principio de privilegio mínimo. Los permisos de este rol de IAM deben actualizarse en función de los recursos específicos que necesite crear su canalización.

Versiones de producto

- Versión de AWS CLI 2.9.15 o posterior
- Versión de Terraform 1.3.7 o posterior

Arquitectura

Pila de tecnología de destino

- AWS CodePipeline
- AWS CodeBuild
- AWS CodeCommit
- AWS IAM
- Amazon Simple Storage Service (Amazon S3)
- AWS Key Management Service (AWS KMS)
- Terraform

Arquitectura de destino

El siguiente diagrama muestra un ejemplo de flujo de trabajo de canalización de CI/CD para probar las configuraciones de Terraform. CodePipeline

En el diagrama, se muestra el siguiente flujo de trabajo:

1. En CodePipeline, un usuario de AWS inicia las acciones propuestas en un plan de Terraform ejecutando el `terraform apply` comando en la CLI de AWS.
2. AWS CodePipeline asume una función de servicio de IAM que incluye las políticas necesarias para acceder CodeCommit a AWS KMS y Amazon S3. CodeBuild
3. CodePipeline ejecuta la etapa de `“checkout”` canalización para extraer la configuración de Terraform de un CodeCommit repositorio de AWS para probarla.
4. CodePipeline ejecuta la `“validate”` etapa para probar la configuración de Terraform ejecutando las herramientas de validación de IaC y los comandos de validación de Terraform IaC en un proyecto. CodeBuild
5. CodePipeline ejecuta la `“plan”` etapa para crear un plan en el CodeBuild proyecto basado en la configuración de Terraform. El usuario de AWS puede revisar este plan antes de aplicar los cambios al entorno de prueba.
6. Code Pipeline ejecuta la `“apply”` fase de implementación del plan utilizando el CodeBuild proyecto para aprovisionar la infraestructura requerida en el entorno de prueba.
7. CodePipeline ejecuta la `“destroy”` etapa, que se utiliza CodeBuild para eliminar la infraestructura de prueba que se creó durante la `“apply”` etapa.
8. Un bucket de Amazon S3 almacena los artefactos de la canalización, que se cifran y descifran mediante una clave administrada por el cliente de AWS KMS.

Herramientas

Herramientas

Servicios de AWS

- AWS le CodePipeline ayuda a modelar y configurar rápidamente las diferentes etapas de una versión de software y a automatizar los pasos necesarios para publicar cambios de software de forma continua.

- AWS CodeBuild es un servicio de compilación totalmente gestionado que le ayuda a compilar código fuente, ejecutar pruebas unitarias y producir artefactos listos para su implementación.
- AWS CodeCommit es un servicio de control de versiones que le ayuda a almacenar y gestionar repositorios de Git de forma privada, sin necesidad de gestionar su propio sistema de control de código fuente.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Key Management Service (AWS KMS) facilita poder crear y controlar claves criptográficas para proteger los datos.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Otros servicios

- HashiCorp Terraform es una aplicación de interfaz de línea de comandos que le ayuda a usar código para aprovisionar y administrar la infraestructura y los recursos de la nube.

Código

El código de este patrón está disponible en el repositorio. GitHub aws-codepipeline-terraform-cicdsamples El repositorio contiene las configuraciones de Terraform necesarias para crear la arquitectura de destino descrita en este patrón.

Epics

Aprovisionar los componentes de la solución

Tarea	Descripción	Habilidades requeridas
Clona el GitHub repositorio.	Clone el GitHub aws-codepipeline-terraform-cicdsamplesrepositorio ejecutando el siguiente comando en una ventana de terminal: `git clone https://github.com/aws-samp`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`les/aws-codepipeli ne-terraform-cicd- samples.git` Para obtener más informaci ón, consulte Clonación de un repositorio en la GitHub documentación.	
Cree un archivo de definicio nes de variables de Terraform.	Cree un archivo `terraform .tfvars` en función de los requisitos del caso de uso. Puede actualizar las variables del archivo `examples/ terraform.tfvars` que se encuentra en el repositorio clonado. Para obtener más informaci ón, consulte Asignación de valores a las variables del módulo raíz en la documenta ción de Terraform. Nota: El archivo del repositor io `Readme.md` incluye más información sobre las variables obligatorias.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Configure AWS como proveedor de Terraform.	1. En un editor de código, abra el archivo `main.tf` del repositorio clonado. 2. Añada las configuraciones necesarias para establecer la conectividad con la cuenta de AWS de destino. Para obtener más información, consulte AWS provider en la documentación de Terraform.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Actualice la configuración del proveedor de Terraform para crear el bucket de replicación de Amazon S3.	1. Ejecute el siguiente comando para abrir el directorio S3 del repositorio: `cd ./modules/s3` 2. Actualice la configuración del proveedor de Terraform para crear el depósito de replicación de Amazon S3 actualizando el valor `region` en del archivo `tf`. Asegúrese de introducir la región en la que desea que Amazon S3 replique los objetos. 3. (Opcional) De forma predeterminada, Terraform usa archivos estatales locales para la administr ación estatal. Si desea añadir Amazon S3 como backend remoto, debe actualizar la configuración de Terraform. Para obtener más información, consulte Configuración de backend en la documentación de Terraform. Nota: Con la replicación de S3 es posible copiar objetos entre buckets de Amazon S3 de	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	forma automática y asincróni ca.	
Inicialice la configuración de Terraform.	Para inicializar el directorio de trabajo que contiene los archivos de configuración de Terraform, ejecute el siguiente comando en la carpeta raíz del repositorio clonado: `terraform init`	DevOps ingeniero
Crear el plan Terraform.	Para crear un plan de Terraform, ejecuta el siguiente comando en la carpeta raíz del repositorio clonado: `terraform plan --var-file=terraform.tfvars -out=tfplan` Nota: Terraform evalúa los archivos de configuración para determinar el estado objetivo de los recursos declarados. A continuación, compara el estado objetivo con el estado actual y crea un plan.	DevOps ingeniero
Verifique el plan de Terraform.	Revise el plan Terraform y confirme que configura la arquitectura requerida en su cuenta de AWS de destino.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Implemente la solución.	1. Para aplicar el plan Terraform, ejecute el siguiente comando en la carpeta raíz del repositorio clonado: `terraform apply "tfplan"` 2. Escriba sí para confirmar que desea implementar los recursos. Nota: Terraform crea, actualiza o destruye la infraestructura para alcanzar el estado objetivo declarado en los archivos de configura ción.	DevOps ingeniero

Validar las configuraciones de Terraform ejecutando la canalización

Tarea	Descripción	Habilidades requeridas
Configurar el repositorio de código fuente.	1. De la salida de Terraform , obtenga los detalles del repositorio de origen del repositorio que contiene las configuraciones de Terraform que desea validar. 2. Inicie sesión en la Consola de administración de AWS.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Luego, abre la CodeCommit consola. 3. Cree una nueva rama en el repositorio de origen denominado `main`. Para obtener instrucciones, consulte Crear una rama en AWS CodeCommit en la CodeCommit documentación. 4. Clone la rama `main` del repositorio de origen en su estación de trabajo local. Para obtener instrucciones, consulte los pasos de configuración de las conexiones HTTPS a CodeCommit los repositorios de AWS en Windows con el asistente de credenciales de la CLI de AWS en la documentación. CodeCommit 5. Copie la **`templates`** carpeta del GitHub aws-codepipeline-terraform-cicdsamplesrepositorio ejecutando el siguiente comando: `cp -r templates $YOUR_CODECOMMIT_REPO_ROOT`	

Tarea	Descripción	Habilidades requeridas
	Nota: La carpeta `templates` contiene los archivos de especific aciones de compilación y el script de validación del directorio raíz del repositor io de origen. 6. Añada las configuraciones de Terraform iAC necesaria s a la carpeta raíz del repositorio de origen. 7. Agñada los detalles del backend remoto en la configuración de Terraform de su proyecto. Para obtener más información, consulte S3 en la documentación de Terraform. 8. (Opcional) Actualice las variables de la carpeta `templates` para activar o desactivar los escaneos preconfigurados, cambiar las versiones de las herramientas y especificar su directorio en archivos de script personalizados. Para obtener más informaci ón, consulte la sección Información adicional de este patrón.	

Tarea	Descripción	Habilidades requeridas
	9. Envía los cambios a la rama `main` del repositorio de origen.	

Tarea	Descripción	Habilidades requeridas
Valide las etapas de la canalización.	1. Inicie sesión en la consola de administración de AWS y abra la consola de CodePipeline . 2. En el resultado generado por el `terraform apply "tfplan"` comando de la sección anterior de Epic, busca el nombre del generado CodePipeline. 3. Abre la canalización en la CodePipeline consola y selecciona Release change. 4. Revise cada etapa de la canalización y confirma que funciona según lo esperado. Para obtener más información, consulte Ver los detalles y el historial de la canalización (consola) en la Guía del CodePipeline usuario de AWS. Importante: cuando se confirma un cambio en la rama principal del repositorio de origen, la canalización de pruebas se activa automáticamente.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Verifique el resultado del informe.	1. En la CodePipeline consola, en el panel de navegación izquierdo, selecciona Construir. A continuación, seleccione Historial de informes. 2. Revise los informes de escaneo tfsec y checkov que genera la canalización. Estos informes pueden ayudarle a identificar problemas mediante visualizaciones y representaciones gráficas. Nota: El `<project_name>-validate` CodeBuild proyecto genera informes de vulnerabilidad para el código durante la “`validate`” fase.	DevOps ingeniero

Eliminación de sus recursos

Tarea	Descripción	Habilidades requeridas
Limpie la canalización y los recursos asociados.	Para eliminar los recursos de prueba de su cuenta de AWS, ejecute el siguiente comando en la carpeta raíz del repositorio clonado:	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`terraform destroy --var-file=terraform.tfvars`	

Solución de problemas

Problema	Solución
Recibes un AccessDenied error durante la `“apply”` etapa.	1. Revise los registros de ejecución del CodeBuild proyecto asociados a la `“apply”` etapa para identificar los permisos de IAM que falten. Para obtener más información, consulte Ver los detalles de la compilación en AWS CodeBuild en la Guía del CodeBuild usuario de AWS. 2. En un editor de código, abra la carpeta del repositorio clonado `modules` . A continuación, navegue hasta la carpeta `iam-role` y abra el archivo `main.tf` que se encuentra en esa carpeta. 3. En la declaración `codepipeline_policy` , añada las políticas de IAM necesarias para aprovisionar recursos en su cuenta de AWS.

Recursos relacionados

- Bloques de módulos (documentación de Terraform)
- Cómo usar la CI/CD para implementar y configurar los servicios de seguridad de AWS con Terraform (entrada del blog de AWS)
- Uso de roles vinculados a servicios (documentación de IAM)
- create-pipeline (documentación de AWS CLI)

- Configurar el cifrado del lado del servidor para los artefactos almacenados en Amazon S3 para (documentación de CodePipeline AWS CodePipeline)
- Cuotas para AWS CodeBuild (CodeBuild documentación de AWS)
- Protección de datos en AWS CodePipeline (CodePipeline documentación de AWS)

Información adicional

Módulos Terraform personalizados

La siguiente es una lista de los módulos personalizados de Terraform que se utilizan en este patrón:

- `codebuild_terraform`crea los CodeBuild proyectos que forman cada etapa del proceso.
- `codecommit_infrastructure_source_repo`captura y crea el CodeCommit repositorio de origen.
- `codepipeline_iam_role` crea las funciones de IAM necesarias para la canalización.
- `codepipeline_kms` crea la clave de AWS KMS necesaria para el cifrado y descifrado de objetos de Amazon S3.
- `codepipeline_terraform`crea la canalización de pruebas para el CodeCommit repositorio de origen.
- `s3_artifacts_bucket` crea un bucket de Amazon S3 para administrar los artefactos de canalización.

Cree archivos de especificaciones

La siguiente es una lista de los archivos de especificaciones de compilación (buildspec) que este patrón utiliza para ejecutar cada etapa de la canalización:

- `buildspec_validate.yml` ejecuta la etapa “`validate`”.
- `buildspec_plan.yml` ejecuta la etapa “`plan`”.
- `buildspec_apply.yml` ejecuta la etapa “`apply`”.
- `buildspec_destroy.yml` ejecuta la etapa “`destroy`”.

Cree variables del archivo de especificaciones

Cada archivo de especificaciones de compilación utiliza las siguientes variables para activar diferentes ajustes específicos de la compilación:

Variable	Valor predeterminado	Descripción
CODE_SRC_DIR	"."	Define el CodeCommit directorio de origen
TF_VERSION	«1.3.7»	Define la versión de Terraform para el entorno de compilación

El archivo buildspec_validate.ymltambién admite las siguientes variables para activar diferentes ajustes específicos de la compilación:

Variable	Valor predeterminado	Descripción
SCRIPT_DIR	»./templates/scripts»	Define el directorio de scripts
ENVIRONMENT	«dev»	Define el nombre del entorno
SKIPVALIDATIONFAILURE	«Y»	Omite la validación en caso de errores
ENABLE_TFVALIDATE	«Y»	Activa la validación de Terraform
ENABLE_TFFORMAT	«Y»	Activa el formato Terraform
ENABLE_TFCHECKOV	«Y»	Activa el análisis de checkov
ENABLE_TFSEC	«Y»	Activa el análisis de TFSec
TFSEC_VERSION	«v1.28.1»	Define la versión tfsec

Más patrones

- ???
- Asocie un CodeCommit repositorio de AWS en una cuenta de AWS con SageMaker Studio en otra cuenta
- Automatice la adición o actualización de entradas de registro de Windows con AWS Systems Manager
- Automatice la formación y el despliegue de Amazon Lookout for Vision para la detección de anomalías
- Automatizar las copias de seguridad de las instancias de base de datos de Amazon RDS para PostgreSQL mediante AWS Batch
- Automatice la implementación de aplicaciones anidadas mediante SAM de AWS
- Automatice la implementación de Node Termination Handler en Amazon EKS mediante una canalización de CI/CD
- ???
- Automatice la creación de recursos AppStream 2.0 con AWS CloudFormation
- Automatice la replicación de las instancias de Amazon RDS en todas las cuentas de AWS
- Crear e implementar de forma automática una aplicación Java en Amazon EKS mediante una canalización de CI/CD
- Genere automáticamente un modelo de PynamoDB y funciones CRUD para Amazon DynamoDB mediante una aplicación de Python
- Valide e implemente automáticamente las políticas y funciones de IAM en una cuenta de AWS mediante CodePipeline IAM Access Analyzer y macros de AWS CloudFormation
- Realice copias de seguridad de los servidores Sun SPARC en el emulador Stromasys Charon-SSP en la nube de AWS
- Cree una canalización de datos para incorporar, transformar y analizar los datos de Google Analytics con el kit de DataOps desarrollo de AWS
- Creación de un PAC de Micro Focus Enterprise Server con Amazon EC2 Auto Scaling y Systems Manager
- Cree un proceso para imágenes de contenedores reforzadas con Generador de imágenes de EC2 y Terraform
- Cree un flujo de trabajo de MLOps mediante Amazon SageMaker y Azure DevOps

- ???
- Encadene los servicios de AWS mediante un enfoque sin servidor
- Configure el registro para aplicaciones.NET en Amazon CloudWatch Logs mediante nLog
- Implemente de forma continua una aplicación web AWS Amplify moderna desde un repositorio de AWS CodeCommit
- Cree una imagen de contenedor Docker personalizada SageMaker y úsela para el entrenamiento de modelos en AWS Step Functions
- Cree una canalización en las regiones de AWS que no sean compatibles con AWS CodePipeline
- Cree alarmas para métricas personalizadas mediante la detección de CloudWatch anomalías de Amazon
- Implemente una canalización que detecte simultáneamente los problemas de seguridad en varios entregables de código
- Implementar y administrar un lago de datos sin servidor en la nube de AWS mediante el uso de la infraestructura como código
- Implementar recursos y paquetes de Kubernetes con Amazon EKS y un repositorio de gráficos de Helm en Amazon S3
- Implemente aplicaciones de varias pilas mediante AWS CDK con TypeScript
- Implementar la solución Security Automations para AWS WAF mediante Terraform
- Desarrolle asistentes avanzados de IA generativa basados en chat mediante RAG y solicitudes ReAct
- ???
- Genere recomendaciones personalizadas y reclasificadas con Amazon Personalize
- Reciba notificaciones de Amazon SNS cuando cambie el estado de clave de una clave de AWS KMS
- Mejore el rendimiento operativo al habilitar Amazon DevOps Guru en varias regiones, cuentas y unidades organizativas de AWS con la AWS CDK
- Instalación del agente SSM en los nodos de trabajo de Amazon EKS mediante Kubernetes DaemonSet
- Integrar el controlador universal Stonebranch con AWS Mainframe Modernization
- Modernización del mainframe: DevOps en AWS con Micro Focus
- Gestione los conjuntos de permisos del AWS IAM Identity Center como código mediante AWS CodePipeline

- Gestión de las aplicaciones de contenedores en las instalaciones mediante la configuración de Amazon ECS Anywhere con AWS CDK
- Migrar registros DNS de forma masiva a una zona alojada privada de Amazon Route 53
- Migre cargas de trabajo de aprendizaje automático: cree, entrene e implemente a Amazon SageMaker con las herramientas para desarrolladores de AWS
- Supervisar el uso de una imagen de máquina de Amazon compartida en varias cuentas de AWS
- Optimizar imágenes de Docker generadas por AWS App2Container
- Orqueste un proceso de ETL con validación, transformación y particionamiento mediante AWS Step Functions
- Preserve el espacio IP enrutable en los diseños de VPC de varias cuentas para subredes que no son de carga de trabajo
- Aprovisione un producto Terraform en AWS Service Catalog mediante un repositorio de código
- ???
- Rotar las credenciales de la base de datos sin reiniciar los contenedores
- Ejecute las tareas de AWS Systems Manager Automation de forma sincrónica desde AWS Step Functions
- Configure una canalización de CI/CD para cargas de trabajo híbridas en Amazon ECS Anywhere mediante AWS CDK y GitLab
- Configure una infraestructura Multi-AZ para una FCI Always On de SQL Server mediante Amazon FSx
- Configure automáticamente los bots de UiPath RPA en Amazon EC2 mediante AWS CloudFormation
- Incorporación de inquilinos en la arquitectura SaaS para el modelo de silo mediante C# y AWS CDK
- Usa Terraform para habilitar Amazon automáticamente GuardDuty para una organización
- Validar Account Factory para el código Terraform (AFT) localmente
- ???

Informática para usuarios finales

Temas

- Automatice la creación de recursos AppStream 2.0 con AWS CloudFormation
- Más patrones

Automatice la creación de recursos AppStream 2.0 con AWS CloudFormation

Creado por Ram Kandaswamy (AWS) y Dzung Nguyen (AWS)

Entorno: producción	Tecnologías: informática para el usuario final; nativa de la nube; gestión de costes; SaaS DevOps	Carga de trabajo: Microsoft
Servicios de AWS: Amazon AppStream 2.0; AWS CloudFormation		

Resumen

Este patrón proporciona ejemplos de código y pasos para automatizar la creación de recursos de Amazon AppStream 2.0 en la nube de Amazon Web Services (AWS) mediante una CloudFormation plantilla de AWS. El patrón le muestra cómo usar una CloudFormation pila de AWS para automatizar la creación de los recursos de su aplicación AppStream 2.0, incluidos un generador de imágenes, una imagen, una instancia de flota y una pila. Puede transmitir su aplicación AppStream 2.0 a los usuarios finales en un navegador compatible con HTML5 mediante el modo de entrega de aplicaciones o de escritorio.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Aceptación de los términos y condiciones de la AppStream versión 2.0
- Conocimientos básicos de AppStream recursos, como pilas, flotas y creadores de imágenes

Limitaciones

- No puede modificar el rol de AWS Identity and Access Management (IAM) asociado a una instancia AppStream 2.0 después de crearla.

- No puede modificar las propiedades (como la subred o el grupo de seguridad) de la instancia del generador de imágenes AppStream 2.0 una vez creado el generador de imágenes.

Arquitectura

El siguiente diagrama muestra cómo automatizar la creación de recursos AppStream 2.0 mediante una CloudFormation plantilla de AWS.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Puede crear una CloudFormation plantilla de AWS basada en el código YAML en la sección de información adicional de este patrón.
2. La CloudFormation plantilla de AWS crea una pila de CloudFormation pruebas de AWS.
   a. (Opcional) Puede crear una instancia de creación de imágenes mediante la AppStream versión 2.0.
   b. (Opcional) Puede crear una imagen de Windows con su software personalizado.
3. La CloudFormation pila de AWS crea una instancia y una pila de flota AppStream 2.0.
4. Usted implementa sus recursos AppStream 2.0 para los usuarios finales en un navegador compatible con HTML5.

Pila de tecnología

- Amazon AppStream 2.0
- AWS CloudFormation

Herramientas

- Amazon AppStream 2.0: Amazon AppStream 2.0 es un servicio de streaming de aplicaciones totalmente gestionado que le proporciona acceso instantáneo a sus aplicaciones de escritorio desde cualquier lugar. AppStream La versión 2.0 administra los recursos de AWS necesarios para alojar y ejecutar las aplicaciones, se escala automáticamente y proporciona acceso a los usuarios cuando lo soliciten.
- AWS CloudFormation: AWS le CloudFormation ayuda a modelar y configurar sus recursos de AWS, a aprovisionarlos de forma rápida y coherente y a gestionarlos durante todo su ciclo de

vida. Facilita poder usar una plantilla para describir los recursos y sus dependencias, y lanzarlos y configurarlos juntos como una pila, en lugar de administrarlos de forma individual. Puede administrar y aprovisionar pilas en varias cuentas y regiones de AWS.

Epics

(Opcional) Cree una imagen AppStream 2.0

Tarea	Descripción	Habilidades requeridas
Instale un software personalizado y cree una imagen.	1. Instale la aplicación AppStream 2.0 que planea implementar para sus usuarios. 2. Utilice el agente de creación de imágenes Photon o un PowerShell script para crear una nueva imagen de Windows para su software personalizado. Nota: Considere la posibilidad de utilizar la AppLocker función de Windows para bloquear aún más la imagen.	AWS DevOps, arquitecto de nube

Implemente la CloudFormation plantilla de AWS

Tarea	Descripción	Habilidades requeridas
Actualice la CloudFormation plantilla de AWS.	1. Guarde el código en la sección Información adicional de este patrón como un archivo YAML.	Administrador de sistemas de AWS, administrador de la nube, arquitecto de la nube, AWS general, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	2. Actualice el archivo YAML con los valores necesarios para los parámetros de su entorno.	
Cree una CloudFormation pila de AWS con la plantilla.	1. Inicie sesión en la consola de administración de AWS y abra la CloudFormation consola de AWS. 2. En el panel de navegación, seleccione Pilas. 3. Seleccione Crear pila y, a continuación, seleccione Con nuevos recursos (estándar). 4. En Requisito previo: preparar la plantilla, seleccione La plantilla está lista. 5. En la sección Especificar plantilla, seleccione Cargar un archivo de plantilla. 6. Seleccione Elegir archivo y, a continuación, elija la CloudFormation plantilla de AWS actualizada. 7. Complete el resto de los pasos del asistente para crear su pila.	Propietario de la aplicación, administrador de sistemas de AWS, ingeniero de Windows

Recursos relacionados

Referencias

- Comience con Amazon AppStream 2.0: configúrelo con aplicaciones de muestra
- Cree una flota AppStream 2.0 y apílela

Tutoriales y videos

- Flujo de trabajo de usuario de Amazon AppStream 2.0
- Cómo migrar una aplicación antigua de Windows Forms a Amazon AppStream 2.0
- AWS re:Invent 2018: entregue aplicaciones de escritorio de forma segura con Amazon AppStream 2.0 (BAP201)

Información adicional

El siguiente código es un ejemplo de una CloudFormation plantilla de AWS que le permite crear automáticamente recursos AppStream 2.0.

```
AWSTemplateFormatVersion: 2010-09-09
Parameters:
  SubnetIds:
    Type: 'List<AWS::EC2::Subnet::Id>'
  testSecurityGroup:
    Type: 'AWS::EC2::SecurityGroup::Id'
  ImageName:
    Type: String
Resources:

  AppStreamFleet:
    Type: 'AWS::AppStream::Fleet'
    Properties:
      ComputeCapacity:
        DesiredInstances: 5
      InstanceType: stream.standard.medium
      Name: appstream-test-fleet
      DisconnectTimeoutInSeconds: 1200
      FleetType: ON_DEMAND
      IdleDisconnectTimeoutInSeconds: 1200
      ImageName: !Ref ImageName
      MaxUserDurationInSeconds: 345600
      VpcConfig:
        SecurityGroupIds:
          - !Ref testSecurityGroup
```

```
      SubnetIds: !Ref SubnetIds
  AppStreamStack:
    Type: 'AWS::AppStream::Stack'
    Properties:
      Description: AppStream stack for test
      DisplayName: AppStream test Stack
      Name: appstream-test-stack
      StorageConnectors:
        - ConnectorType: HOMEFOLDERS
      UserSettings:
        - Action: CLIPBOARD_COPY_FROM_LOCAL_DEVICE
          Permission: ENABLED
        - Action: CLIPBOARD_COPY_TO_LOCAL_DEVICE
          Permission: ENABLED
        - Action: FILE_DOWNLOAD
          Permission: ENABLED
        - Action: PRINTING_TO_LOCAL_DEVICE
          Permission: ENABLED
  AppStreamFleetAssociation:
    Type: 'AWS::AppStream::StackFleetAssociation'
    Properties:
      FleetName: appstream-test-fleet
      StackName: appstream-test-stack
    DependsOn:
      - AppStreamFleet
      - AppStreamStack
```

Más patrones

- Conectarse a una instancia de Amazon EC2 mediante el uso de Session Manager
- Mejorar la calidad de las llamadas en las estaciones de trabajo de los agentes en los centros de contacto de Amazon Connect
- Ejecute las tareas de AWS Systems Manager Automation de forma sincrónica desde AWS Step Functions

Computación de alto rendimiento

Temas

Configurar un panel de monitoreo de Grafana para AWS ParallelCluster

Creado por Dario La Porta (AWS) y William Lu (AWS)

Repositorio de código: parallelcluster-monitoring-dashboard	Entorno: PoC o piloto	Tecnologías: computación de alto rendimiento; análisis; gestión y gobierno
Carga de trabajo: código abierto	Servicios de AWS: AWS ParallelCluster	

Resumen

AWS le ParallelCluster ayuda a implementar y administrar clústeres de computación de alto rendimiento (HPC). Es compatible con los programadores de trabajos de código abierto AWS Batch y Slurm. Aunque AWS ParallelCluster está integrado con Amazon CloudWatch para el registro y las métricas, no proporciona un panel de supervisión de la carga de trabajo.

El panel de control de Grafana para AWS ParallelCluster (GitHub) es un panel de supervisión para AWS. ParallelCluster Proporciona información sobre el programador de tareas y métricas de supervisión detalladas a nivel del sistema operativo (SO). Para obtener más información sobre los paneles incluidos en esta solución, consulte Ejemplos de paneles en el repositorio. GitHub Estas métricas le ayudan a comprender mejor la carga de trabajo de HPC y su rendimiento. Sin embargo, el código del panel de control no se actualiza para las versiones más recientes de AWS ParallelCluster ni para los paquetes de código abierto que se utilizan en la solución. Este patrón mejora la solución para proporcionar los siguientes beneficios:

- Compatible con AWS ParallelCluster v3
- Usa la última versión de los paquetes de código abierto, incluidos Prometheus, Grafana, Prometheus Slurm Exporter y NVIDIA DCGM-Exporter
- Aumenta el número de núcleos de CPU y GPU que usan los trabajos de Slurm
- Añade un panel de supervisión de trabajos
- Mejora el panel de supervisión de nodos de GPU para nodos con 4 u 8 unidades de procesamiento gráfico (GPU)

Esta versión de la solución mejorada se ha implementado y verificado en el entorno de producción de HPC de un cliente de AWS.

Requisitos previos y limitaciones

Requisitos previos

- AWS ParallelCluster CLI, instalada y configurada.
- Una configuración de red compatible con AWS ParallelCluster. Este patrón usa la configuración de AWS ParallelCluster con dos subredes, que requiere una subred pública, una subred privada, una puerta de enlace a Internet y una puerta de enlace NAT.
- Todos los nodos ParallelCluster del clúster de AWS deben tener acceso a Internet. Esto es necesario para que los scripts de instalación puedan descargar el software de código abierto y las imágenes de Docker.
- Un par de claves en Amazon Elastic Compute Cloud (Amazon EC2). Los recursos con este par de claves tienen acceso Secure Shell (SSH) al nodo principal.

Limitaciones

- Este patrón está diseñado para Ubuntu 20.04 LTS. Si usa una versión diferente de Ubuntu, o si usa Amazon Linux o CentOS, tendrá que modificar los scripts que se proporcionan con esta solución. Dichas modificaciones no se incluyen en este patrón.

Versiones de producto

- Ubuntu 20.04 LTS
- ParallelCluster 3.X

Consideraciones de costos y facturación

- La solución implementada en este patrón no está cubierta por el nivel gratuito. Se aplican cargos a Amazon EC2, Amazon FSx para Lustre, la puerta de enlace NAT de Amazon VPC y Amazon Route 53.

Arquitectura

Arquitectura de destino

En el siguiente diagrama, se muestra cómo un usuario puede acceder al panel de supervisión de AWS ParallelCluster en el nodo principal. El nodo principal ejecuta NICE DCV, Prometheus, Grafana, Prometheus Slurm Exporter, Prometheus Node Exporter y NGINX Open Source. Los nodos de cómputo ejecutan Prometheus Node Exporter y, si el nodo contiene GPU, también ejecutan NVIDIA DCGM-Exporter. El nodo principal recupera información de los nodos de cómputo y muestra esos datos en el panel de control de Grafana.

En la mayoría de los casos, el nodo principal no está muy cargado, ya que el programador de tareas no requiere una cantidad significativa de CPU o memoria. Los usuarios acceden al panel de control del nodo principal mediante SSL en el puerto 443.

Todos los usuarios con acceso de lectura autorizado pueden ver los paneles de supervisión de forma anónima. Solo el administrador de Grafana puede modificar los paneles. Debe configurar una contraseña para el administrador de Grafana en el archivo `aws-parallelcluster-monitoring/docker-compose/docker-compose.head.yml`.

Herramientas

Servicios de AWS

- NICE DCV es un protocolo de visualización remota de alto rendimiento que le permite ofrecer escritorios remotos y streaming de aplicaciones desde cualquier nube o centro de datos a cualquier dispositivo, en condiciones de red variables.
- AWS le ParallelCluster ayuda a implementar y administrar clústeres de computación de alto rendimiento (HPC). Es compatible con los programadores de trabajos de código abierto AWS Batch y Slurm.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido.

Otras herramientas

- Docker es un conjunto de productos de plataforma como servicio (PaaS) que utiliza la virtualización a nivel del sistema operativo para entregar software en contenedores.
- Grafana es un software de código abierto que le permite consultar, visualizar, alertar y explorar métricas, registros y trazas.
- NGINX Open Source es un servidor web de código abierto y proxy inverso.
- NVIDIA Data Center GPU Manager (DCGM) es un conjunto de herramientas para administrar y supervisar las unidades de procesamiento gráfico (GPU) de los centros de datos de NVIDIA en entornos de clúster. Este patrón usa DCGM-Exporter, que le ayuda a exportar las métricas de GPU de Prometheus.
- Prometheus es un conjunto de herramientas de supervisión de sistemas de código abierto que recopila y almacena sus métricas como datos de serie temporal con pares clave-valor asociados, denominados etiquetas. Este patrón también usa Prometheus Slurm Exporter para recopilar y exportar métricas, y Prometheus Node Exporter para exportar métricas de los nodos de cómputo.
- Ubuntu es un sistema operativo de código abierto basado en Linux y diseñado para servidores empresariales, escritorios, entornos de nube e IoT.

Repositorio de código

El código de este patrón está disponible en el GitHub pcluster-monitoring-dashboardrepositorio.

Epics

Cree los recursos necesarios

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3.	Crear un bucket de Amazon S3. Este bucket se usa para almacenar los scripts de configuración. Para obtener instrucciones, consulte Crear un bucket en la documenta ción de Amazon S3.	AWS general
Clonar el repositorio.	Clona el GitHub pcluster-monitoring-dashboardrepositor	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	io ejecutando el siguiente comando. `git clone https://github.com/aws-samples/parallelcluster-monitoring-dashboard.git`	
Cree una contraseña de administrador.	1. Seleccione la carpeta `aws-parallelcluster-monitoring` , seleccione la carpeta `docker-compose` y abra el archivo docker-compose.head.yml. 2. En la variable `GF_SECURITY_ADMIN_PASSWORD` , sustituya `Grafana4PC!` por una contraseña de su elección. Esta es la contraseña administrativa que usará para gestionar la cuenta de Grafana. 3. Guarde y cierre el archivo docker-compose.head.yml.	Scripts Linux Shell
Copie los archivos necesarios en el bucket de S3.	Copie el script post_install.sh y la aws-parallelcluster-monitoringcarpeta en el depósito de S3 que creó. Para más instrucciones, consulte Cargar objetos en la documentación de Amazon S3.	AWS general

Tarea	Descripción	Habilidades requeridas
Configure un grupo de seguridad adicional para el nodo principal.	1. Cree un grupo de seguridad para el nodo principal. Este grupo de seguridad permitirá que el tráfico entrante llegue a los paneles de supervisión del nodo principal. Para más instrucciones, consulte Crear un grupo de seguridad en la documentación de Amazon VPC. 2. Agregar una regla de entrada al grupo de seguridad Para obtener más instrucciones, consulte Cómo añadir reglas a un grupo de seguridad en la documentación de Amazon VPC. Utilice los siguientes parámetros para la regla: • Tipo: HTTPS • Protocolo: TCP • Intervalo de puertos: 443 • Origen: introduzca su dirección IP • Descripción: permitir a los usuarios acceder al panel de supervisión	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Configure una política de IAM para el nodo principal.	Cree una política basada en identidades para el nodo principal. Esta política permite al nodo recuperar datos métricos de Amazon CloudWatch. El GitHub repositorio contiene un ejemplo de política. Para obtener más instrucciones, consulte Creación de políticas de IAM en la documentación de AWS Identity and Access Management (IAM).	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Configure una política de IAM para los nodos de cómputo.	Cree una política basada en identidades para los nodos de computación. Esta política permite al nodo crear las etiquetas que contienen la ID y el propietario del trabajo. El GitHub repositorio contiene un ejemplo de política. Para obtener más información, consulte Creación de políticas de IAM en la documentación de IAM. Si usa el archivo de ejemplo proporcionado, sustituya los siguientes valores: • <REGION>: la región de AWS donde se aloja el clúster. • <ACCOUNT_ID>: ID de la cuenta de AWS.	Administrador de AWS

Cree el clúster

Tarea	Descripción	Habilidades requeridas
Modifique el archivo de plantilla de clúster proporcio nado.	Cree el ParallelCluster clúster de AWS. Utilice el archivo de plantilla de CloudFormation AWS cluster.yaml proporcio nado como punto de partida para crear el clúster. Sustituya	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	los siguientes valores en la plantilla proporcionada: • <REGION>: la región de AWS donde se aloja el clúster. • <HEADNODE_SUBNET> – La subred pública de la VPC. • <ADDITIONAL_HEAD_NODE_SG> – El nombre del grupo de seguridad que ha creado para el nodo principal. • <KEY_NAME> – Introduzca el nombre de un par de claves de Amazon EC2 existente. Los recursos con este par de claves tienen acceso Secure Shell (SSH) al nodo principal. • <ALLOWED_IPS> –– Introduzca el rango de direcciones IP con formato CIDR que puede realizar conexiones SSH en el nodo principal. • <ADDITIONAL_HEAD_NODE_POLICY> – Introduzca el nombre de la política de IAM que ha creado para el nodo principal.	

Tarea	Descripción	Habilidades requeridas
	• <BUCKET_NAME>: escriba el nombre del bucket de S3·que creó. • <COMPUTE_SUBNET> – Introduzca el nombre de la subred privada en la VPC. • <ADDITIONAL_HEAD_NODE_POLICY> – Introduzca el nombre de la política de IAM que ha creado para el nodo de computación.	
Cree el clúster.	En la AWS ParallelCluster CLI, introduzca el siguiente comando. Esto despliega la CloudFormation plantilla y crea el clúster. Para obtener más información sobre este comando, consulte pcluster create-cluster en la documentación de AWS. ParallelCluster `pcluster create-cluster -n <cluster_name> -c cluster.yaml`	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Supervise la creación del clúster.	Introduzca el siguiente comando para supervisar la creación del cluster. Para obtener más información sobre este comando, consulte pcluster describe-cluster en la documentación de AWS. ParallelCluster `pcluster describe-cluster -n <cluster_name>`	Administrador de AWS

Use los paneles de Grafana

Tarea	Descripción	Habilidades requeridas
Acceda al portal de Grafana.	1. Introduzca el siguiente comando para obtener la dirección IP pública del nodo principal. `pcluster describe-cluster -n <cluster_name> --query headNode.publicIpAddress` 2. En un navegador web, acceda a la siguiente URL para entrar en el panel de control de Grafana. https://<head_node_public_ip_address>	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	3. En la página de inicio de Grafana, elija el icono de cuatro cuadrados Panel de control, en el menú de la izquierda, y seleccione General. Se mostrará una lista de paneles configura dos. Grafana ofrece los siguientes paneles: • Costo del clúster: contiene información sobre el costo del clúster • Registros del clúster: contiene información sobre los registros del clúster • Detalles del nodo de cómputo: contiene información sobre las estadísticas de uso de los nodos de cómputo • Lista de nodos de cómputo: contiene una lista de los nodos de cómputo del clúster • Nodos de GPU: contiene información sobre las estadísticas de uso de los nodos de GPU • Detalles de los trabajos: contiene información sobre la utilización de los recursos del trabajo	

Tarea	Descripción	Habilidades requeridas
	• Detalles del nodo principal: contiene información sobre las estadísticas de uso del nodo principal • ParallelCluster Resumen: contiene información sobre el uso del clúster	

Limpie la solución para dejar de incurrir en costos asociados

Tarea	Descripción	Habilidades requeridas
Eliminar el clúster.	Para eliminar el clúster, escriba siguiente comando. Para obtener más información sobre este comando, consulte pcluster delete-cluster en la documentación de AWS. ParallelCluster `pcluster delete-cluster -n <cluster_name>`	Administrador de AWS
Elimine las políticas de IAM.	Elimine las políticas que creó para el nodo principal y el nodo de cómputo. Para más información acerca de la eliminación de políticas , consulte Eliminación de políticas de IAM en la documentación de IAM.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Eliminar la regla y el grupo de seguridad.	Elimine el grupo de seguridad que creó para el nodo principal. Para obtener más información, consulte Eliminar reglas de grupo de seguridad y Eliminar un grupo de seguridad en la documentación de Amazon VPC.	Administrador de AWS
Elimine el bucket de S3.	Elimine el bucket de S3 que creó para almacenar los scripts de configuración. Para obtener más información, consulte Eliminación de un bucket en la documentación de Amazon S3.	AWS general

Solución de problemas

Problema	Solución
No se puede acceder al nodo principal en el navegador.	Compruebe el grupo de seguridad y confirme que el puerto de entrada 443 esté abierto.
Grafana no se abre.	En el nodo principal, busque `docker logs Grafana` en el registro del contenedor.
Algunas métricas no tienen datos.	En el nodo principal, compruebe los registros de todos los contenedores.

Recursos relacionados

Documentación de AWS

- Políticas de IAM para Amazon EC2

Otros recursos de AWS

- AWS ParallelCluster
- Panel de monitoreo para AWS ParallelCluster (entrada del blog de AWS)

Otros recursos

- Sistema de monitorización Prometheus
- Grafana

Configure una infraestructura de escritorio virtual (VDI) con escalado automático mediante NICE EnginFrame y el administrador de sesiones NICE DCV

Creado por Dario La Porta y Salvatore Maccarone (AWS)

Repositorio de código: elastic-vdi-infrastructure	Entorno: PoC o piloto	Tecnologías: computación de alto rendimiento; infraestructura
Servicios de AWS: AWS CDK; AWS CloudFormation; Amazon EC2 Auto Scaling; Elastic Load Balancing (ELB)		

Resumen

NICE DCV es un protocolo de visualización remota de alto rendimiento que le ayuda a transmitir escritorios remotos y aplicaciones desde cualquier nube o centro de datos a cualquier dispositivo, en condiciones de red variables. Con NICE DCV y Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2), puede ejecutar aplicaciones con uso intensivo de gráficos de forma remota en instancias EC2 y transmitir sus interfaces de usuario a equipos cliente remotos y más sencillos. Esto elimina la necesidad de costosas estaciones de trabajo dedicadas y la necesidad de transferir grandes cantidades de datos entre la nube y las equipos cliente.

Este patrón establece una infraestructura de escritorio virtual (VDI) para Linux y Windows completamente funcional y con escalado automático, a la que se pueda acceder a través de una interfaz de usuario basada en la web. La solución VDI proporciona a los usuarios de investigación y desarrollo (I+D) una interfaz de usuario accesible y eficaz para enviar solicitudes de análisis con uso intensivo de gráficos y revisar los resultados de forma remota.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.

- Permisos de administrador y un conjunto de claves de acceso.
- Kit de herramientas AWS Cloud Development Kit (AWS CDK), instalado y configurado. Para obtener más información, consulte Instalación de AWS CDK.
- Interfaz de la línea de comandos de AWS (AWS CLI), instalada y configurada para su cuenta AWS. Para obtener más información, consulte Installing or updating the latest version of the AWS CLI.
- Python, instalado y configurado. Para obtener más información, consulte Versiones de origen (sitio web de Python).
- Una o varias nubes privadas virtuales (VPC) disponibles.
- Dos o varias direcciones IP elásticas disponibles. Para obtener más información sobre el límite predeterminado, consulte límite de direcciones IP elásticas.
- Para las instancias EC2 de Linux, configure un par de claves Secure Shell (SSH). Para obtener más información, consulte Pares de claves e instancias Linux.

Versiones de producto

- CDK de AWS, versión 2.26.0 o posterior
- Python, versión 3.8 o posterior

Arquitectura

Arquitectura de destino

En el siguiente gráfico se muestran los diferentes componentes de esta solución VDI. El usuario interactúa con NICE EnginFrame para lanzar instancias de Amazon EC2 según los grupos de Auto Scaling de Amazon EC2 para instancias NICE DCV de Windows y Linux.

Automatizar y escalar

El código incluido en este patrón crea una VPC personalizada, subredes públicas y privadas, una puerta de enlace de Internet, una puerta de enlace NAT, un Equilibrador de carga de aplicación, grupos de seguridad y políticas de IAM. AWS también CloudFormation se utiliza para crear la flota de servidores NICE DCV para Linux y Windows.

Herramientas

Servicios de AWS

- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura de la nube de AWS en código.
- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- NICE DCV es un protocolo de visualización remota de alto rendimiento que le permite ofrecer escritorios remotos y streaming de aplicaciones desde cualquier nube o centro de datos a cualquier dispositivo, en condiciones de red variables. En este patrón, se proporciona una experiencia de uso eficiente del ancho de banda que permite transmitir gráficos 3D de computación de alto rendimiento (HPC) de forma remota.
- NICE DCV Session Manager le ayuda a crear y gestionar el ciclo de vida de las sesiones NICE DCV en una flota de servidores NICE DCV.
- NICE EnginFrame es una interfaz web frontend avanzada que permite acceder a aplicaciones técnicas y científicas en la nube.

Repositorio de código

El código de este patrón está disponible en la solución VDI de escalado automático con los repositorios NICE EnginFrame y NICE DCV Session Manager.

Epics

Implemente la infraestructura de escritorios virtuales

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Clone el repositorio que contiene el código. `git clone https://github.com/aws-samples/elastic-vdi-infrastructure.git`	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Instale las bibliotecas de AWS CDK requeridas.	Instale las bibliotecas de AWS CDK. `cd elastic-vdi-infrastructure` `python3 -m venv .venv` `source .venv/bin/activate` `pip3 install -r requirements.txt`	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Actualice los parámetros.	1. Abra el archivo app.py con el editor de texto que prefiera. 2. Reemplace el valor `CHANGE_ME` para los siguientes parámetros requeridos: • `region`: la región de AWS de destino. Para obtener una lista completa, consulte Regiones de AWS. • `account`: el ID de la cuenta AWS de destino. Para obtener más información, consulte Buscar el ID de cuenta de AWS. • `key_name`: el par de claves utilizado para acceder a las instancias EC2 de Linux. 3. (Opcional) Modifique los valores de los siguientes parámetros con el fin de personalizar la solución para su entorno: • `ec2_type_enginframe` — El tipo de instancia EnginFrame • `ec2_type_broker` : el tipo de instancia de Session Manager Broker	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	• `ebs_enginframe_size` — El tamaño del volumen de Amazon Elastic Block Store (Amazon EBS) de la instancia EnginFrame • `ebs_broker_size` : el tamaño del volumen de EBS para la instancia de Session Manager Broker • `TagName and TagValue`: ea etiqueta de facturación de los recursos • `efadmin_uid` — El identificador único del usuario EnginFrame administrador (efadmin) • `linux_shared_storage_size` : el tamaño de OpenZFS en gibibytes (GiB) • `Shared_Storage_Linux` : el punto de montaje del almacenamiento compartido • `Enginframe_installer` — El enlace de descarga de EnginFrame • `Session_Manager_Broker_Installer` : el enlace de descarga del Session Manager Broker	

Tarea	Descripción	Habilidades requeridas
	4. Guarde y cierre el archivo app.py.	
Implemente la solución.	Ejecute los comandos siguientes secuencialmente. `cdk bootstrap` `cdk deploy Assets-Stack Parameters-Stack` `cdk deploy Elastic-Vdi-Infrastructure` Una vez completada la implementación, se devuelven los dos resultados siguientes: • `Elastic-Vdi-Infrastructure.EnginFrameURL` — La dirección HTTPS del EnginFrame portal • `Elastic-Vdi-InfrastruSecretEFadminPassword` : el nombre de recurso de Amazon (ARN) del secreto que contiene la contraseña del usuario efadmin Anote el valor de estos valores. Los usará más adelante en este patrón.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Implemente la flota de servidores de Linux.	1. Inicie sesión en la consola de administración de AWS y abra la consola de CloudFormation . 2. Seleccione Create stack (Crear pila) y, a continuación, seleccione With new resources (Con nuevos recursos). 3. En la carpeta cloudformation_files, selecciona el archivo.yaml. dcv-linux-fleet 4. En la página Specify stack details (Especificar detalles de la pila), ingrese los siguientes parámetros: • Nombre de pila: el nombre de la pila. • DcvFleet— El nombre de la flota de NICE DCV. No deje este valor en blanco ni utilice espacios. • InstanceType— El tipo de instancia de la flota. • RootVolumeSize— El tamaño del volumen raíz de la instancia EC2 de Linux. • MinSize— El número mínimo de nodos que deberían estar disponibles y que no deberían ejecutar ninguna sesión	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	de DCV. Por ejemplo, si introduce 2, la solución comienza con 2 nodos. Cuando un usuario crea una sesión, el número de nodos disponibles se reduce a 1 y la solución crea otro nodo para mantener el mínimo. • MaxSize— El número máximo de nodos de la flota. Los usuarios no pueden iniciar nuevas sesiones si se ha alcanzado el máximo. • BillingTagName— El nombre de la etiqueta utilizada para la facturación. El nombre de esta etiqueta debe ser diferente del que se usa para la pila de Windows. • BillingTagValue— El valor de la etiqueta utilizado para la facturación. 5. Complete el asistente de creación de pilas y, a continuación, seleccione Submit (Enviar) para empezar a crear la pila.	

Tarea	Descripción	Habilidades requeridas
Implemente la flota de servidores de Windows.	1. Inicie sesión en la consola de administración de AWS y abra la consola de CloudFormation . 2. Seleccione Create stack (Crear pila) y, a continuación, seleccione With new resources (Con nuevos recursos). 3. En la carpeta cloudformation_files, selecciona el archivo.yaml. dcv-windows-fleet 4. En la página Specify stack details (Especificar detalles de la pila), ingrese los siguientes parámetros: • Nombre de pila: el nombre de la pila. • DcvFleet— El nombre de la flota de NICE DCV. No deje este valor en blanco ni utilice espacios. • InstanceType— El tipo de instancia de la flota. • RootVolumeSize— El tamaño del volumen raíz de la instancia EC2 de Windows. • MinSize— El número mínimo de nodos que deberían estar disponibles y que no deberían	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	estar ejecutando ninguna sesión de DCV. • MaxSize— El número máximo de nodos de la flota. • BillingTagName— El nombre de la etiqueta utilizada para la facturación. El nombre de esta etiqueta debe ser diferente del que se usa para la pila de Linux. • BillingTagValue— El valor de la etiqueta utilizado para la facturación. 5. Complete el asistente de creación de pilas y, a continuación, seleccione Submit (Enviar) para empezar a crear la pila.	

Acceda al entorno imlementado

Tarea	Descripción	Habilidades requeridas
Recupera la contraseña de EnginFrame administrador.	La cuenta de EnginFrame administración se denomina efadmin y la contraseña se guarda en AWS Secrets Manager como un secreto. El ARN del secreto se genera de forma dinámica y está	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	visible en el resultado de la implementación de AWS CDK. 1. En la épica anterior, en Implementar la historia de la solución, debajo del resultado `Elastic-Vdi-Infrastructure.SecretEFadminPassword` , busque el ARN del secreto generado. 2. Realice una de las siguientes acciones para recuperar el secreto: • Use la consola de Secrets Manager. Para obtener más información, consulte Recuperar secretos. • Escriba el comando get-secret-value . `aws secretsmanager get-secret-value \ --secret-id <secret_arn> \ --query SecretString \ --output text`	

Tarea	Descripción	Habilidades requeridas
Acceda al EnginFrame portal.	1. En la epopeya anterior, en la historia sobre cómo implementar la solución, debajo del `Elastic-Vdi-Infrastructure.EnginFrameURL` resultado, busca la dirección HTTPS del EnginFrame portal. 2. En un navegador web, escriba la dirección HTTPS del portal. 3. Introduzca las credenciales del usuario efadmin.	Arquitecto de la nube
Inicie una sesión de Windows.	1. En el EnginFrame portal, en el menú, elija Windows Desktop. 2. Cuando se le pida que inicie sesión como administrador de Windows, introduzca la misma contraseña utilizada para el usuario efadmin. 3. Confirme que la sesión de Windows se ha iniciado correctamente.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Inicie una sesión de Linux.	1. En el EnginFrame portal, en el menú, elija Linux Desktop. 2. Cuando se le pida que inicie sesión, introduzca las credenciales del usuario efadmin. 3. Confirme que la sesión de Linux se ha iniciado correctamente.	Arquitecto de la nube

Limpieza

Tarea	Descripción	Habilidades requeridas
Elimine las pilas.	En la CloudFormation consola de AWS, elimine las pilas de las flotas de servidores de Windows y Linux. Para obtener más información, consulte Eliminación de pilas.	Arquitecto de la nube
Configurar la infraestructura.	Elimine la infraestructura implementada mediante el siguiente comando de AWS CDK. `cdk destroy --all`	Arquitecto de la nube

Solución de problemas

Problema	Solución
La implementación no se completó porque se interrumpió.	Siga las instrucciones de la épica sobre la Limpieza y, a continuación, repita este patrón para volver a implementar el entorno.

Recursos relacionados

- NICE DCV
- BONITO EnginFrame

Nube híbrida

Temas

- Configure una extensión de centro de datos para VMware Cloud en AWS mediante el modo Hybrid Linked Mode
- Configurar VMware vRealize Automation para aprovisionar máquinas virtuales en VMware Cloud en AWS
- Implemente un SDDC de VMware en AWS mediante VMware Cloud en AWS
- Integre VMware vRealize Network Insight con VMware Cloud on AWS
- Migración de las máquinas virtuales a VMware Cloud en AWS mediante la migración asistida por HCX OS
- Envíe registros desde VMware Cloud on AWS a Splunk mediante VMware Aria Operations for Logs
- Configure una canalización de CI/CD para cargas de trabajo híbridas en Amazon ECS Anywhere mediante AWS CDK y GitLab
- Más patrones

Configure una extensión de centro de datos para VMware Cloud en AWS mediante el modo Hybrid Linked Mode

Creado por Deepak Kumar (AWS)

Entorno: producción	Tecnologías: Nube híbrida; Infraestructura; Migración	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: AWS Direct Connect		

Resumen

Aviso: A partir del 30 de abril de 2024, VMware Cloud on AWS ya no será revendido por AWS sus socios de canal. El servicio seguirá estando disponible a través de Broadcom. Le recomendamos que se ponga en contacto con su AWS representante para obtener más información.

Este patrón describe cómo puede utilizar el Hybrid Linked Mode para ver y gestionar los inventarios en un centro de datos en las instalaciones y en un centro de datos definido por software (SDDC) de VMware Cloud en AWS mediante una única interfaz de cliente de VMware vSphere.

Al configurar Hybrid Linked Mode, puede migrar sus máquinas virtuales (VM) y aplicaciones en las instalaciones al SDDC en la nube. De este modo, sus equipos de TI pueden administrar sus recursos basados en la nube con las conocidas herramientas de VMware y sin necesidad de herramientas nuevas. También puede garantizar operaciones coherentes y una administración simplificada mediante el uso del VMware Cloud Gateway Appliance.

Este patrón ofrece dos opciones para configurar el modo Hybrid Linked Mode, pero solo puede usar una opción a la vez. La primera opción instala el dispositivo Cloud Gateway y lo usa para conectarse desde el vCenter Server en las instalaciones al SDDC en la nube. La segunda opción configura el modo Hybrid Linked Mode desde el SDDC en la nube.

Requisitos previos y limitaciones

Requisitos previos (ambas opciones)

- Un centro de datos en las instalaciones y un SDDC en nube.
- Una conexión existente entre el centro de datos en las instalaciones y el SDDC en la nube, mediante AWS Direct Connect, una VPN o ambas.
- El centro de datos en las instalaciones y el SDDC en la nube están sincronizados con el protocolo de tiempo de red (NTP) u otra fuente horaria autorizada.
- La latencia máxima de un tiempo de ida y vuelta entre el centro de datos en las instalaciones y el SDDC en la nube no supera los 100 ms.
- Administradores de nube con acceso a su entorno en las instalaciones.
- El nombre de dominio (FQDN) de vCenter Server debe resolverse en una dirección IP privada.

Requisitos previos para la opción 1

- El entorno en las instalaciones debe ejecutarse en vSphere 6.5.0d o una versión posterior.
- El dispositivo Cloud Gateway y vCenter Server se pueden comunicar a través de AWS Direct Connect, una VPN o ambas.
- El dispositivo Cloud Gateway cumple con los requisitos de hardware.
- Los puertos del firewall están abiertos.

Requisitos previos para la opción 2

- El vCenter Server en las instalaciones se ejecuta en vSphere 6.0 Update 3 o posterior, o en vSphere 6.5.0d o posterior.
- Las credenciales de inicio de sesión están disponibles para el dominio de inicio de sesión único (SSO) de vSphere (SSO) en las instalaciones.
- Los usuarios del entorno en las instalaciones tienen acceso de solo lectura al nombre distintivo base (DN base).
- El servidor del Sistema de nombres de dominio (DNS) en las instalaciones está configurado para VMware Management Gateway.
- Implemente pruebas de conectividad de red mediante el validador de conectividad de VMware.
- Los puertos del firewall están abiertos.

Limitaciones

- El modo Hybrid Linked Mode solo puede conectar un dominio de vCenter Sever Enhanced Linked Mode en las instalaciones.
- El modo Hybrid Linked Mode solo es compatible con vCenter Server en las instalaciones que ejecute la versión 6.7 o posterior.

Arquitectura

En el siguiente diagrama, se muestran ambas opciones para configurar el modo Hybrid Linked Mode.

Migración de diferentes tipos de carga de trabajo mediante el modo Hybrid Linked Mode

El modo Hybrid Linked Mode admite la migración de cargas de trabajo entre un centro de datos en las instalaciones y un SDDC en la nube mediante una migración en frío o una migración en vivo con VMware vSphere vMotion. Los factores que se deben tener en cuenta al elegir el método de migración incluyen el tipo y la versión del conmutador virtual, el tipo de conexión al SDDC en la nube y la versión del hardware virtual.

Una migración en frío es adecuada para las máquinas virtuales que sufren tiempos de inactividad. Puede apagar las máquinas virtuales, migrarlas y, a continuación, volver a encenderlas. El tiempo de migración es más rápido porque no es necesario copiar la memoria activa. Recomendamos utilizar una migración en frío para las aplicaciones que aceptan tiempos de inactividad (por ejemplo, las aplicaciones de nivel 3 o las cargas de trabajo de desarrollo y prueba). Si sus máquinas virtuales no pueden sufrir tiempos de inactividad, debería considerar la posibilidad de realizar una migración en vivo con VMotion para sus aplicaciones de misión crítica.

En el diagrama siguiente se proporciona información general sobre los diferentes tipos de migración de carga de trabajo mediante el modo Hybrid Linked Mode.

Herramientas

- VMware Cloud en AWS es una oferta de nube integrada desarrollada conjuntamente por AWS y VMware.
- VMware Cloud Gateway Appliance permite varios casos de uso de la nube híbrida en los que los recursos locales están conectados a los recursos de la nube.

- VMware vSphere es la plataforma de virtualización de VMware, que transforma los centros de datos en infraestructuras informáticas agregadas que incluyen recursos de CPU, almacenamiento y redes.

Epics

Opción 1: utilice el modo Hybrid Linked Mode con el dispositivo Cloud Gateway

Tarea	Descripción	Habilidades requeridas
Configure el dispositivo Cloud Gateway.	1. Inicie sesión en la consola de VMware Cloud en AWS y descargue Cloud Gateway Appliance. 2. Instale el dispositivo Cloud Gateway en su entorno en las instalaciones siguiendo estos dos pasos: • Seleccione Empezar a configurar y, a continuación, implementar el dispositivo Cloud Gateway. • Configure el modo Hybrid Linked Mode. Para obtener más información y pasos detallados, consulte Configuración del modo Hybrid Linked Mode mediante vCenter Cloud Gateway Appliance en la documentación de VMware.	Administrador de la nube

Opción 2: utilizar el modo Hybrid Linked Mode desde el SDDC en la nube

Tarea	Descripción	Habilidades requeridas
Configure el modo Hybrid Linked Mode desde el SDDC en la nube.	1. Inicie sesión en la consola de VMware Cloud en AWS y utilice el validador de conectividad para comprobar todas las conexiones de red necesarias. Para obtener más información al respecto, consulte Validar la conectividad de red para el modo Hybrid Linked Mode en la documentación de VMware. 2. Inicie sesión en vSphere Client del SDDC en la nube, elija Menú, Administración y, a continuación, Dominios. 3. En la sección Nube híbrida, elija Dominios enlazados y, a continuación, conéctese a su vCenter Server en las instalaciones. 4. Agregue una fuente de identidad al dominio del Protocolo ligero de acceso a directorios (LDAP) del SDDC en la nube. Para obtener más información al respecto, consulte Agregar una fuente de identidad al dominio LDAP del SDDC	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	en la documentación de VMware.	

Recursos relacionados

- Configuración del modo Hybrid Linked Mode
- Configuración del modo Hybrid Linked Mode para VMware Cloud en AWS

Configurar VMware vRealize Automation para aprovisionar máquinas virtuales en VMware Cloud en AWS

Creado por Deepak Kumar (AWS)

Entorno: producción	Tecnologías: nube híbrida; infraestructura	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS AWS Direct Connect; AWS Site-to-Site VPN		

Resumen

Aviso: A partir del 30 de abril de 2024, VMware Cloud on AWS ya no será revendido por AWS sus socios de canal. El servicio seguirá estando disponible a través de Broadcom. Le recomendamos que se ponga en contacto con su AWS representante para obtener más información.

VMware vRealize Automation es un software de automatización que puede utilizar para solicitar y administrar recursos de TI. Si decide configurar vRealize Automation con VMware Cloud en AWS, puede automatizar la entrega de máquinas virtuales (VM), aplicaciones y servicios de TI en varios centros de datos y entornos de nube.

A continuación, sus equipos de TI pueden crear elementos de catálogo para configurar el aprovisionamiento de servicios y las capacidades operativas que los usuarios pueden solicitar y utilizar con sus herramientas de vRealize Automation existentes. También puede mejorar la agilidad y la eficiencia de su TI integrando VMware Cloud en AWS con vRealize Automation Cloud Assembly.

Este patrón describe cómo configurar VMware vRealize Automation para crear automáticamente capacidades de aplicaciones o máquinas virtuales en VMware Cloud en AWS.

Requisitos previos y limitaciones

Requisitos previos

- Un centro de datos local existente y un centro de datos definido por software (SDDC) de VMware Cloud en AWS. Para obtener más información sobre el SDCC en la nube, consulte Acerca de los centros de datos definidos por software en la documentación de VMware.
- Una conexión existente entre el centro de datos local y el SDDC en la nube, mediante AWS Direct Connect, una VPN (basada en rutas o políticas) o ambas.
- El centro de datos en las instalaciones y el SDDC en la nube están sincronizados con el protocolo de tiempo de red (NTP) u otra fuente horaria autorizada.
- La latencia máxima de un tiempo de ida y vuelta entre el centro de datos en las instalaciones y el SDDC en la nube no supera los 100 ms.
- El nombre de dominio (FQDN) de vCenter Server debe resolverse en una dirección IP privada.
- Usuarios del SDDC en la nube con acceso a su entorno local.
- Acceso de propietario de la organización en la función de servicio Cloud Assembly de vRealize Automation.
- Usuarios finales con permiso en vRealize Automation Service Broker para consumir el servicio.
- El rango de enrutamiento entre dominios sin clase (CIDR) del centro de datos local debe estar abierto para la generación de tokens de API desde la consola de VMware Cloud en AWS. La siguiente lista proporciona las funciones mínimas necesarias para generar los tokens de API:
  - Miembro de la organización
  - Propietario de la organización
  - Funciones de servicio: VMware Cloud en AWS
  - Administrador
  - NSX Cloud Directory
  - Auditor de NSX Cloud

Para obtener más información al respecto, consulte Opciones de conectividad para los SDDC de VMware Cloud en AWS en el blog de la red de socios de AWS.

Limitaciones

- Solo puede configurar 20 cuentas de VMware Cloud con puntos de enlace públicos en una sola instancia de vRealize Automation. Para obtener más información al respecto, consulte los máximos de escalabilidad y simultaneidad en la documentación de VMware.

Versiones de producto

- vRealize Automation, versión 8.x o posterior
- VMware vRealize Identity Manager versión 3.x o posterior
- VMware vRealize Suite Lifecycle Manager, versión 8.x o posterior

Arquitectura

En el siguiente diagrama se muestran los servicios de vRealize Automation que pueden utilizar la infraestructura de entornos locales y de VMware Cloud en AWS.

Componentes de VMware Cloud Assembly

VMware Cloud Assembly es un componente fundamental de vRealize Automation y puede usarlo para implementar y aprovisionar máquinas virtuales y recursos de cómputo. En la siguiente tabla se describen los componentes de VMware Cloud Assembly que se deben configurar para el aprovisionamiento de máquinas virtuales en VMware Cloud en AWS.

Componentes	Definición
Cuenta en la nube	La cuenta en la nube proporciona los detalles de la conexión (por ejemplo, el nombre del servidor, el nombre de usuario y la contraseña, la clave de acceso y el token de API). VMware Cloud Assembly utiliza la cuenta de nube para recopilar un inventario de sus recursos.
Zonas de nube	Las zonas de nube identifican los límites de los recursos en la cuenta de nube (por ejemplo, las regiones de AWS y el SDDC de la nube). Las zonas de nube asocian los recursos de cómputo al proyecto de Cloud Assembly.
Proyectos	Un proyecto es una entidad lógica que consta de usuarios y recursos, como las zonas de nube. También consta de cuotas de recursos y políticas de nomenclatura de máquinas

	virtuales que se utilizan al crear la máquina virtual.
Mapeos de versiones	El mapeo de tipos proporciona información sobre la capacidad de la máquina virtual (por ejemplo, la cantidad de CPU y la cantidad de memoria) que se utiliza en la plantilla de nube.
Mapeos de imágenes	El mapeo de imágenes mapea la plantilla de máquina virtual VMware vSphere y la imagen de Amazon Web Services (AWS) que se utilizan en la plantilla de nube. Para obtener más información al respecto, consulte Más información sobre las asignaciones de imágenes en vRealize Automation en la documentación de VMware.
Perfiles de red	El perfil de red controla la decisión de ubicación para elegir una red durante el aprovisio namiento de máquinas virtuales.
Perfil de almacenamiento	El perfil de almacenamiento controla la decisión de ubicación para elegir el almacenamiento durante el aprovisionamiento de máquinas virtuales.
Plantillas en la nube	Las plantillas de nube de VMware son un componente importante de vRealize Automatio n porque definen el aprovisionamiento y la organización de la infraestructura de nube. Las plantillas en la nube son especificaciones de los recursos e incluyen el tipo de recurso, las propiedades de los recursos y los datos que deben recopilarse de los usuarios.

Herramientas

- VMware vRealize Automation: vRealize Automation es una plataforma de automatización de infraestructuras con una gestión del estado y un cumplimiento basados en eventos. Está diseñado para ayudar a las organizaciones a controlar y proteger las nubes de autoservicio, la automatización multinube con gobernanza y DevOps la entrega de infraestructura basada en datos.
- VMware Cloud en AWS: VMware Cloud en AWS es una oferta de nube integrada desarrollada conjuntamente por AWS y VMware.

Epics

Genera los tokens de la API

Tarea	Descripción	Habilidades requeridas
Genere los tokens de API desde su cuenta de VMware Cloud en AWS.	1. Inicie sesión en la consola de VMware Cloud. 2. En la barra de herramientas de VMware Cloud Services, seleccione Mi cuenta y, a continuación, API Token. 3. Introduzca un nombre para el token de API, indique la vida útil requerida y defina los ámbitos del token. 4. Seleccione la casilla Abrir ID y, a continuación, seleccione Generar. 5. Registra las credenciales del token de API. Para obtener más informaci ón al respecto, consulte Cómo se generan los tokens de	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	API en la documentación de VMware.	

Instale vRealize Automation en su centro de datos en las instalaciones

Tarea	Descripción	Habilidades requeridas
Descargue el software necesario.	Descargue el archivo ISO de VMware vRealize Suite desde el portal My VMware. Este paquete contiene vRealize Suite Lifecycle Manager, VMware Identity Manager y vRealize Automation.	Administrador de la nube
Instale el software.	Instale el software y conéctese al SDCC de su nube siguiendo las instrucciones que se indican en la documenta ción de VMware sobre cómo instalar vRealize Suite Lifecycle Manager con Easy Installer for vRealize Automation y VMware Identity Manager. Importante: asegúrese de que lo siguiente esté disponible para la instalación: • La configuración local de VMware vCenter Server y las credenciales de inicio de sesión	Administrador de la nube, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	• Los detalles de red de la IP y la subred de vRealize Automation • La clave de licencia de vRealize Automation	

Conectar VMware Cloud en AWS con VMware Cloud Assembly

Tarea	Descripción	Habilidades requeridas
Configurar sus cuentas de nube.	1. En VMware Cloud Console, abra la pestaña Infraestructura, seleccione Administrar: cuentas de nube y, a continuación, Añadir cuentas de nube. 2. Seleccione VMware Cloud en AWS como tipo. 3. Pegue la información del token de API que registró anteriormente. Esto rellena todos los SDDC en la nube disponibles en su organización de VMware Cloud en AWS. 4. Seleccione el SDCC en la nube necesario y, a continuación, proporcione el nombre de usuario y la contraseña de vCenter para el SDDC. 5. Una vez que se haya autenticado correctam	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	ente, podrá ver la cuenta integrada de VMware Cloud en AWS con el estado OK. Para obtener más informaci ón al respecto, consulte Crear una cuenta de nube de VMware Cloud en AWS en vRealize Automation en la documentación de VMware.	
Configure el proyecto.	1. En VMware Cloud Console, abra la pestaña Proyectos y, a continuación, elija Nuevo proyecto. 2. Ingrese el nombre de su proyecto. 3. Abra la pestaña Zonas de nube y seleccione la cuenta en la nube predeterminada de VMware Cloud en AWS .	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Configure la zona de nube.	1. En VMware Cloud Console, abra Zonas de nube y elija la zona de nube para su centro de datos del SDDC. 2. De forma predeterminada, `cloudadmin@vmc.local` (este es el ID de usuario local predeterminado para el vCenter del SDDC en la nube) sólo tiene acceso a la provisión en. `Compute-ResourcePool` 3. Abre la pestaña Compute en Cloud Zones y, a continuación, selecciona Compute -. ResourcePool	Administrador de la nube
Configure el mapeo de versiones.	1. Abra la pestaña de Mapeos de versiones y cree un nuevo mapeo de versiones. 2. Introduzca el nombre del tipo, elija la cuenta de VMware Cloud en AWS y, a continuación, indique la cantidad de vCPU y la cantidad de memoria.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Configure el mapeo de imágenes.	1. Abra Image Mappings y cree un nuevo mapeo de imágenes. 2. Escriba el nombre de la imagen. 3. Elija la cuenta de VMware Cloud en AWS y proporcio ne las plantillas de cuentas de nube necesarias.	Administrador de la nube
Configure el perfil de red.	1. Abra el perfil de red y cree un nuevo perfil de red. 2. Ingrese el nombre del perfil de red. 3. Abra la pestaña Red y elija la red existente que desee usar para el aprovisio namiento.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Configure el perfil de almacenamiento.	1. Abra el Perfil de almacenamiento y seleccione Nuevo perfil de almacenamiento. 2. Introduzca el nombre del perfil de almacenamiento. 3. En la sección Políticas, cree una nueva política. 4. Seleccione almacén de datos de la carga de trabajo. De forma predeterminada, `cloudadmin@vmc.local` solo tiene acceso al aprovisionamiento en el almacén de datos de la carga de trabajo.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Cree la plantilla de nube.	1. Abra la pestaña Diseño, seleccione Plantillas en la nube y, a continuación, Nuevo desde y Hoja en blanco. 2. Proporcione el nombre y la descripción de la plantilla en la nube. 3. Seleccione el proyecto que creó anteriormente. 4. Desde la página de diseño de recursos de Cloud Template, arrastre los componentes al lienzo en blanco según sus necesidades. 5. Seleccione Probar para probar la plantilla y solucionar cualquier problema. 6. Seleccione Implementación y proporcione el nombre de la implementación para implementar las máquinas virtuales. Para obtener más informaci ón al respecto, consulte Crear una plantilla de nube básica en la documentación de VMware.	Administrador de la nube

Recursos relacionados

- Conecte la versión 8.x de vRealize Automation al SDDC:
- Implemente un SDDC desde la consola VMware Cloud en AWS
- Integración de AWS Direct Connect con VMware Cloud en AWS

Implemente un SDDC de VMware en AWS mediante VMware Cloud en AWS

Creado por Deepak Kumar (AWS) y Derek Cox (AWS)

Entorno: producción	Tecnologías: nube híbrida; infraestructura	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon VPC		

Resumen

Aviso: A partir del 30 de abril de 2024, VMware Cloud on AWS dejará de ser revendido por AWS sus socios de canal. El servicio seguirá estando disponible a través de Broadcom. Le recomenda mos que se ponga en contacto con su AWS representante para obtener más información.

Este patrón describe cómo crear un centro de datos definido por software (SDDC) basado en VMware que esté alojado en la nube de Amazon Web Services (AWS). Puede implementar un SDDC para migrar sus cargas de trabajo basadas en VMware vSphere a la nube de AWS y aprovechar los servicios de AWS mientras utiliza sus herramientas y habilidades de VMware existentes. Puede usar este SDDC para ejecutar sus aplicaciones de producción en entornos de nube privada, pública e híbrida basados en VMware vSphere, con acceso optimizado a los servicios de AWS. Por ejemplo, puede usar el SDDC como sitio secundario para la recuperación de desastres o para ampliar su centro de datos a diferentes ubicaciones geográficas.

VMware Cloud on AWS es un servicio pay-as-you-go (bajo demanda) que permite a las empresas de todos los tamaños ejecutar cargas de trabajo en entornos de nube basados en VMware vSphere mediante una amplia gama de servicios de AWS. Puede empezar con un mínimo de 2 hosts por clúster de SDDC y escalar hasta 16 hosts por clúster en su entorno de producción. Para obtener más información, consulte el sitio web de VMware Cloud en AWS. Para obtener más información sobre los SDCC, consulte Acerca de los centros de datos definidos por software en la documentación de VMware.

Requisitos previos y limitaciones

Requisitos previos

- Regístrese para obtener una cuenta de MyVMware y complete todos los campos.
- Inscribirse en una cuenta de AWS. Para obtener instrucciones, consulte el Centro de conocimiento de AWS.
- Regístrese para obtener una cuenta de MyVMware Cloud en AWS. Se envía un enlace de activación a la dirección de correo electrónico que especifique al registrarse.

Limitaciones

- Consulte las páginas de límites de configuración de VMware Cloud en AWS en el sitio web de VMware.

Versiones de producto

- Consulte Notas de la versión de VMware Cloud en AWS en la documentación de VMware.

Arquitectura

Pila de tecnología de destino

El siguiente diagrama muestra la pila de software de VMware, que incluye vSphere, vCenter, vSAN y NSX-T, que se ejecuta en una infraestructura bare-metal dedicada de AWS. Puede gestionar sus recursos y herramientas basados en VMware en AWS con una integración perfecta con otros servicios de AWS como Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), Amazon Redshift, AWS Direct Connect, Amazon Relational Database Service (Amazon RDS) y Amazon DynamoDB.

La entidad básica de VMware Cloud en AWS es un SDDC, que incluye los siguientes componentes:

- Computación: el componente de computación es la capa más baja del SDDC de VMware Cloud en AWS. VMware Cloud en AWS se ejecuta en tipos de instancias bare-metal de Amazon EC2. Estos incluyen `i3.metal`, `i3en.metal` y `i4i.metal`, y proporcionan acceso directo a recursos físicos como procesadores y memoria.

Importante: El tipo de instancia `i3.metal` de VMware Cloud en AWS, incluidas las opciones bajo demanda y de suscripción con plazos de uno y tres años, llegará al final de su vida útil y del soporte el 31 de diciembre de 2026. Además, los nuevos clientes actualmente no pueden solicitar instancias `i3.metal`. Para obtener más información, consulte el anuncio en el blog de VMware Cloud.

- Almacenamiento: los clústeres de SDDC admiten VMware vSAN con una configuración basada íntegramente en tecnología flash para el almacenamiento mediante almacenamiento flash express de memoria no volátil (NVMe), que proporciona un almacenamiento rápido y de alto rendimiento. A partir de la versión 1.20 del SDDC, VMware Cloud on AWS ofrece soporte para dos tipos de almacenamiento externo: Amazon FSx para NetApp ONTAP y VMware Cloud Flex Storage.
- Redes: las capacidades y políticas de red se administran mediante VMware NSX-T en el clúster del SDDC. Las redes virtuales de varios niveles se crean en el clúster del SDDC para separar los recursos de la red del equipo físico. Esto permite a los usuarios de VMware Cloud en AWS crear redes lógicas definidas por software.

Herramientas

- VMware Cloud en AWS es una oferta de nube integrada desarrollada conjuntamente por AWS y VMware.

Epics

Cree una VPC y una subred en su cuenta de AWS

Tarea	Descripción	Habilidades requeridas
Inicie sesión en su cuenta de AWS.	Inicie sesión en su cuenta de AWS con credenciales que tengan permisos de administrador.	Administrador de la nube
Cree una nueva VPC.	En este paso, definirá una nube privada virtual (VPC) que se vincule al SDDC. Si ya tiene una VPC que desee	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	utilizar para el SDDC, omita este paso. 1. Elija la región de AWS para implementar su SDDC de VMware Cloud en AWS. 2. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/. 3. En el panel de navegación, elija Your VPCs (Sus VPC). 4. Seleccione Crear VPC. 5. Especifique la configuración de la VPC, como la etiqueta de nombre de la VPC, el bloque CIDR de IPv4, la tenencia (mantenga la como predeterminada) y, a continuación, elija Crear VPC. 6. Cuando se haya creado la VPC, elija Cerrar. Para obtener más información, consulte la sección sobre cómo crear y configurar la VPC en la documentación de AWS.	

Tarea	Descripción	Habilidades requeridas
Cree una subred privada.	Ahora creará una subred privada para la interfaz de red elástica (ENI) de cada zona de disponibilidad. Le recomendamos que utilice una subred sin una puerta de enlace de Internet conectada. 1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/. 2. En el panel de navegación, elija Subnets (Subredes). 3. Elija Create Subnet (Crear subred). 4. En la página de Create Subnet (Crear subred), elija la VPC que creó antes. 5. Complete la configuración de la subred, incluidos el nombre de la subred, la zona de disponibilidad y el bloque CIDR de IPv4. 6. Elija Create Subnet (Crear subred). Repita estos pasos para crear subredes para cada zona de disponibilidad de la región.	Administrador de la nube

Active VMware Cloud en AWS

Tarea	Descripción	Habilidades requeridas
Active el servicio.	Al registrarse para obtener una cuenta de MyVMware, VMware le envía un correo electrónico de bienvenida y un enlace de activación a la dirección de correo electrónico que especificó. 1. Abra el enlace Activar el servicio que aparece en el correo electróni co de bienvenida de su navegador. 2. Inicie sesión con las credenciales de MyVMware. 3. Revise y acepte los términos y condiciones de uso de los servicios. 4. Complete el proceso de activación de la cuenta. Se le redirigirá a la consola de VMware Cloud en AWS. (Nota: Las cuentas de VMware Cloud en AWS se basan en una organizac ión, que representa un grupo o línea de negocio suscrito a la cuenta. Esta organización no tiene ninguna relación con AWS Organizations.)	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	5. En la página Seleccionar o crear una organización, cree una organización que esté vinculada a la cuenta de MyVMware. 6. Introduzca el Nombre de la organización y la Dirección para distinguirlos de forma lógica. 7. Elija Crear organización para completar este proceso. Para obtener más información sobre este proceso, consulte la Guía de implementación y prácticas recomendadas del SDDC en AWS en la documentación de AWS.	

Tarea	Descripción	Habilidades requeridas
Asigne roles de IAM.	Cuando se haya creado la organización, asigne acceso privilegiado a usuarios específicos para acceder a los servicios en la nube y a la consola del SDDC, al SDDC y a los componentes de NSX. Para obtener instrucciones, consulte Asignar un rol de servicio de VMC a un miembro de la organización en la documentación de VMware. Existen dos tipos de roles de organización: • Los propietarios de la organización pueden añadir, eliminar y modificar usuarios y acceder a todos los recursos de nube. • Los miembros de la organización solo pueden acceder a los recursos de la nube.	Administrador de la nube

Implemente un SDDC

Tarea	Descripción	Habilidades requeridas
Implemente un SDDC en su cuenta de VMware Cloud en AWS.	Importante: Una vez que se ha asociado una cuenta de AWS a una organización de VMware como vendedor	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	registrado, el número de cuenta de AWS no se puede actualizar. Solo puede haber un vendedor registrado de AWS por organización de VMware. Para implementar un SDDC: 1. Inicie sesión en la consola de VMC en https://vmc.vmware.com. 2. Elija el servicio VMware Cloud en AWS entre los servicios disponibles. 3. Elija Create SDDC (Creación de SDDC). 4. Introduzca las propiedades del SDDC, como la región de AWS, la implement ación (host único, host múltiple o clúster ampliado), tipo de host, nombre del SDDC, número de hosts, capacidad del host y capacidad total y, a continuación, seleccione Siguiente. 5. Conéctese a su cuenta de AWS y, a continuación, seleccione Siguiente. 6. Seleccione la VPC y la subred configura das anteriormente y, a	

Tarea	Descripción	Habilidades requeridas
	continuación, elija Siguiente . 7. Introduzca el bloque CIDR de la subred de administración para el SDDC y, a continuación, seleccione SIGUIENTE. Para obtener más información, consulte Selección de subredes IP y conectividad para el SDDC en el blog de VMware Cloud. 8. Seleccione las dos casillas de verificación para confirmar que asume la responsabilidad de los costos de implementación de un SDDC y, a continuación, seleccione Implementar SDDC. Se le cobrará cuando elija Implementar SDDC. No podrá pausar ni cancelar el proceso de implementación, que tarda algún tiempo en completarse. Para obtener más información sobre la creación de un SDDC, consulte Implementación de un SDDC desde la consola de VMC en la documentación de VMware.	

Recursos relacionados

- Implementación y administración de un centro de datos definido por software (documentación de VMware)
- Características de VMware Cloud en AWS (sitio web de AWS)
- Acelere la migración y la modernización de la nube con VMware Cloud en AWS (video)

Integre VMware vRealize Network Insight con VMware Cloud on AWS

Creado por Deepak Kumar (AWS), Piotr Pitera (AWS) y Sachin Trivedi (AWS)

Entorno: PoC o piloto	Fuente: VMware vRealize Network Insight	Destino: VMware Cloud en AWS
Tipo R: reubicar	Carga de trabajo: todas las demás cargas de trabajo	Tecnologías: Nube híbrida; Infraestructura; Migración
Servicios de AWS: VMware Cloud en AWS		

Resumen

Aviso: A partir del 30 de abril de 2024, VMware Cloud on AWS ya no será revendido por AWS sus socios de canal. El servicio seguirá estando disponible a través de Broadcom. Le recomendamos que se ponga en contacto con su AWS representante para obtener más información.

Este patrón describe cómo integrar VMware vRealize Network Insight con VMware Cloud on AWS e inspeccionar el flujo de tráfico de sus máquinas virtuales. Esta integración también le ayuda a planificar las migraciones de aplicaciones a VMware Cloud on. AWS

vRealize Network Insight ofrece visibilidad de su infraestructura de red. Proporciona funciones de supervisión y análisis de la red para mejorar la seguridad, mitigar los riesgos de migración y optimizar el rendimiento. Puede usar esta herramienta para monitorear los flujos de tráfico de sus máquinas virtuales y ver las reglas de seguridad recomendadas en función del tráfico observado. Para obtener más información sobre vRealize Network Insight, consulte la documentación de VMware.

VMware Cloud on AWS es un servicio pay-as-you-go (bajo demanda) que permite a las empresas de todos los tamaños ejecutar cargas de trabajo en entornos de nube basados en VMware vSphere mediante una amplia gama de. Servicios de AWS Puede empezar con un mínimo de 2 hosts por clúster de SDDC y escalar hasta 16 hosts por clúster en su entorno de producción. Para obtener más

información, consulte el sitio web de VMware Cloud on. AWS Para obtener más información sobre los SDCC, consulte Acerca de los centros de datos definidos por software en la documentación de VMware.

Requisitos previos y limitaciones

Requisitos previos

- SDDC de VMware Cloud on AWS, implementado

Limitaciones

- Para conocer las limitaciones conocidas, consulte la documentación de VMware.

Versiones de producto

- vRealize Network Insight, versión 5.0.0
- SDDC de VMware Cloud on AWS, versión 1.24

Arquitectura

Pila de tecnología de origen

- vRealize Network Insight

Pila de tecnología de destino

- VMware Cloud en AWS

Arquitectura de destino

El siguiente diagrama muestra la conectividad entre VMware Cloud on AWS y vRealize Network Insight in situ.

Herramientas

- VMware Cloud on AWS es una oferta de nube integrada desarrollada conjuntamente por AWS VMware.
- VMware vRealize Network Insight es una herramienta de monitoreo y análisis que proporciona visibilidad de la infraestructura de red para planificar y solucionar problemas de seguridad.

Epics

Configure su entorno para vRealize Network Insight

Tarea	Descripción	Habilidades requeridas
Cree una cuenta de usuario de VMware.	Cree una cuenta de usuario de VMware o inicie sesión en su cuenta de VMware existente. Para abrir una cuenta nueva: 1. Para obtener una cuenta de VMware Customer Connect, complete el formulario de registro. Los nuevos usuarios recibirán un correo electrónico para activar sus cuentas. 2. Introduzca el código de autenticación del correo electrónico. 3. Inicie sesión en Customer Connect.	Administrador de la nube
Descargue los archivos OVA de vRealize Network Insight.	Descargue los archivos OVA para vRealize Network Insight:.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	1. Diríjase a la página de descarga de productos de VMware en https://my.vmware.com/group/vmware/home. 2. Busque vRealize Network Insight. 3. Descargue la plataforma y los archivos OVA recopiladores más recientes de vRealize Network Insight, versión 5.0.0.	
Implemente vRealize Network Insight.	Para obtener instrucciones de implementación, consulte la documentación de VMware.	Administrador de la nube

Agregue una fuente de datos y un recopilador

Tarea	Descripción	Habilidades requeridas
Agregue una fuente de datos.	1. Inicie sesión en vRealize Network Insight. 2. Seleccione la configuración, las cuentas y las fuentes de datos y añada la fuente. 3. En Tipo, elija Servidor vCenter local. Para obtener más información, consulte la documentación de VMware.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Configure un recopilador para la fuente de datos.	Para obtener instrucciones, consulte la documentación de VMware.	Administrador de la nube

Analice las dependencias de las aplicaciones

Tarea	Descripción	Habilidades requeridas
Crear una aplicación.	Si no tiene una aplicación existente en vRealize Network Insight, siga los pasos de la documentación de VMware para crear una.	Administrador de la nube
Descubra y analice su aplicación.	1. Utilice vRealize Network Insight para descubrir su aplicación. Para obtener instrucciones, consulte la documentación de VMware. 2. Analice su aplicación. Para obtener instrucciones, consulte la documentación de VMware.	Administrador de la nube

Recursos relacionados

- Implemente un SDDC de VMware en AWS mediante VMware Cloud on AWS(orientaciónAWS prescriptiva)
- Configure una extensión de centro de datos para VMware Cloud AWS mediante el modo híbrido vinculado (AWS guía prescriptiva)
- Migre el SDDC de VMware a VMware Cloud AWS con VMware HCX (guía prescriptiva)AWS
- Documentación sobre VMware vRealize Network Insight (sitio web de VMware)

Migración de las máquinas virtuales a VMware Cloud en AWS mediante la migración asistida por HCX OS

Creado por Deepak Kumar (AWS) e Himanshu Gupta (AWS)

Entorno: PoC o piloto	Origen: entorno que no es de vSphere	Destino: SDDC de VMware Cloud en AWS
Tipo R: reubicar	Carga de trabajo: todas las demás cargas de trabajo	Tecnologías: nube híbrida, migración

Resumen

Aviso: A partir del 30 de abril de 2024, VMware Cloud on AWS ya no será revendido por AWS sus socios de canal. El servicio seguirá estando disponible a través de Broadcom. Le recomendamos que se ponga en contacto con su AWS representante para obtener más información.

Este patrón describe cómo migrar una máquina virtual (VM) de un entorno que no es de vSphere a VMware Cloud on Amazon Web Services (AWS) mediante la migración asistida por sistema operativo (OSAM).

OSAM forma parte de VMware Hybrid Cloud Extension (HCX), que se incluye con VMware Cloud en AWS. Puede usar OSAM para migrar un entorno que no sea de vSphere, como VMware KVM o Hyper-V, a VMware Cloud en AWS. OSAM utiliza el software Sentinel, que se instala en una máquina virtual huésped de Windows o Linux para ayudar a replicar la máquina virtual desde su entorno local a un centro de datos definido por software (SDDC) en VMware Cloud en AWS.

Este patrón explica cómo habilitar OSAM, instalar el software Sentinel en una máquina virtual Windows, conectarse y registrarse en un dispositivo HCX Sentinel Gateway (SGW) en el sitio de origen y establecer una conexión de reenvío con un dispositivo HCX Sentinel Data Receiver (SDR) en el sitio de destino para iniciar la migración.

Para obtener más información acerca de OSAM, consulte la documentación de VMware.

Requisitos previos y limitaciones

Requisitos previos

- Instale HCX en sus entornos de origen y destino. Para conocer los requisitos previos de HCX, consulte Migración del SDDC de VMware a VMware Cloud en AWS con VMware HCX en la documentación de recomendaciones de AWS.
- Para conocer los requisitos previos de OSAM, consulte la lista de verificación de instalación en la documentación de VMware.
- Para obtener información sobre los puertos OSAM, consulte los requisitos de puertos HCX de VMware en el sitio web de puertos y protocolos de VMware.

Limitaciones

- Límites de configuración de VMware HCX 4.2.0
- Consideraciones para la implementación de OSAM
- Sistemas operativos huéspedes compatibles
- Consideraciones sobre el sistema operativo huésped

Versiones de producto

- VMware HCX 4.2.0
- VMware SDDC 1.12

Arquitectura

El siguiente diagrama muestra cómo HCX OSAM trabaja con el software Sentinel para replicar máquinas virtuales que no son de vSphere desde su entorno local a VMware Cloud en AWS.

OSAM consta de tres componentes:

- El dispositivo Sentinel Gateway (SGW), que se utiliza para conectar y reenviar cargas de trabajo y aplicaciones en el entorno de origen basado en VMware
- El receptor de datos Sentinel (SDR), que se utiliza en el entorno VMware Cloud en AWS de destino para recibir las cargas de trabajo migradas desde el origen

- El software Sentinel, que debe estar instalado en cada máquina virtual invitada que desee migrar

OSAM utiliza el software Sentinel que se instala en las máquinas virtuales invitadas de Windows o Linux para ayudar a replicar una máquina virtual desde las instalaciones a un SDDC de VMware. El software Sentinel que se instala en las máquinas virtuales invitadas recopila las configuraciones del sistema de las máquinas virtuales invitadas y ayuda a replicar los datos. Esta información también se utiliza para crear el inventario de las máquinas virtuales invitadas para la migración y ayuda a preparar los discos de la máquina virtual de réplica para fines de replicación y migración.

Herramientas

- VMware HCX 4.2.0
- SDDC de VMware Cloud en AWS

Epics

Configuración de HCX

Tarea	Descripción	Habilidades requeridas
Implemente HCX Cloud y HCX Connector.	Siga las instrucciones de las instalaciones de HCX Connector y HCX Cloud de la documentación de VMware.	Administrador de la nube, administrador de sistemas

Configure OSAM y migre las máquinas virtuales

Tarea	Descripción	Habilidades requeridas
Instale HCX Sentinel.	Para instalar Sentinel en Linux: 1. En vCenter Server para el conector HCX, seleccione Interconnect, Multi-Site	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	Service Mesh o Sentinel Management. 2. Seleccione Descargar el paquete de Linux. 3. Instale el agente Sentinel en una máquina Linux. Para obtener más información, consulte Descarga e instalación del software HCX Sentinel Agent en la documentación de VMware.	

Tarea	Descripción	Habilidades requeridas
Migre las máquinas virtuales.	Para migrar las máquinas virtuales en grupos (denominados grupos de movilidad), siga estos pasos: 1. En vSphere Client, en el complemento HCX, elija Servicios, Migración. 2. Seleccione Migrar. 3. Elija Non vSphere Inventory, Remote Connections. Esto mostrará la lista de máquinas virtuales en las que instaló HCX Sentinel. 4. En Nombre de grupo, introduzca el nombre del grupo de movilidad que desee crear para las máquinas virtuales. 5. Elija las máquinas virtuales que desee migrar y, a continuación, elija Agregar para agregarlas al grupo de movilidad. 6. Para cada máquina virtual: a. Seleccione el contenedor de cómputo de destino. b. Seleccione el almacenamiento de destino. c. Seleccione el perfil de migración.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	d. Seleccione la carpeta de destino. 7. Para iniciar el proceso de migración, selecciona Ir. HCX valida sus selecciones de máquinas virtuales antes de que comience la migración. Para obtener más informaci ón, consulte Migración de máquinas virtuales con grupos de movilidad y Supervisión y estimación de la migración con grupos de movilidad en la documentación de VMware.	

Recursos relacionados

Documentación de VMware:

- Guía de usuario de VMware HCX
- Instale la lista de verificación B: HCX con un entorno de destino de VMC SDDC
- VMware HCX en VMware Cloud en AWS
- Migración asistida por HCX OS para VMware Cloud en AWS
- Notas de versión 4.2.1 de VMware HCX

Envíe registros desde VMware Cloud on AWS a Splunk mediante VMware Aria Operations for Logs

Creado por Deepak Kumar (AWS) y Piotr Pitera (AWS)

Entorno: producción	Fuente: registros y eventos de VMware Cloud on AWS	Objetivo: punto final local de Splunk
Tipo R: reubicar	Carga de trabajo: todas las demás cargas de trabajo	Tecnologías: Nube híbrida; Infraestructura; Migración
Servicios de AWS: VMware Cloud en AWS		

Resumen

Aviso: A partir del 30 de abril de 2024, VMware Cloud on ya no AWS será revendido por parte de sus socios de AWS canal. El servicio seguirá estando disponible a través de Broadcom. Le recomendamos que se ponga en contacto con su AWS representante para obtener más informaci ón.

Este patrón describe cómo reenviar los AWS eventos o registros de VMware Cloud a un syslog o a un punto final HTTP, como Splunk, mediante VMware Aria Operations for Logs.

VMware Aria Operations for Logs es una herramienta de análisis de registros que ofrece una mayor visibilidad y agiliza la resolución de problemas en el entorno VMware Cloud on. AWS Puede configurar esta herramienta para enviar todos o una parte de los registros o eventos de VMware Cloud AWS a un punto final syslog o HTTP. El punto final puede ser un punto final de software como servicio (SaaS) o un punto final local como Splunk. (Este patrón proporciona las instrucciones para Splunk). Para obtener más información sobre VMware Aria Operations for Logs, consulte la documentación de VMware.

VMware Cloud on AWS es un servicio pay-as-you-go (bajo demanda) que permite a las empresas de todos los tamaños ejecutar cargas de trabajo en entornos de nube basados en VMware vSphere

mediante una amplia gama de. Servicios de AWS Puede empezar con un mínimo de 2 hosts por clúster de centro de datos definido por software (SDDC) y escalar hasta 16 hosts por clúster en su entorno de producción. Para obtener más información, consulte el sitio web de VMware Cloud on. AWS Para obtener más información sobre los SDCC, consulte Acerca de los centros de datos definidos por software en la documentación de VMware.

Requisitos previos y limitaciones

Requisitos previos

- Splunk, configurado localmente

Limitaciones

Puede suscribirse a una suscripción de prueba gratuita a VMware Aria Operations for Logs. Esta suscripción es válida durante 30 días y tiene las siguientes limitaciones:

- Tamaño máximo de registros que puede reenviar: 50 GB de registros por día
- Número máximo de configuraciones de reenvío de registros que puede crear: 10
- Número máximo de configuraciones de reenvío de registros que puede activar: 5

Para acceder a todas las funciones del servicio, debe actualizar a una suscripción premium.

Para obtener más información sobre las suscripciones de prueba y premium, consulte Suscripciones y facturación de VMware Aria Operations for Logs (SaaS) en la documentación de VMware. Para obtener más información sobre los límites de uso, consulte las limitaciones de uso de las funciones en la documentación de VMware.

Versiones de producto

- VMware Cloud on AWS SDDC, versión 1.24
- VMware Aria Operations for Logs, versión 8.10
- Splunk local, versión 9.x

Arquitectura

Pila de tecnología de origen

- VMware Cloud en AWS
- Operaciones de VMware Aria para registros

Pila de tecnología de destino

- Splunk local

Arquitectura de destino

El siguiente diagrama muestra la conectividad entre un centro de datos corporativo y VMware Aria Operations for Logs en VMware Cloud on. AWS

Herramientas

- VMware Cloud on AWS es una oferta de nube integrada desarrollada conjuntamente por AWS VMware.
- VMware Aria Operations for Logs es una herramienta de análisis de registros y solución de problemas para VMware Cloud on AWS.

Epics

Implemente un SDDC y habilite VMware Aria Operation for Logs

Tarea	Descripción	Habilidades requeridas
Implemente una nube de VMware en AWS un SDDC.	Siga las instrucciones de la Guía prescriptiva sobre cómo implementar un SDDC de VMware AWS mediante VMware Cloud on AWS. AWS	Arquitecto de la nube, administrador de la nube
Inscríbase en VMware Aria Operations for Logs.	Para obtener instrucciones, consulte la documentación de VMware.	Arquitecto de la nube

Implemente un proxy en la nube

Tarea	Descripción	Habilidades requeridas
Implemente un proxy en la nube.	Para reenviar los registros a una instancia local de Splunk, debe añadir un proxy en la nube para VMware Aria Operations for Logs. Este proxy recibe información del centro de datos local y la envía a VMware Aria Operations for Logs para su análisis. Para descargar e instalar el proxy en la nube: 1. Asegúrese de que los puertos 443, 22 y 514 estén abiertos entre su entorno local y VMware Cloud on AWS. Para puertos adicionales, puede usar 1514/TCP o 6514/TCP. Para obtener más informaci ón sobre los puertos, consulte las recomenda ciones de VMware Aria Operations for Logs Firewall en la documentación de VMware. 2. Inicie sesión en VMware Aria Operations for Logs. 3. En la página de inicio, seleccione Añadir recopilad or en el widget.	Administrador de la nube, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	4. En la pantalla del dispositivo virtual Cloud Proxy, copie la clave del token. Debe utilizar esta clave en un plazo de 24 horas para completar los siguientes pasos. 5. Elija el enlace de descarga del archivo OVA. 6. Vaya al cliente web VMware vSphere, elija su clúster y, a continuación, seleccione Implementar plantilla OVF. 7. Cuando se le pida la clave, pegue la clave simbólica que copió en el paso 4. 8. Selecciona Finalizar para instalar el proxy en la nube.	

Reenvíe los registros a un punto final de Splunk local

Tarea	Descripción	Habilidades requeridas
Configure el reenvío de registros.	Para reenviar los registros al punto final de Splunk: 1. Inicie sesión en VMware Aria Operations para ver los registros. 2. Vaya a Administración de registros. 3. Elija el reenvío de registros.	

Tarea	Descripción	Habilidades requeridas
	4. Elija Nueva configuración y complete los siguientes ajustes: • Proporcione un nombre para la configuración de reenvío de registros. • En Destino, elija On Premises. • Para Cloud Proxy, seleccione el proxy en la nube que instaló anteriormente. • En Tipo de punto final, selecciona TCP. • Para la URL de Endpoint, proporciona la URL de Splunk local en el formato: `tcp://x.x.x.x (your Splunk IP address): 514` • (Opcional) En el caso de las etiquetas, puede especificar los nombres y valores de las etiquetas para facilitar las consultas . • Seleccione Aplicar a todos los registros o Aplicar a registros específicos. Si desea enviar todos los registros	

Tarea	Descripción	Habilidades requeridas
	de VMware Cloud on AWS a Splunk, elija Aplicar a todos los registros. 5. Seleccione Verificar. 6. Seleccione Guardar. Para obtener más información, consulte Reenviar registros de operaciones de VMware Aria para ver los registros en la documentación de VMware.	

Recursos relacionados

- VMware Cloud en el sitio AWS web
- Acerca de los centros de datos definidos por software (documentación de VMware)
- Implemente un SDDC de VMware AWS mediante VMware Cloud on AWS (guía prescriptiva)AWS
- Migre las cargas de trabajo a VMware Cloud On AWS mediante VMware HCX (guía prescriptiva)AWS
- Configure una extensión de centro de datos a VMware Cloud On AWS mediante el modo híbrido vinculado (AWS guía prescriptiva)

Configure una canalización de CI/CD para cargas de trabajo híbridas en Amazon ECS Anywhere mediante AWS CDK y GitLab

Creado por el Dr. Rahul Sharad Gaikwad (AWS)

Repositorio de código: - amazon-ecs-anywhere-cicd pipeline-cdk-sample	Entorno: PoC o piloto	Tecnologías: nube híbrida; contenedores y microserv icios; infraestructura; DevOps
Carga de trabajo: código abierto	Servicios de AWS: AWS CDK; AWS CodePipeline; Amazon ECS; AWS Systems Manager; AWS CodeCommit	

Resumen

Amazon ECS Anywhere es una extensión de Amazon Elastic Container Service (Amazon ECS). Permite registrar una instancia externa, como un servidor en las instalaciones o una máquina virtual (VM), en su clúster de Amazon ECS. Esta característica ayuda a reducir los costos y mitigar la compleja operativa y orquestación de los contenedores locales. Puede usar ECS Anywhere para implementar y ejecutar aplicaciones de contenedor tanto en entornos en las instalaciones como en la nube. Evita que su equipo tenga que aprender varios dominios y conjuntos de habilidades, o administrar software complejo por su cuenta.

Este patrón describe un step-by-step enfoque para aprovisionar un clúster de Amazon ECS con instancias de Amazon ECS Anywhere mediante pilas del Cloud Development Kit (AWS CDK) de Amazon Web Services (AWS). A continuación, utiliza AWS CodePipeline para configurar una canalización de integración e implementación continuas (CI/CD). A continuación, replica el repositorio de GitLab código en AWS CodeCommit e implementa la aplicación en contenedores en el clúster de Amazon ECS.

Este patrón está diseñado para ayudar a quienes utilizan la infraestructura local a ejecutar aplicaciones de contenedores y GitLab a administrar la base de código de la aplicación. Puede administrar esas cargas de trabajo con los servicios en la nube de AWS sin interrumpir su infraestructura existente en las instalaciones.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una aplicación en contenedor ejecutada en una infraestructura en las instalaciones.
- Un GitLab repositorio en el que puede administrar la base de código de su aplicación. Para obtener más información, consulte Repository (GitLab).
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada. Para obtener más información, consulte Instalar o actualizar la última versión de la CLI de AWS (documentación de la CLI de AWS).
- Kit de herramientas de AWS CDK, instalado y configurado globalmente. Para más información, consulte Instalar el CDK de AWS (documentación sobre el CDK de AWS).
- npm, instalado y configurado para la AWS CDK en. TypeScript Para obtener más información, consulte Descargar e instalar Node.js y npm (documentación de npm).

Limitaciones

- Para ver las limitaciones y consideraciones, consulte Instancias externas (Amazon ECS Anywhere) en la documentación de Amazon ECS.

Versiones de producto

- Kit de herramientas de AWS CDK, versión 2.27.0 o posterior
- npm versión 7.20.3 o posterior
- Node.js versión 16.6.1 o posterior

Arquitectura

Pila de tecnología de destino

- AWS CDK
- AWS CloudFormation
- AWS CodeBuild
- AWS CodeCommit

- AWS CodePipeline
- Amazon ECS Anywhere
- Amazon Elastic Container Registry (Amazon ECR)
- AWS Identity y Access Management (IAM)
- AWS Systems Manager
- GitLab repositorio

Arquitectura de destino

Este diagrama presenta los dos flujos de trabajo principales descritos en este patrón: el aprovisionamiento del clúster de Amazon ECS y la configuración del proceso de CI/CD, que se configura e implementa de la siguiente manera:

1. Aprovisionamiento del clúster de Amazon ECS
    a. Al implementar la primera pila de CDK de AWS, se crea una CloudFormation pila en AWS.
    b. Esta CloudFormation pila aprovisiona un clúster de Amazon ECS y los recursos de AWS relacionados.
    c. Para registrar una instancia externa en un clúster de Amazon ECS, debe instalar AWS Systems Manager Agent (SSM Agent) en su máquina virtual y registrar la máquina virtual como instancia gestionada por AWS Systems Manager.
    d. También debe instalar el agente de contenedores de Amazon ECS y Docker en su máquina virtual para registrarla como instancia externa en el clúster de Amazon ECS.
    e. Cuando la instancia externa está ya registrada y configurada con el clúster de Amazon ECS, puede ejecutar varios contenedores en su máquina virtual, registrada como instancia externa.
    f. El clúster de Amazon ECS está activo y puede ejecutar las cargas de trabajo de la aplicación a través de contenedores. La instancia de contenedor de Amazon ECS Anywhere se ejecuta en un entorno en las instalaciones, pero está asociada al clúster de Amazon ECS en la nube.
2. Configuración e implementación del proceso de CI/CD
    a. Al implementar la segunda pila de CDK de AWS, se crea otra CloudFormation pila en AWS.
    b. Esta CloudFormation pila proporciona una canalización CodePipeline y los recursos de AWS relacionados.

c. Los cambios en el código de la aplicación se insertan y se combinan en un GitLab repositorio local.

d. El GitLab repositorio se replica automáticamente en el CodeCommit repositorio.

e. Las actualizaciones del CodeCommit repositorio se inician automáticamente. CodePipeline

f. CodePipeline copia el código de la aplicación desplegable integrada CodeCommit y la crea. CodeBuild

g. CodePipeline crea una imagen de Docker del entorno de CodeBuild compilación y la envía al repositorio de Amazon ECR.

h. CodePipeline inicia CodeDeploy acciones que extraen la imagen del contenedor del repositorio de Amazon ECR.

i. CodePipeline implementa la imagen del contenedor en el clúster de Amazon ECS.

Automatizar y escalar

Este patrón emplea AWS CDK como herramienta de infraestructura como código (IaC) para configurar e implementar esta arquitectura. AWS CDK le permite orquestar los recursos de AWS y configurar Amazon ECS Anywhere y el proceso de CI/CD.

Herramientas

Servicios de AWS

- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura de la nube de AWS en código.
- AWS CodeCommit es un servicio de control de versiones que le ayuda a almacenar y gestionar repositorios de Git de forma privada, sin necesidad de gestionar su propio sistema de control de código fuente.
- AWS le CodePipeline ayuda a modelar y configurar rápidamente las diferentes etapas de una versión de software y a automatizar los pasos necesarios para publicar cambios de software de forma continua.
- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.
- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable.

- Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores escalable y rápido que ayuda a ejecutar, detener y administrar contenedores en un clúster. Este patrón también emplea Amazon ECS Anywhere, que permite registrar un servidor en las instalaciones o una máquina virtual en el clúster de Amazon ECS.

Otras herramientas

- Node.js es un entorno de JavaScript ejecución basado en eventos diseñado para crear aplicaciones de red escalables.
- npm es un registro de software que se ejecuta en un entorno Node.js y se utiliza para compartir o tomar prestados paquetes y administrar la implementación de paquetes privados.
- Vagrant es una utilidad de código abierto para compilar y mantener entornos de desarrollo de software virtual portátiles. Este patrón usa Vagrant con fines de demostración para crear una máquina virtual en las instalaciones.

Repositorio de código

El código de este patrón está disponible en la canalización de GitHub CI/CD de Amazon ECS Anywhere mediante el repositorio CDK de AWS.

Prácticas recomendadas

Tenga en cuenta las siguientes prácticas recomendadas al implementar este patrón:

- Prácticas recomendadas para desarrollar e implementar una infraestructura de nube con AWS CDK
- Prácticas recomendadas para desarrollar aplicaciones en la nube con AWS CDK (publicación del blog de AWS)

Epics

Verificar la configuración de AWS CDK

Tarea	Descripción	Habilidades requeridas
Verifique la versión de AWS CDK.	Compruebe la versión del kit de herramientas de AWS	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	CDK ejecutando el siguiente comando. `cdk --version` Este patrón requiere la versión 2.27.0 o posterior. Si tiene una versión anterior, siga las instrucciones de la documentación de AWS CDK para actualizarla.	
Verifique la versión de npm.	Verifique la versión de npm introduciendo el siguiente comando. `npm --version` Este patrón requiere la versión 7.20.3 o posterior. Si tiene una versión anterior, siga las instrucciones de la documentación de npm para actualizarla.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Configure las credenciales de AWS.	Para configurar las credencia les de AWS, ejecute el comando `aws configure` y siga las instrucciones. `$aws configure` `AWS Access Key ID` `[None]: <your-access-key-ID>` `AWS Secret Access Key` `[None]: <your-secret-access-key>` `Default region name` `[None]: <your-Region-name>` `Default output format` `[None]:`	DevOps ingeniero

Inicie el entorno de AWS CDK

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio de código de AWS CDK.	1. Clone el repositorio Proceso de CI/CD para Amazon ECS Anywhere mediante AWS CDK para usarlo en este patrón ejecutando el siguiente comando. `git clone https://github.com/aws-samples/amazon-ecs-anywhere-cicd-pipeline-cdk-sample.git`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	2. Acceda al directorio clonado ejecutando el siguiente comando. `cd amazon-ecs-anywhere-cicd-pipeline-cdk-sample`	
Inicie el entorno.	Implemente la CloudFormation plantilla en la cuenta y la región de AWS que desee utilizar introduciendo el siguiente comando. `cdk bootstrap <account-number>/<Region>` Para obtener más información, consulte Proceso de arranque en la documentación de AWS CDK.	DevOps ingeniero

Creación e implementación de la infraestructura para Amazon ECS Anywhere

Tarea	Descripción	Habilidades requeridas
Instale las dependencias del paquete y compile los TypeScript archivos.	Instale las dependencias del paquete y compile los TypeScript archivos introduciendo los siguientes comandos. `$cd EcsAnywhereCdk` `$npm install` `$npm fund`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Estos comandos instalan todos los paquetes del repositorio de muestra. Para obtener más información, consulte npm ci y npm install en la documentación de npm. Si recibe algún error relacionado con la falta de paquetes al ejecutar estos comandos, consulte la sección de Solución de problemas de este patrón.	
Compilar el proyecto.	Para construir el código del proyecto, introduzca el siguiente comando. `npm run build` Para obtener más informaci ón sobre la compilaci ón e implementación del proyecto, consulte Su primera aplicación de AWS CDK en la documentación de AWS CDK.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Implemente la pila de infraestructura de Amazon ECS Anywhere.	1. Haga una lista de las pilas introduciendo el siguiente comando. `$cdk list` 2. Confirme que el resultado devuelve las pilas `EcsAnywhereInfraStack` y `ECSAnywherePipelineStack` . 3. Implementar la pila de `EcsAnywhereInfraStack` introduciendo el siguiente comando. `$cdk deploy EcsAnywhereInfraStack`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Verifique la creación y el resultado de la pila.	1. Inicie sesión en la consola de administración de AWS y abra la CloudFormation consola en https://console.aws.amazon.com/cloudformation/. 2. En la página Pilas, seleccione la pila `EcsAnywhereInfraStack` . 3. Confirme que el estado de la pila es `CREATE_IN_PROGRESS` o `CREATE_COMPLETE` . La configuración del clúster de Amazon ECS puede llevar algún tiempo. No proceda hasta que se haya completado la creación de la pila.	DevOps ingeniero

Configure una máquina virtual en las instalaciones

Tarea	Descripción	Habilidades requeridas
Configurar su VM.	Cree una máquina virtual de Vagrant ejecutando el comando `vagrant up` desde el directorio raíz donde se encuentra Vagrantfile. Para obtener más información,	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	consulte la documentación de Vagrant.	

Tarea	Descripción	Habilidades requeridas
Registre su máquina virtual como instancia externa.	1. Inicie sesión en la máquina virtual de Vagrant ejecutando el comando `vagrant ssh`. Para obtener más información, consulte la documentación de Vagrant. 2. Instale la CLI de AWS en la máquina virtual siguiendo las instrucciones de instalación de la CLI de AWS y ejecute los siguientes comandos. `$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" \` `> -o "awscliv2.zip"` `$sudo apt install unzip` `$unzip awscliv2.zip` `$sudo ./aws/install` `$aws configure` `AWS Access Key ID [None]: <your-access-key-ID>` `AWS Secret Access Key [None]: <your-secret-access-key>` `Default region name [None]: <your-Region-name>` `Default output format [None]:` 1. Cree un código de activación y una ID que usará para	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	registrar su máquina virtual en AWS Systems Manager y activar su instancia externa. El resultado de este comando incluye los valores de ID de activación y código de activación. `aws ssm create-activation \ > --iam-role EcsAnywhereInstanceRole \ > | tee ssm-activation.json` Si recibe un error al ejecutar este comando, consulte la sección Solución de problemas. 2. Exporte los valores de ID de activación y código. `export ACTIVATION_ID=<activation-ID> export ACTIVATION_CODE=<activation-code>` 3. Descargue el script de instalación en su máquina virtual. `curl --proto "https" -o "ecs-anywhere-install.sh" \`	

Tarea	Descripción	Habilidades requeridas
	<pre>> "https://amazon-ecs-agent.s3.amazonaws.com/ecs-anywhere-install-latest.sh"</pre> 4. Ejecute el script de instalación en su VM. <pre>sudo bash ecs-anywhere-install.sh \ --cluster EcsAnywhereCluster \ --activation-id $ACTIVATION_ID \ --activation-code $ACTIVATION_CODE \ --region <region-name></pre> Este paso configura la máquina virtual como una instancia externa de Amazon ECS Anywhere, y registra la instancia en el clúster de Amazon ECS. Para obtener más información, consulte Registrar una instancia externa en un clúster en la documentación de Amazon ECS. Si tiene algún problema, consulte la sección Solución de problemas.	

Tarea	Descripción	Habilidades requeridas
Compruebe el estado de Amazon ECS Anywhere y de la máquina virtual externa.	Para comprobar si su máquina virtual está conectada al plano de control de Amazon ECS y en funcionamiento, ejecute los siguientes comandos. `$aws ssm describe-instance-information` `$aws ecs list-container-instances --cluster $CLUSTER_NAME`	DevOps ingeniero

Implemente el proceso de CI/CD

Tarea	Descripción	Habilidades requeridas
Crea una rama en el CodeCommit repositorio.	Crea una rama con un nombre `main` en el CodeCommit repositorio creando la primera confirmación para el repositorio. Puede seguir la documentación de AWS para crear una confirmación CodeCommit. El siguiente comando es un ejemplo. `aws codecommit put-file \ --repository-name EcsAnywhereRepo \ --branch-name main \ --file-path README.md \ --file-content "Test" \ --name "Dev Ops" \`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`--email "devops@example.com" \ --commit-message "Adding README."`	
Configure la replicación de repositorios.	Puede duplicar un GitLab repositorio desde y hacia fuentes externas. Puede seleccionar qué repositorio servirá como origen. Las ramificaciones, las etiquetas y las confirmaciones se sincronizan automáticamente. Configura una réplica automática entre el GitLab repositorio que aloja tu aplicación y el CodeCommit repositorio. Para obtener instrucciones, consulte Configurar una réplica push de GitLab a CodeCommit (GitLab documentación). Nota: De forma predeterminada, la replicación sincroniza automáticamente el repositorio. Si desea actualizar manualmente los repositorios, consulte Actualizar una réplica (GitLab documentación).	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Implemente la pila proceso de CI/CD.	Implementar la pila de `EcsAnywherePipelineStack` introduciendo el siguiente comando. `$cdk deploy EcsAnywherePipelineStack`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Pruebe el proceso de CI/CD.	1. Realice cambios en el código de la aplicación y envíelo al GitLab repositorio local de origen. Para obtener más información, consulte Opciones de inserción (GitLab documentación). Por ejemplo, edite el archivo `../application/index.html` para actualizar el valor de versión de la aplicación. 2. Cuando el código se replica en el CodeCommit repositorio, se inicia la canalización de CI/CD. Realice una de las acciones siguientes: • Si utilizas la duplicación automática para sincronizar el repositorio con el GitLab repositorio, continúa con el CodeCommit siguiente paso. • Si utiliza la duplicación manual, inserte los cambios en el código de la aplicación en el CodeCommit repositorio siguiendo las instrucciones de Actualizar una réplica (documentación). GitLab	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	3. En su máquina local, abra un navegador web y acceda a http://localhost:80. Se abrirá la página web de NGINX, ya que el puerto 80 se reenvía a localhost en Vagrantfile. Confirme que puede ver el valor de la versión actualizada de la aplicación. Este paso valida la implementación del proceso y la imagen. 4. (Opcional) Si desea verificar la implementación en la consola de administración de AWS, haga lo siguiente: a. Abra la consola de Amazon ECS en https://console.aws.amazon.com/ecs/. b. En la barra de navegación, seleccione la región a utilizar. c. En el panel de navegación, seleccione Clusters (Clústeres). d. En la página Clústeres, seleccione el clúster. EcsAnywhereCluster e. Elija Definiciones de tareas.	

Tarea	Descripción	Habilidades requeridas
	f. Confirme que el contenedor se está ejecutando.	

Limpieza

Tarea	Descripción	Habilidades requeridas
Limpie y elimine los recursos.	Después de seguir este patrón, debe eliminar los proof-of-concept recursos que ha creado. Para limpiar, introduzca los siguientes comandos. `$cdk destroy EcsAnywherePipelineStack` `$cdk destroy EcsAnywhereInfraStack`	DevOps ingeniero

Solución de problemas

Problema	Solución
Errores relacionados con la falta de paquetes al instalar dependencias de paquetes.	Ejecute uno de los siguientes comandos para resolver los paquetes que faltan. `$npm ci` o `$npm install -g @aws-cdk/<package_name>`

Problema	Solución
Al ejecutar el comando `aws ssm create-activation` en la máquina virtual, recibe el siguiente error. `An error occurred (ValidationException) when calling the CreateActivation operation: Nonexistent role or missing ssm service principal in trust policy: arn:aws:iam::000000000000:role/EcsAnywhereInstanceRole`	La pila `EcsAnywhereInfraStack` no se ha implementado por completo, y el rol de IAM necesario para ejecutar este comando no se ha creado todavía. Comprueba el estado de la pila en la CloudFormation consola. Vuelva a intentar el comando después de que el estado cambie a `CREATE_COMPLETE`.
La comprobación de estado de Amazon ECS devuelve el resultado `UNHEALTHY`, y aparece el siguiente error en la sección Servicios del clúster en la consola de Amazon ECS. `service EcsAnywhereService was unable to place a task because no container instance met all of its requirements. Reason: No Container Instances were found in your cluster.`	Reinicie el agente de Amazon ECS en su máquina virtual de Vagrant ejecutando los siguientes comandos. `$vagrant ssh` `$sudo systemctl restart ecs` `$sudo systemctl status ecs`

Recursos relacionados

- Página de marketing de Amazon ECS Anywhere
- Documentación de Amazon ECS Anywhere
- Demostración de Amazon ECS Anywhere (video)
- Muestras de talleres de Amazon ECS Anywhere (GitHub)
- Duplicación de repositorios (documentación) GitLab

Más patrones

- Automatice la configuración del emparejamiento entre regiones con AWS Transit Gateway
- Gestión de las aplicaciones de contenedores en las instalaciones mediante la configuración de Amazon ECS Anywhere con AWS CDK
- Migre los datos de Hadoop a Amazon S3 mediante WanDisco Migrator LiveData
- Migración de las máquinas virtuales de VMware con HCX Automation mediante PowerCLI
- Migración de las cargas de trabajo a VMware Cloud en AWS mediante VMware HCX
- Modificar los encabezados HTTP al migrar de F5 a un equilibrador de carga de aplicación en AWS
- ???
- Utilice las consultas de BMC Discovery para extraer datos de migración para planificar la migración
- Use Serverspec para desarrollar código de infraestructura basado en pruebas

infraestructura

Temas

- Acceder a un host bastión mediante Session Manager y Amazon EC2 Instance Connect
- Centralice la resolución de DNS con AWS Managed Microsoft AD y Microsoft Active Directory en las instalaciones
- Centralice la supervisión mediante Amazon CloudWatch Observability Access Manager
- Compruebe las instancias EC2 para ver si hay etiquetas obligatorias en el lanzamiento
- Conectarse a una instancia de Amazon EC2 mediante el uso de Session Manager
- Cree una canalización en las regiones de AWS que no sean compatibles con AWS CodePipeline
- Implementar un clúster de Cassandra en Amazon EC2 con IP estáticas privadas para evitar el reequilibrio
- Amplíe las VRF a AWS mediante AWS Transit Gateway Connect
- Reciba notificaciones de Amazon SNS cuando cambie el estado de clave de una clave de AWS KMS
- Modernización del mainframe: DevOps en AWS con Micro Focus
- Preserve el espacio IP enrutable en los diseños de VPC de varias cuentas para subredes que no son de carga de trabajo
- Aprovisione un producto Terraform en AWS Service Catalog mediante un repositorio de código
- Registre varias cuentas de AWS con una sola dirección de correo electrónico mediante Amazon SES
- Configure la resolución de DNS para redes híbridas en un entorno de AWS de varias cuentas
- Configure la resolución de DNS para redes híbridas en un entorno de AWS de una sola cuenta
- Configure automáticamente los bots de UiPath RPA en Amazon EC2 mediante AWS CloudFormation
- Configure la recuperación ante desastres para Oracle JD Edwards EnterpriseOne con AWS Elastic Disaster Recovery
- Sincronice los datos entre los sistemas de archivos de Amazon EFS en distintas regiones de AWS mediante AWS DataSync
- Actualizar los clústeres de SAP Pacemaker de ENSA1 a ENSA2
- Utilice zonas de disponibilidad coherentes en las VPC en diferentes cuentas de AWS

- Validar Account Factory para el código Terraform (AFT) localmente
- Más patrones

Acceder a un host bastión mediante Session Manager y Amazon EC2 Instance Connect

Creado por Piotr Chotkowski (AWS) y Witold Kowalik (AWS)

Repositorio de código: acceda a un host bastión mediante Session Manager y Amazon EC2 Instance Connect	Entorno: PoC o piloto	Tecnologías: Infraestructura; nativo en la nube; seguridad, identidad, conformidad; redes
Servicios de AWS: Amazon EC2; AWS Systems Manager; Amazon VPC		

Resumen

Un host bastión, también denominado jump box, es un servidor que proporciona un único punto de acceso desde una red externa a los recursos ubicados en una red privada. Un servidor expuesto a una red pública externa, como Internet, supone un posible riesgo de seguridad en caso de acceso no autorizado. Es importante proteger y controlar el acceso a estos servidores.

Este patrón describe cómo puede utilizar Session Manager y Amazon EC2 Instance Connect para conectarse de forma segura a un host bastión de Amazon Elastic Compute Cloud (Amazon EC2) implementado en su cuenta de AWS. Session Manager es una funcionalidad de AWS Systems Manager. Las ventajas de este patrón incluyen:

- El host bastión implementado no tiene ningún puerto de entrada abierto expuesto a la Internet pública. Esto reduce la posible superficie expuesta a ataques.
- No necesita almacenar ni mantener las claves de Secure Shell (SSH) a largo plazo en su cuenta de AWS. En su lugar, cada usuario genera un nuevo par de claves SSH cada vez que se conecta al host bastión. Las políticas de AWS Identity and Access Management (IAM) adjuntas a las credenciales del usuario de AWS controlan el acceso al host bastión.

Destinatarios previstos

Este patrón está pensado para lectores que tienen experiencia con conocimientos básicos de Amazon EC2, la nube privada virtual (VPC) de Amazon y Hashicorp Terraform.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Interfaz de la línea de comandos de AWS (AWS CLI) versión 2, instalada y configurada
- Plugin de Session Manager para la CLI de AWS, instalado
- CLI de Terraform, instalada
- Almacenamiento para el estado de Terraform, como un bucket de Amazon Simple Storage Service (Amazon S3) y una tabla de Amazon DynamoDB que sirven como un backend remoto para almacenar el estado de Terraform. Para obtener más información sobre el uso de backends remotos para el estado de Terraform, consulte los backends de S3 (documentación de Terraform). Para ver un ejemplo de código que configura la administración remota del estado con un backend de S3, consulte remote-state-s3-backend (Terraform Registry). Tenga en cuenta los siguientes requisitos:
  - El bucket de S3 y la tabla de DynamoDB deben estar en la misma región de AWS.
  - Al crear la tabla de DynamoDB, la clave de partición debe ser `LockID` (distingue entre mayúsculas y minúsculas) y el tipo de clave de partición debe ser `String`. Todos los demás valores de la tabla deben estar en sus valores predeterminados. Para obtener más información, consulte Acerca de las claves principales y Crear una tabla en la documentación de DynamoDB.
- Un cliente SSH, instalado.

Limitaciones

- Este patrón pretende ser una prueba de concepto (PoC) o una base para un mayor desarrollo. No debe utilizarse en su forma actual en entornos de producción. Antes de la implementación, ajuste el código de muestra del repositorio para que se adapte a sus requisitos y a su caso de uso.
- Este patrón supone que el host bastión de destino utiliza Amazon Linux 2 como sistema operativo. Si bien es posible utilizar otras imágenes de máquina de Amazon (AMI), otros sistemas operativos están fuera del ámbito de aplicación de este patrón.
- En este patrón, el host bastión está ubicado en una subred privada sin una puerta de enlace NAT ni una puerta de enlace de Internet. Este diseño aísla la instancia EC2 de Internet pública.

Puede añadir una configuración de red específica que le permita comunicarse con Internet. Para obtener más información, consulte Conectar su nube privada virtual (VPC) a otras redes en la documentación de Aamazon VPC. Del mismo modo, siguiendo el principio de privilegio mínimo, el host bastión no tiene acceso a ningún otro recurso de su cuenta de AWS a menos que usted conceda permisos de forma explícita. Para más información, consulte Políticas basadas en recursos en la documentación de IAM.

Versiones de producto

- CLI de AWS versión 2
- Terraform versión 1.3.9

Arquitectura

Pila de tecnología de destino

- Una VPC con una única subred privada
- Los siguientes puntos de conexión de VPC de interfaz:
  - `amazonaws.<region>.ssm`: el punto de conexión para el servicio de Systems Manager.
  - `amazonaws.<region>.ec2messages`: Systems Manager utiliza este punto de conexión para realizar llamadas desde SSM Agent al servicio de Systems Manager.
  - `amazonaws.<region>.ssmmessages` – Session Manager utiliza este punto de conexión para conectarse a la instancia EC2 a través de un canal de datos seguro.
- Una instancia `t3.nano` de EC2 que ejecute Amazon Linux 2.
- Rol de IAM y perfil de instancia
- Grupos de seguridad de Amazon VPC y reglas de grupos de seguridad para los puntos de conexión y la instancia EC2

Arquitectura de destino

El diagrama muestra el proceso siguiente:

1. El usuario asume un rol de IAM que tiene permisos para hacer lo siguiente:
   - Autenticar, autorizar y conectarse a la instancia EC2

- Iniciar una sesión con Session Manager

2. El usuario inicia una sesión SSH a través de Session Manager.
3. Session Manager autentica al usuario, verifica los permisos de las políticas de IAM asociadas, comprueba los ajustes de configuración y envía un mensaje al agente SSM para abrir una conexión bidireccional.
4. El usuario envía la clave pública SSH al host bastión mediante los metadatos de Amazon EC2. Esto debe hacerse antes de cada conexión. La clave pública SSH permanece disponible durante 60 segundos.
5. El host bastión se comunica con los puntos de conexión de VPC de la interfaz para Systems Manager y Amazon EC2.
6. El usuario accede al host bastión a través de Session Manager mediante un canal de comunicación bidireccional cifrado con TLS 1.2.

Automatizar y escalar

Las siguientes opciones están disponibles para automatizar la implementación o escalar esta arquitectura:

- Puede implementar la arquitectura mediante una canalización de integración y entrega continuas (CI/CD).
- Puede modificar el código para cambiar el tipo de instancia del host bastión.
- Puede modificar el código para implementar varios hosts bastión. En el archivo `bastion-host/main.tf`, en el bloque de recursos `aws_instance`, añada el meta argumento `count`. Para obtener más información, consulte la documentación de Terraform.

Herramientas

Servicios de AWS

- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.

- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Systems Manager le permite administrar las aplicaciones y la infraestructura que se ejecutan en la nube de AWS. Simplifica la administración de aplicaciones y recursos, reduce el tiempo requerido para detectar y resolver problemas operativos y ayuda a utilizar y administrar los recursos de AWS a escala de manera segura. Este patrón utiliza Session Manager, una capacidad de Systems Manager.
- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esta red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Otras herramientas

- HashiCorp Terraform es una herramienta de código abierto de infraestructura como código (IaC) que le ayuda a usar el código para aprovisionar y administrar la infraestructura y los recursos de la nube. Este patrón usa Terraform CLI.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub Access a bastion host mediante Session Manager y Amazon EC2 Instance Connect.

Prácticas recomendadas

- Recomendamos usar herramientas de escaneo de código automatizadas para mejorar la seguridad y la calidad del código. Este patrón se escaneó con Checkov, una herramienta de análisis de código estático para IaC. Como mínimo, le recomendamos que realice comprobaciones básicas de validación y formato mediante los comandos `terraform validate` y `terraform fmt -check -recursive` de Terraform.
- Es una buena práctica añadir pruebas automatizadas para la iAC. Para obtener más información sobre los diferentes enfoques para probar el código de Terraform, consulte Testing Terraform (entrada del blog de HashiCorp Terraform).
- Durante la implementación, Terraform utiliza la instancia EC2 que reemplaza cada vez que se detecta una nueva versión de la AMI de Amazon Linux 2. Esto implementa la nueva versión del sistema operativo, que incluye los parches y las actualizaciones. Si el programa de implementación no es frecuente, esto puede suponer un riesgo para la seguridad, ya que la instancia no tiene los

parches actualizados. Es importante actualizar y aplicar con frecuencia los parches de seguridad a las instancias EC2 implementadas. Para obtener más información, consulte Actualizar la gestión en Amazon EC2.

- Como este patrón es una prueba de concepto, utiliza políticas administradas de AWS, como `AmazonSSMManagedInstanceCore`. Las políticas administradas de AWS cubren casos de uso comunes, pero no conceden permisos de privilegios mínimos. Según sea necesario en su caso, le recomendamos que cree políticas personalizadas que concedan permisos con privilegios mínimos para los recursos implementados en esta arquitectura. Para más información, consulte Introducción a las políticas administradas de AWS y el objetivo de los permisos de privilegios mínimos.
- Use una contraseña para proteger el acceso a las claves SSH y guarde las claves en un lugar seguro.
- Configure el registro y la supervisión del host bastión. El registro y la supervisión son partes importantes del mantenimiento de los sistemas, tanto desde una perspectiva operativa como de seguridad. Existen varias formas de supervisar las conexiones y la actividad en su host bastión. Para obtener más información, consulte los siguientes temas en la documentación de Systems Manager.
  - Supervisión de AWS Systems Manager
  - Registro y supervisión en AWS Systems Manager
  - Auditoría de la actividad de sesiones
  - Registro de la actividad de la sesión

Epics

Implementación de recursos

Tarea	Descripción	Habilidades requeridas
Clone el repositorio de código.	1. En una interfaz de la línea de comandos, cambie el directorio de trabajo a la ubicación en la que desee almacenar los archivos de muestra.	DevOps ingeniero, desarroll ador

Tarea	Descripción	Habilidades requeridas
	2. Escriba el siguiente comando. `git clone https://github.com/aws-samples/secured-bastion-host-terraform.git`	

Tarea	Descripción	Habilidades requeridas
Inicialice el directorio de trabajo de Terraform.	Este paso solo es necesario para la primera implement ación. Si va a realizar una reimplementación del patrón, vaya al paso siguiente. En el directorio raíz del repositorio clonado, introduzca el siguiente comando, donde: • `$S3_STATE_BUCKET` es el nombre del bucket de S3 que contiene el estado de Terraform • `$PATH_TO_STATE_FIL E` es la clave del archivo de estado de Terraform, como `infra/bastion-host/ tetfstate` • `$AWS_REGION` es la Región donde se despliega el bucket de S3 `terraform init \ -backend-config="b ucket=$S3_STATE_BU CKET" \ -backend-config="k ey=$PATH_TO_STATE_ FILE" \ -backend-config="r egion=$AWS_REGION` Nota: También puede abrir el archivo config.tf y, en	DevOps ingeniero, desarroll ador, Terraform

Tarea	Descripción	Habilidades requeridas
	la sección `terraform` , proporcionar estos valores manualmente.	
Implementación de recursos.	1. En el directorio raíz del repositorio clonado, introduzca el siguiente comando. `terraform apply -var-file="dev.tfvars"` 2. Revise la lista de todos los cambios que se aplicarán a su cuenta de AWS y, a continuación, confirme la implementación. 3. Espere a que se implement en todos los recursos.	DevOps ingeniero, desarroll ador, Terraform

Configurar el entorno local

Tarea	Descripción	Habilidades requeridas
Configure la conexión SSH.	Actualice el archivo de configuración de SSH para permitir las conexiones SSH a través de Session Manager. Para obtener instrucciones, consulte Permitir conexiones SSH para Session Manager. Esto permite a los usuarios autorizados introducir un comando proxy que inicia una sesión de Session Manager	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	y transfiere todos los datos a través de una conexión bidireccional.	
Genere las claves SSH.	Introduzca el siguiente comando para general un par de claves de SSH locales privadas y publicas. Use este par de claves para conectarse al host bastión. `ssh-keygen -t rsa -f my_key`	DevOps ingeniero, desarrollador

Conectarse al host bastión mediante Session Manager

Tarea	Descripción	Habilidades requeridas
Obtenga el ID de la instancia.	1. Para conectarse al host bastión implementado, necesita el ID de la instancia de EC2. Realice una de las siguientes acciones para localizar la ID: • Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/. En el panel de navegación, seleccione Instancias. Localice la instancia del host bastión. • En la AWS CLI, ingrese el comando siguiente.	AWS general

Tarea	Descripción	Habilidades requeridas
	`aws ec2 describe-instances` Para filtrar los resultados, introduzca el siguiente comando, donde `$BASTION_HOST_TAG` es la etiqueta que asignó al host bastión. El valor predeterminado para esta etiqueta es `sandbox-dev-bastion-host` . `aws ec2 describe-instances \ --filters "Name=tag:Name,Values=$BASTION_HOST_TAG" \ --output text \ --query 'Reservations[*].Instances[*].InstanceId' \ --output text` 2. Copie el ID de la instancia EC2. Usará este ID más tarde.	

Tarea	Descripción	Habilidades requeridas
Envíe la clave pública SSH.	Nota: En esta sección, debe cargar la clave pública en los metadatos de la instancia del host bastión. Una vez cargada la clave, dispone de 60 segundos para iniciar una conexión con el host bastión. Transcurridos 60 segundos, se elimina la clave pública. Para obtener más información, consulte la sección Solución de problemas de este patrón. Complete los siguientes pasos rápidamente para evitar que se extraiga la clave antes de conectarse al host bastión. 1. Envíe la clave SSH al host bastión mediante EC2 Instance Connect. Escriba el siguiente comando, cuando: • `$INSTANCE_ID` es el ID de la instancia EC2. • `$PUBLIC_KEY_FILE` es la ruta al archivo de claves públicas, como `my_key.pub` Importante: Asegúrese de usar la clave pública y no la clave privada.	AWS general

Tarea	Descripción	Habilidades requeridas
	`` aws ec2-instance- connect send-ssh- public-key \ --instance-id $INSTANCE_ID \ --instance-os- user ec2-user \ --ssh-public-key file://$PUBLIC_KEY _FILE ``` 2. Espere hasta que reciba un mensaje que indique que la clave se ha cargado correctamente. Continúe inmediatamente al siguiente paso.	

Tarea	Descripción	Habilidades requeridas
Conéctese al host bastión.	1. Por ejemplo, introduzca el siguiente comando para conectarse al host bastión a través de Session Manager, donde: • `$PRIVATE_KEY_FILE` es la ruta a su clave privada, como `my_key` • `$INSTANCE_ID` es el ID de la instancia EC2. `ssh -i $PRIVATE_KEY_FILE ec2-user@$INSTANCE_ID` 2. Confirme la conexión introduciendo `yes`. Esto abre una conexión SSH mediante Session Manager. Nota: Existen otras opciones para abrir una conexión SSH con el host bastión. Para obtener más información, consulte Enfoques alternativos para establecer una conexión SSH con el host bastión en la sección de Información adicional de este patrón.	AWS general

(Opcional) Limpieza

Tarea	Descripción	Habilidades requeridas
Elimine los recursos implementados.	1. Para eliminar todos los recursos implement ados, ejecute el siguiente comando del directorio raíz del repositorio clonado. `terraform destroy -var-file="dev.tfvars"` 2. Confirme la eliminación de los recursos.	DevOps ingeniero, desarroll ador, Terraform

Solución de problemas

Problema	Solución
`TargetNotConnected` error al intentar conectarse al host bastión	1. Reinicie el host bastión según las instrucci ones de Reiniciar la instancia en la documentación de Amazon EC2. 2. Cuando la instancia se haya reiniciado correctamente, vuelva a enviar la clave pública al host bastión y vuelva a intentar la conexión.
`Permission denied` error al intentar conectarse al host bastión	Una vez cargada la clave pública en el host bastión, solo dispondrá de 60 segundos para iniciar la conexión. Transcurridos 60 segundos, la clave se elimina automáticamente y no puede usarla para conectarse a la instancia. Si esto ocurre, puede repetir el paso para volver a enviar la clave a la instancia.

Recursos relacionados

Documentación de AWS

- Administrador de sesiones de AWS Systems Manager (documentación de Systems Manager)
- Instalar el plugin de Session Manager para la CLI de AWS (documentación de Systems Manager)
- Permitir conexiones SSH para Session Manager (documentación de Systems Manager)
- Acerca del uso de EC2 Instance Connect (documentación de Amazon EC2)
- Conexión mediante la instancia EC2 (documentación de Amazon EC2)
- Gestión de identidad y acceso para Amazon EC2 (documentación de Amazon EC2)
- Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 (documentación de IAM)
- Prácticas recomendadas de seguridad en IAM (documentación de IAM)
- Control del tráfico hacia los recursos mediante grupos de seguridad (documentación de Amazon VPC)

Otros recursos

- Página web para desarrolladores de Terraform
- Comando: validar (documentación de Terraform)
- Comando: fmt (documentación de Terraform)
- Probando HashiCorp Terraform (HashiCorp entrada de blog)
- Página web Checkov

Información adicional

Enfoques alternativos para establecer una conexión SSH con el host bastión

Enrutamiento de puertos

Puede usar la opción `-D 8888` para abrir una conexión SSH con reenvío dinámico de puertos. Para obtener más información, consulte estas instrucciones en explainshell.com. El siguiente es un ejemplo de un comando para abrir una conexión SSH mediante el reenvío de puertos.

```
ssh -i $PRIVATE_KEY_FILE -D 8888 ec2-user@$INSTANCE_ID
```

Este tipo de conexión abre un proxy SOCKS que puede reenviar el tráfico de su navegador local a través del host bastión. Si utiliza Linux o macOS, para ver todas las opciones, introduzca `man ssh`. Se mostrará el manual de referencia de SSH.

Uso del script proporcionado

En lugar de ejecutar manualmente los pasos descritos en Conectar al host bastión mediante Session Manager en la sección Epics, puede utilizar el script connect.sh incluido en el repositorio de código. Este script genera el par de claves SSH, envía la clave pública a la instancia EC2 e inicia una conexión con el host bastión. Al ejecutar el script, se pasan la etiqueta y el nombre de la clave como argumentos. A continuación se muestra un ejemplo del comando para ejecutar el script.

```
./connect.sh sandbox-dev-bastion-host my_key
```

Centralice la resolución de DNS con AWS Managed Microsoft AD y Microsoft Active Directory en las instalaciones

Creado por Brian Westmoreland (AWS)

Entorno: producción	Tecnologías: infraestructura; redes DevOps; seguridad , identidad y cumplimiento; sistemas operativos	Carga de trabajo: Microsoft
Servicios de AWS: AWS Managed Microsoft AD; Amazon Route 53; AWS RAM; AWS Directory Service; AWS Organizations; AWS Direct Connect; AWS CLI		

Resumen

Este patrón proporciona instrucciones para centralizar la resolución del sistema de nombres de dominio (DNS) en un entorno multicuenta de AWS mediante AWS Directory Service para Microsoft Active Directory (AWS Managed Microsoft AD). En este patrón, el espacio de nombres DNS de AWS es un subdominio del espacio de nombres DNS en las instalaciones. Este patrón también proporciona instrucciones para configurar los servidores DNS en las instalaciones de modo que reenvíen consultas a AWS cuando la solución DNS local use Microsoft Active Directory.

Requisitos previos y limitaciones

Requisitos previos

- Un entorno multicuenta de AWS configurado mediante AWS Organizations.
- Conectividad de red establecida entre cuentas de AWS.
- Conectividad de red establecida entre AWS y el entorno en las instalaciones (mediante AWS Direct Connect o cualquier tipo de conexión VPN).
- Interfaz de la línea de comandos de AWS (AWS CLI) configurada en un equipo de trabajo local.

- AWS Resource Access Manager (AWS RAM) se usa para compartir reglas de Amazon Route 53 entre cuentas. Por lo tanto, el uso compartido debe estar habilitado en el entorno de AWS Organizations, tal y como se describe en la sección Epics.

Limitaciones

- La edición Standard de AWS Managed Microsoft AD tiene un límite de 5 acciones.
- Microsoft AD Enterprise Edition administrado por AWS tiene un límite de 125 acciones.
- La solución de este patrón se limita a las regiones de AWS que admiten uso compartido a través de AWS RAM.

Versiones de producto

- Microsoft Active Directory ejecutado en Windows Server 2008, 2012 R2 o 2016

Arquitectura

Arquitectura de destino

En este diseño, AWS Managed Microsoft AD se instala en la cuenta de AWS de servicios compartidos. Si bien no es un requisito, este patrón presupone dicha configuración. Si configura AWS Managed Microsoft AD en una cuenta de AWS diferente, es posible que tenga que modificar los pasos de la sección Epics en consecuencia.

Este diseño emplea Route 53 Resolvers para admitir la resolución de nombres mediante el uso de reglas de Route 53. Si la solución de DNS en las instalaciones usa Microsoft DNS, no es fácil crear una regla de reenvío condicional para el espacio de nombres de AWS (`aws.company.com`), que es un subdominio del espacio de nombres DNS (`company.com`) de la empresa. Si intenta crear un reenviador condicional tradicional, se producirá un error. Esto se debe a que Microsoft Active Directory ya se considera autorizado para cualquier subdominio de `company.com`. Para evitar este error, primero debe crear una delegación para `aws.company.com` que permita delegar la autoridad de ese espacio de nombres. A continuación, puede crear el reenviador condicional.

La nube privada virtual (VPC) de cada cuenta radial puede tener su propio espacio de nombres DNS único basado en el espacio de nombres raíz de AWS. En este diseño, cada cuenta radial añade una abreviatura del nombre de cuenta al espacio de nombres base de AWS. Una vez creadas las zonas

alojadas privadas en la cuenta radial, estas zonas se asocian a la VPC de la cuenta radial y a la VPC de la cuenta de red central de AWS. Esto permite que la cuenta de red central de AWS responda a las consultas de DNS relacionadas con las cuentas radiales.

Automatizar y escalar

Este diseño emplea los puntos de conexión de Route 53 Resolver para escalar las consultas de DNS entre AWS y su entorno en las instalaciones. Cada punto de conexión de Route 53 Resolver incluye varias interfaces de red elásticas (distribuidas en varias zonas de disponibilidad), y cada interfaz de red puede gestionar hasta 10 000 consultas por segundo. Route 53 Resolver admite hasta 6 direcciones IP por punto de conexión, por lo que, en total, este diseño admite hasta 60 000 consultas de DNS por segundo distribuidas en varias zonas de disponibilidad para lograr una alta disponibilidad.

Además, este patrón tiene en cuenta automáticamente el crecimiento futuro en AWS. No es necesario modificar las reglas de reenvío de DNS configuradas en las instalaciones para admitir las nuevas VPC y las zonas alojadas privadas asociadas que se agreguen a AWS.

Herramientas

Servicios de AWS

- AWS Directory Service para Microsoft Active Directory permite que las cargas de trabajo compatibles con un directorio y los recursos de AWS utilicen Active Directory de Microsoft administrado en la nube de AWS.
- AWS Organizations es un servicio de administración de cuentas que le permite agrupar varias cuentas de AWS en una organización que usted crea y administra de manera centralizada.
- AWS Resource Access Manager (AWS RAM) le ayuda a compartir sus recursos de forma segura entre las cuentas de AWS para reducir los gastos operativos y brindar visibilidad y auditabilidad.
- Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad.

Herramientas

- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos. En este patrón, la CLI de AWS se usa para configurar las autorizaciones de Route 53.

Epics

Crear y compartir un directorio Microsoft AD administrado por AWS

Tarea	Descripción	Habilidades requeridas
Implemente AWS Managed Microsoft AD.	1. Crear y configurar un nuevo directorio. Para más detalles sobre cómo hacerlo, consulte Crear su directorio de AWS Managed Microsoft AD en la Guía de administración de AWS Directory Service. 2. Registre las direccion es IP de los controlad ores de dominio de AWS Managed Microsoft AD. Se emplearán en un paso posterior.	Administrador de AWS
Compartir el directorio.	Una vez creado el directorio, compártalo con otras cuentas de AWS de la organizac ión de AWS. Para obtener más instrucciones, consulte Compartir su directorio en la Guía de administración de AWS Directory Service. Nota: La edición Standard de AWS Managed Microsoft AD tiene un límite de 5 acciones. La edición Enterprise tiene un límite de 125 acciones.	Administrador de AWS

Configure Route 53

Tarea	Descripción	Habilidades requeridas
Cree Route 53 Resolvers.	Los Route 53 Resolvers facilitan la resolución de las consultas de DNS entre AWS y el centro de datos en las instalaciones. 1. Instale Route 53 Resolvers siguiendo las instrucciones de la Guía del desarrollador de Route 53. 2. Configure Route 53 Resolvers en subredes privadas de, al menos, dos zonas de disponibilidad en la VPC de la cuenta de red central de AWS para obtener una alta disponibilidad. Nota: Aunque el uso de la VPC de la cuenta de red central de AWS no es obligatorio, en los pasos restantes se presupone esta configuración.	Administrador de AWS
Cree reglas de Route 53.	Es posible que su caso de uso específico requiera una gran cantidad de reglas de Route 53, pero tendrá que configurar las siguientes reglas como base:	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	• Una regla de salida para el espacio de nombres en las instalaciones (`company.com`) mediante Resolvers salientes de Route 53. • Comparta esta regla con las cuentas de AWS radiales. • Asocie esta regla a las VPC de cuentas radiales. • Una regla de salida para el espacio de nombres de AWS (`aws.company.com`) que apunta a la cuenta de red central Route 53 Inbound Resolvers. • Comparta esta regla con las cuentas de AWS radiales. • Asocie la regla a las VPC de cuentas radiales. • No asocie esta regla a la VPC de la cuenta de red central de AWS (que alberga Route 53 Resolvers). • Una segunda regla saliente para el espacio de nombres de AWS (`aws.company.com`) que apunta a los controladores de dominio de Microsoft AD gestionados	

Tarea	Descripción	Habilidades requeridas
	por AWS (utilice las IP de la epopeya anterior). • Asocie esta regla a la VPC de la cuenta de red central de AWS (que alberga Route 53 Resolvers). • No comparta ni asocie esta regla con otras cuentas de AWS. Para más información, consulte Gestión de reglas de reenvío en la Guía del desarrollador de Route 53.	

Configure el DNS de Active Directory en las instalaciones

Tarea	Descripción	Habilidades requeridas
Cree la delegación.	Use el complemento DNS de Microsoft (`dnsmgmt.msc`) para crear una nueva delegación para el espacio de nombres `company.com` de Active Directory. El nombre del dominio delegado debe ser `aws`. Esto lo convierte en el nombre completo del dominio (FQDN) de la delegación `aws.company.com`. En los servidores de nombres, use las direcciones IP de	Active Directory

Tarea	Descripción	Habilidades requeridas
	los Resolvers entrantes de Route 53 de AWS en la cuenta DNS central de AWS para los valores de IP y use `server.aws.company.com` para el nombre.	
Cree el reenviador condicional.	Use el complemento DNS de Microsoft (`dnsmgmt.msc`) para crear un nuevo reenviador condicional para `aws.company.com`. Use las direcciones IP de los controladores de dominio de AWS Managed Microsoft AD para el destino del reenviador condicional.	Active Directory

Cree zonas alojadas privadas de Route 53 para cuentas de AWS radiales

Tarea	Descripción	Habilidades requeridas
Cree las zonas alojadas privadas de Route 53.	Crear una zona alojada privada de Route 53 en cada cuenta radial. Asocie esta zona alojada privada con la VPC de la cuenta radial. Para ver los pasos detallados, consulte Crear una zona alojada privada en la Guía del desarrollador de Route 53.	Administrador de AWS
Cree autorizaciones.	Use la CLI de AWS para crear una autorización para la VPC de la cuenta de red de AWS central. Ejecute este comando	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	desde el contexto de cada cuenta de AWS radial: `aws route53 create-vpc-association-authorization --hosted-zone-id <hosted-zone-id> \ --vpc VPCRegion=<region>,VPCId=<vpc-id>` donde: • `<hosted-zone-id>` es la zona alojada privada de Route 53 en la cuenta radial. • `<region>` y `<vpc-id>` son la región de AWS y la ID de la VPC de la cuenta de red central de AWS.	

Tarea	Descripción	Habilidades requeridas
Cree asociaciones.	Cree la asociación de zonas alojadas privadas de Route 53 para la VPC de la cuenta de red central de AWS mediante la CLI de AWS. Ejecute este comando desde el contexto de la cuenta de red central de AWS: `aws route53 associate -vpc-with-hosted-zone --hosted-zone-id <hosted-zone-id> \ --vpc VPCRegion=<region>,VPCId=<vpc-id>` donde: • `<hosted-zone-id>` es la zona alojada privada de Route 53 en la cuenta radial. • `<region>` y `<vpc-id>` son la región de AWS y la ID de la VPC de la cuenta de red central de AWS.	Administrador de AWS

Recursos relacionados

- Simplifique la administración de DNS en un entorno multicuenta con Route 53 Resolver (publicación del blog de AWS de Mahmoud Matouk)
- Creación de un directorio con AWS Managed Microsoft AD (documentación de AWS Directory Service)

- Compartir un directorio con AWS Managed Microsoft AD (documentación de AWS Directory Service)
- Instalación de Route 53 Resolver (documentación de Amazon Route 53)
- Creación de una zona alojada privada en Route 53 (documentación de Amazon Route 53)

Centralice la supervisión mediante Amazon CloudWatch Observability Access Manager

Creado por Anand Krishna Varanasi (AWS), Jimmy Morgan (AWS), Ashish Kumar (AWS), Balaji Vedagiri (AWS), JAGDISH KOMAKULA (AWS), Sarat Chandra Pothula (AWS) y Vivek Thangamuthu (AWS)

cloudwatch-obervability-access-managerRepositorio de código: -terraform	Entorno: producción	Tecnologías: infraestructura, estrategia de varias cuentas, operaciones
Servicios de AWS: Amazon CloudWatch; Amazon CloudWatch Logs		

Resumen

La observabilidad es fundamental para la supervisión, la comprensión y la solución de problemas de las aplicaciones. Las aplicaciones que abarcan varias cuentas, como las implementaciones de AWS Control Tower o zona de aterrizaje, generan una gran cantidad de registros y datos de rastreo. Para solucionar problemas rápidamente o comprender los análisis de usuarios o empresariales, necesita una plataforma de observabilidad común en todas las cuentas. El Amazon CloudWatch Observability Access Manager le permite acceder a varios registros de cuentas y controlarlos desde una ubicación central.

Puede usar Observability Access Manager para ver y administrar los registros de datos de observabilidad generados por las cuentas de origen. Una cuenta de origen es una cuenta individual de AWS que genera datos de observabilidad para los recursos que residen en ella. Las cuentas de origen comparten sus datos de observabilidad con la cuenta de monitoreo. Los datos de observabilidad compartidos pueden incluir métricas en Amazon CloudWatch, registros en Amazon CloudWatch Logs y trazos en AWS X-Ray. Para más información, consulte la documentación de Observability Access Manager.

Este patrón es para los usuarios que tienen aplicaciones o infraestructuras que se ejecutan en varias cuentas de AWS y necesitan un lugar común para ver los registros. En él se explica cómo puede

configurar Observability Access Manager mediante Terraform para supervisar el estado y el estado de estas aplicaciones o infraestructuras. Puede instalar esta solución de varias maneras:

- Como un módulo de Terraform independiente que se configura manualmente
- Mediante una canalización de integración y entrega continuas (CI/CD)
- Mediante la integración con otras soluciones, como AWS Control Tower Account Factory for Terraform (AFT)

Las instrucciones de la sección Epics tratan sobre la implementación manual. Para ver los pasos de instalación de AFT, consulte el archivo readme del repositorio de GitHub Observability Access Manager.

Requisitos previos y limitaciones

Requisitos previos

- Terraform está instalado o referenciado en su sistema o en canalizaciones automatizadas. (Le recomendamos que utilice la última versión.)
- Una cuenta que puede usar como cuenta de monitoreo central. Otras cuentas crean enlaces a la cuenta de monitoreo central para ver los registros.
- (Opcional) Un repositorio de código fuente como AWS GitHub CodeCommit, Atlassian Bitbucket o un sistema similar. No es necesario disponer de un repositorio de código fuente si utilizas canalizaciones de CI/CD automatizadas.
- (Opcional) Permisos para crear solicitudes de cambios (PR) con el fin de revisar el código y colaborar con él. GitHub

Limitaciones

Observability Access Manager tiene las siguientes Service quotas, que no se pueden cambiar. Tenga en cuenta estas cuotas antes de implementar esta característica. Para obtener más información, consulta las cuotas CloudWatch de servicio en la CloudWatch documentación.

- Vínculos de cuentas de origen: puede vincular cada cuenta de origen a un máximo de cinco cuentas de supervisión.
- Receptores: solo puede usar un receptor por cuenta.

Además:

- Los sumideros y los enlaces deben crearse en la misma región de AWS; no pueden ser interregionales.
- Para el monitoreo entre regiones y cuentas, puede crear CloudWatch paneles de control entre cuentas y regiones para las alarmas y las métricas, excepto para los registros y los rastreos. Otra opción es crear un registro centralizado mediante Amazon OpenSearch Service.

Arquitectura

Componentes

Amazon CloudWatch Observability Access Manager consta de dos componentes principales que permiten la observabilidad entre cuentas:

- Un receptor permite a las cuentas de origen enviar datos de observabilidad a la cuenta de monitoreo central. Básicamente, un receptor proporciona una puerta de enlace a la que se pueden conectar las cuentas de origen. Solo puede haber una puerta de enlace o conexión receptora y varias cuentas pueden conectarse a ella.
- Cada cuenta de origen tiene un enlace al cruce de la puerta de enlace receptora y los datos de observabilidad se envían a través de este enlace. Debe crear un receptor antes de crear enlaces desde cada cuenta de origen.

Arquitectura

El siguiente diagrama ilustra Observability Access Manager y sus componentes.

Herramientas

Servicios de AWS

- Amazon le CloudWatch ayuda a monitorizar las métricas de sus recursos de AWS y las aplicaciones que ejecuta en AWS en tiempo real.
- AWS Organizations es un servicio de administración de cuentas que le permite agrupar varias cuentas de AWS en una organización que usted crea y administra de manera centralizada.

- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.

Herramientas

- Terraform es una herramienta de infraestructura como código (IaC) HashiCorp que le ayuda a crear y administrar recursos locales y en la nube.
- AWS Control Tower Account Factory para Terraform (AFT) configura una canalización de Terraform para ayudarle a aprovisionar y personalizar cuentas en AWS Control Tower. Si lo desea, puede utilizar AFT para configurar Observability Access Manager de forma escalable en varias cuentas.

Repositorio de código

El código de este patrón está disponible en el repositorio de GitHub Observability Access Manager.

Prácticas recomendadas

- En los entornos de AWS Control Tower, marque la cuenta de registro como la cuenta de supervisión central (receptor).
- Si tiene varias organizaciones con varias cuentas en AWS Organizations, le recomendamos que incluya las organizaciones en lugar de las cuentas individuales en la política de configuración. Si tiene un número reducido de cuentas o si las cuentas no forman parte de una organización en la política de configuración de destino, puede optar por incluir cuentas individuales en su lugar.

Epics

Configure el módulo de receptor

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Clona el repositorio de GitHub Observability Access Manager: `git clone https://github.com/aws-samp`	AWS DevOps, administrador de la nube, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	`les/cloudwatch-obe rvability-access-m anager-terraform`	

Tarea	Descripción	Habilidades requeridas
Especifique los valores de las propiedades del módulo receptor.	En el archivo `main.tf` (en la carpeta `deployments/aft-account-customizations/LOGGING/terraform/` del repositorio), especifique los valores de las siguientes propiedades: • `sink_name` : El nombre del CloudWatch fregadero de Amazon. • `allowed_oam_resource_types` : Observability Access Manager admite actualmente CloudWatch métricas, grupos de registros y rastreos de AWS X-Ray. • `allowed_source_accounts` : Las cuentas de origen que pueden enviar registros a la cuenta receptora CloudWatch central. • `allowed_source_organizations` : Las organizaciones de la Torre de Control de origen a las que se les permite enviar registros a la cuenta CloudWatch receptora central.	AWS DevOps, administrador de la nube, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	Para obtener más información, consulte AWS::Oam::Sinkla CloudFormation documenta ción de AWS.	
Instale el módulo receptor.	Exporte las credenciales de la cuenta de AWS que ha seleccionado como cuenta de monitoreo e instale el módulo receptor Observability Access Manager: `Terraform Init` `Terrafom Plan` `Terraform Apply`	AWS DevOps, administrador de la nube, administrador de AWS

Configure el módulo receptor

Tarea	Descripción	Habilidades requeridas
Especifique los valores de las propiedades del módulo de enlace.	En el archivo `main.tf` (en la carpeta `deploymen ts/aft-account-cus tomizations/LOGGIN G/terraform/` del repositorio), especifique los valores de las siguientes propiedades: • `account_label` : utilice uno de los siguientes valores: • `$AccountName` : el nombre de la cuenta.	AWS DevOps, administrador de nube, arquitecto de nube

Tarea	Descripción	Habilidades requeridas
	• `$AccountEmail` : una dirección de correo electrónico única a nivel mundial, que incluye el dominio del correo electrónico (por ejemplo, `hello@example.com`) • `$AccountEmailNoDomain` : una dirección de correo electrónico sin el nombre de dominio. • `allowed_oam_resource_types` : Observability Access Manager admite actualmente CloudWatch métricas, grupos de registros y rastreos de AWS X-Ray. Para obtener más información, consulte AWS::Oam::Link la CloudFormation documentación de AWS.	

Tarea	Descripción	Habilidades requeridas
Instale el módulo de enlace para cuentas individuales.	Exporte las credenciales de las cuentas individuales e instale el módulo de enlace Observability Access Manager: `Terraform Plan` `Terraform Apply` Puede configurar el módulo de enlace de forma individual para cada cuenta o usar AFT para instalar automáticamente este módulo en una gran cantidad de cuentas.	AWS DevOps, administrador de nube, arquitecto de nube

Apruebe sink-to-link las conexiones

Tarea	Descripción	Habilidades requeridas
Verifique el mensaje del estado.	1. Inicie sesión en la cuenta de monitoreo. 2. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/. 3. En el panel de navegación izquierdo, elija Configuración. A la derecha, debería ver el mensaje de estado Supervisar la cuenta con una cuenta	

Tarea	Descripción	Habilidades requeridas
	habilitada con una marca de verificación verde. Esto significa que la cuenta de monitoreo tiene un receptor de Observability Access Manager al que se conectarán los enlaces de otras cuentas.	

Tarea	Descripción	Habilidades requeridas
Apruebe las link-to-sink conexiones.	1. Elija la opción Recursos para vincular cuentas situada debajo del mensaje de estado. La informaci ón confirma que se trata de la cuenta de monitoreo , muestra los datos que se comparten desde las cuentas de origen del inquilino (registros , métricas, rastreos) y muestra la etiqueta de la cuenta como $AccountN ame. Esta pantalla ofrece dos opciones para vincular las cuentas de los inquilinos a la cuenta de monitoreo : aprobación a nivel de organización o aprobació n a nivel de cuenta. Para cada opción, puede elegir entre descargar una CloudFormation plantilla de AWS para la aprobación o aprobar cada cuenta de forma individual. 2. Para simplificar, elija Cualquier cuenta para aprobarla en cada nivel de cuenta. Esta opción proporciona un enlace de aprobación para la cuenta.	AWS DevOps, administrador de nube, arquitecto de nube

Tarea	Descripción	Habilidades requeridas
	3. Seleccione Copiar URL para copiar el enlace. 4. Inicie sesión en cada cuenta de origen. 5. En una ventana del navegador, pegue el enlace y seleccione Aprobar enlace conectar con el receptor. 6. Repita la operación para todas las demás cuentas de origen. Para obtener más informaci ón, consulta Cómo vincular las cuentas de monitoreo con las cuentas de origen en la CloudWatch documentación de Amazon.	

Verificar los datos de observabilidad entre cuentas

Tarea	Descripción	Habilidades requeridas
Ver datos entre cuentas.	1. Inicie sesión en la cuenta central de monitoreo. 2. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/. 3. En el panel de navegación izquierdo, elija las opciones para ver los registros, las	AWS DevOps, administrador de nube, arquitecto de nube

Tarea	Descripción	Habilidades requeridas
	métricas y los seguimientos entre cuentas.	

(Opcional) Habilite las cuentas de origen para que confíen en la cuenta de monitoreo

Tarea	Descripción	Habilidades requeridas
Consulte las métricas, los paneles, los registros, los widgets y las alarmas de otras cuentas.	Como función adicional, puede compartir CloudWatch las métricas, los paneles, los registros, los widgets y las alarmas con otras cuentas. Cada cuenta utiliza un rol de IAM denominado CloudWatch: CrossAccountSharingRole para acceder a estos datos. Las cuentas de origen que tienen una relación de confianza con la cuenta de supervisión central pueden asumir esta función y ver los datos de la cuenta de supervisión. CloudWatch proporciona un ejemplo de CloudFormation script para crear el rol. Elija Administrar el rol en IAM y ejecute este script en las cuentas en las que desee ver los datos. `{`	AWS DevOps, administrador de nube, arquitecto de nube

Tarea	Descripción	Habilidades requeridas
	"Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Principal": { "AWS": ["arn:aws:iam::XXXXXXXXXX:root", "arn:aws:iam::XXXXXXXXXX:root", "arn:aws:iam::XXXXXXXXXX:root", "arn:aws:iam::XXXXXXXXXX:root"] }, "Action": "sts:AssumeRole" }] } Para obtener más información, consulte Habilitar la funcionalidad multicuenta CloudWatch en la documentación CloudWatch	

(Opcional) Ver las cuentas y Regiones cruzadas desde la cuenta de monitoreo

Tarea	Descripción	Habilidades requeridas
Configuración del acceso entre cuentas y regiones.	En la cuenta de supervisión central, si lo desea, puede añadir un selector de cuentas para cambiar fácilmente de una cuenta a otra y ver sus datos sin tener que autentica rse. 1. Inicie sesión en la cuenta central de monitoreo. 2. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/. 3. En el panel de navegació n de la izquierda, elija Setttings (Ajustes). 4. En la sección Ver varias cuentas en todas las regiones, seleccione Configure (Configurar). 5. Seleccione Activar y, a continuación, seleccione la casilla Mostrar el selector en la consola. 6. Elija una de estas opciones: • Introducir el identific ador de cuenta: esta opción le pide que introduzca manualmen te el identificador de la cuenta siempre que	AWS DevOps, administrador de nube, arquitecto de nube

Tarea	Descripción	Habilidades requeridas
	desee cambiar de cuenta para ver los datos de varias cuentas. • Selector de cuentas de AWS Organization: si se ha integrado CloudWatch con AWS Organizations, esta opción proporciona un selector desplegable con una lista completa de las cuentas de la organización. • Selector de cuentas personalizado: esta opción le permite introducir manualmente una lista de identificadores de cuentas para completar el selector. 7. Seleccione Guardar cambios. Para obtener más información, consulte la CloudWatch consola multicuentas entre regiones en la documentación. CloudWatch	

Recursos relacionados

- CloudWatch observabilidad entre cuentas (documentación de Amazon CloudWatch)
- Referencia de la API de Amazon CloudWatch Observability Access Manager (CloudWatch documentación de Amazon)

- Recurso: aws_oam_sink (documentación de Terraform)
- Origen de datos: aws_oam_link (documentación de Terraform)
- CloudWatchObservabilityAccessManager(documentación de AWS Boto3)

Compruebe las instancias EC2 para ver si hay etiquetas obligatorias en el lanzamiento

Entorno: producción	Tecnologías: infraestructura; administración y gobierno; seguridad, identidad, conformidad; nativo en la nube	Servicios de AWS: Amazon EC2; AWS; Amazon CloudWatch; CloudTrail Amazon SNS

Resumen

Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de Amazon Web Services (AWS). El uso de Amazon EC2 elimina la necesidad de invertir inicialmente en hardware, de manera que puede desarrollar e implementar aplicaciones en menos tiempo.

Las etiquetas le permiten clasificar los recursos de AWS de diversas maneras. El etiquetado de instancias de EC2 es útil cuando tiene muchos recursos en la cuenta y desea identificar rápidamente un recurso específico en función de las etiquetas. Puede asignar metadatos personalizados a sus instancias de EC2 mediante etiquetas. Una etiqueta es una marca que consta de una clave y un valor definidos por el usuario. Le recomendamos que cree un conjunto de etiquetas coherente para satisfacer los requisitos de su organización.

Este patrón proporciona una CloudFormation plantilla de AWS que le ayuda a supervisar las instancias de EC2 en busca de etiquetas específicas. La plantilla crea un evento de Amazon CloudWatch Events que vigila los UntagResourceeventos de AWS para detectar el etiquetado CloudTrail TagResourceo la eliminación de etiquetas de nuevas instancias de EC2. Si falta una etiqueta predefinida, llama una función de Lambda de AWS, que envía un mensaje de infracción a la dirección de correo electrónico que usted proporcione mediante Amazon Simple Notification Service (Amazon SNS).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.

- Cargue el código de Lambda proporcionado en un bucket de Amazon Simple Storage Service (Amazon S3).
- Una dirección de correo electrónico en la que desee recibir las notificaciones de infracciones.

Limitaciones

- Esta solución es compatible con nuestros eventos CloudTrail TagResource. UntagResource No crea notificaciones para ningún otro evento.
- Esta solución solo comprueba las claves de las etiquetas. No supervisa los valores clave.

Arquitectura

Arquitectura de flujo de trabajo

Automatizar y escalar

- Puede utilizar la CloudFormation plantilla de AWS varias veces para distintas regiones y cuentas de AWS. Debe ejecutar la plantilla solo una vez en cada región o cuenta.

Herramientas

Servicios de AWS

- Amazon EC2: Amazon Elastic Compute Cloud (Amazon EC2) es un servicio web que proporciona capacidad de computación segura de tamaño variable en la nube. Se ha diseñado para facilitar a los desarrolladores la computación en la nube en la Web.
- AWS CloudTrail: CloudTrail es un servicio de AWS que le ayuda con la gobernanza, el cumplimiento y la auditoría operativa y de riesgos de su cuenta de AWS. Las acciones realizadas por un usuario, un rol o un servicio de AWS se registran como eventos en CloudTrail.
- Amazon CloudWatch Events: Amazon CloudWatch Events ofrece una transmisión casi en tiempo real de los eventos del sistema que describen los cambios en los recursos de AWS. CloudWatch Events se da cuenta de los cambios operativos a medida que se producen y toma las medidas correctivas necesarias, mediante el envío de mensajes en respuesta al entorno, la activación de funciones, la introducción de cambios y la recopilación de información sobre el estado.

- AWS Lambda: Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos altamente escalable que se puede utilizar para una amplia gama de soluciones de almacenamiento, incluidos sitios web, aplicaciones móviles, copias de seguridad y lagos de datos.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) es un servicio web que permite a las aplicaciones, los usuarios finales y los dispositivos enviar y recibir al instante notificaciones desde la nube.

Codigo

Este patrón incluye un adjunto con dos archivos:

- `index.zip` es un archivo comprimido que incluye el código de Lambda de este patrón.
- `ec2-require-tags.yaml`es una CloudFormation plantilla que despliega el código Lambda.

Consulte la sección Epics para obtener información sobre cómo usar estos archivos.

Epics

Implementar el código de Lambda

Tarea	Descripción	Habilidades requeridas
Cargue el código en un bucket de S3.	Cree un bucket de S3 nuevo o utilice un bucket de S3 ya existente para cargar el archivo adjunto `index.zip` (código de Lambda). Este bucket debe estar en la misma región de AWS que los recursos (instancias EC2) que desea monitorear.	Arquitecto de la nube
Implemente la plantilla CloudFormation .	Abra la consola de Cloudform ation en la misma región de	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	AWS que el bucket de S3 e implemente el archivo `ec2-require-tags.yaml` que se incluye en el archivo adjunto. En la siguiente Epic, proporcione los valores de los parámetros.	

Complete los parámetros de la CloudFormation plantilla

Tarea	Descripción	Habilidades requeridas
Proporcione el nombre del bucket de S3.	Escriba el nombre del bucket de S3 que ha creado o seleccionado en la primera Epic. Este bucket de S3 contiene el archivo.zip del código Lambda y debe estar en la misma región de AWS que CloudFormation la plantilla y las instancias de EC2 que desea supervisar.	Arquitecto de la nube
Proporcione la clave de S3.	Proporcione la ubicación del archivo .zip del código de Lambda en su bucket de S3, sin barras diagonales iniciales (por ejemplo, `index.zip` o `controls/index.zip`).	Arquitecto de la nube
Proporcione una dirección de correo electrónico.	Proporcione una dirección de correo electrónico activa en la que desee recibir notificac iones de infracciones.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Defina un nivel de registro.	Especifique el nivel de registro y el detalle. `Info` designa mensajes informativos detallados sobre el progreso de la aplicación y solo debe usarse para la depuración. `Error` designa los eventos de error que aún podrían permitir que la aplicación siguiera ejecutándose. `Warning` designa situaciones potencial mente dañinas.	Arquitecto de la nube
Ingrese las claves de etiqueta requeridas.	Escriba las claves de etiqueta que desea comprobar. Si desea especificar varias claves, sepárelas con comas, sin espacios. (Por ejemplo, `ApplicationId,Crea tedBy,Environment, Organization` busca cuatro claves). El evento CloudWatch Events busca estas claves de etiquetas y envía una notificación si no las encuentra.	Arquitecto de la nube

Confirmar la suscripción

Tarea	Descripción	Habilidades requeridas
Confirme la suscripción de correo electrónico.	Cuando la CloudFormation plantilla se implementa correctamente, envía un	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	mensaje de correo electrónico de suscripción a la dirección de correo electrónico que has proporcionado. Debe confirmar esta suscripción de correo electrónico para recibir notificaciones.	

Recursos relacionados

- Creación de un bucket (documentación de Amazon S3)
- Carga de objetos (documentación de Amazon S3)
- Etiquetado de los recursos de Amazon EC2 (documentación de Amazon EC2)
- Creación de una regla de CloudWatch eventos que se active en una llamada a la API de AWS mediante AWS CloudTrail (CloudWatch documentación de Amazon)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Conectarse a una instancia de Amazon EC2 mediante el uso de Session Manager

Creado por Jason Cornick (AWS), Abhishek Bastikoppa (AWS) y Yaniv Ron (AWS)

Entorno: producción	Tecnologías: infraestructura; nativa en la nube; informática para el usuario final; operaciones	Servicios de AWS: Amazon CloudWatch Logs; AWS Systems Manager; Amazon EC2

Resumen

Este patrón describe cómo conectarse a una instancia de Amazon Elastic Compute Cloud (Amazon EC2) mediante el AWS Manager, una capacidad de AWS Manager. Con este patrón, puede ejecutar comandos bash en una instancia EC2 a través de un navegador web. El administrador de sesiones no requiere que abra los puertos de entrada ni requiere direcciones IP públicas para las instancias EC2. Además, elimina la necesidad de mantener los hosts bastión con diferentes claves de Secure Shell (SSH). Puede controlar el acceso al administrador de sesiones con las políticas de AWS Identity and Access Management (IAM) y configurar el registro, que registra información importante, como el acceso a las instancias y las acciones.

En este patrón, configura una función de IAM y la asocia a una instancia EC2 de Linux que aprovisiona mediante una imagen de máquina de Amazon (AMI). A continuación, configura el registro en Amazon CloudWatch Logs y usa el Administrador de sesiones para iniciar una sesión con la instancia.

Aunque este patrón se conecta a una instancia EC2 de Linux en la nube de Amazon Web Services (AWS), puede usar este enfoque para usar el Administrador de sesiones para las conexiones con otros servidores, como servidores locales u otras máquinas virtuales.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.

- Permisos para acceder al nodo gestionado. Para obtener información, consulte Control del acceso de las sesiones de usuario a nodos administrados.
- Puntos finales de VPC para `ssm`, `ec2`, `ec2messages`, `ssmmessages` y `s3`. Para obtener instrucciones, consulte Crear puntos de conexión de VPC en la documentación del Administrador de sistemas.

Arquitectura

Pila de tecnología de destino

- Session Manager
- Amazon EC2
- CloudWatch Registros

Arquitectura de destino

1. El usuario autentica su identidad y sus credenciales a través de IAM.
2. El usuario inicia una sesión SSH a través del administrador de sesiones y envía llamadas a la API a la instancia EC2.
3. El agente SSM de AWS Systems Manager, que está instalado en la instancia EC2, se conecta al administrador de sesiones y ejecuta los comandos.
4. Con fines de auditoría y supervisión, el administrador de sesiones envía los datos de registro a CloudWatch Logs. También puede enviar datos de registro a un bucket de Amazon Simple Storage Service (Amazon S3). Para obtener más información, consulte Registrar datos de sesión mediante Amazon S3 (documentación del Administrador de sistemas).

Herramientas

Servicios de AWS

- Amazon CloudWatch Logs le ayuda a centralizar los registros de todos sus sistemas, aplicaciones y servicios de AWS para que pueda supervisarlos y archivarlos de forma segura.
- Amazon Elastic Compute Cloud (Amazon EC2) brinda capacidad de computación escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos

con rapidez. Este patrón utiliza una Imagen de máquina de Amazon (AMI)) para aprovisionar una instancia de Linux EC2.

- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Systems Manager le permite administrar las aplicaciones y la infraestructura que se ejecutan en la nube de AWS. Simplifica la administración de aplicaciones y recursos, reduce el tiempo requerido para detectar y resolver problemas operativos y ayuda a utilizar y administrar los recursos de AWS a escala de manera segura. Este patrón utiliza el Administrador de sesiones, una capacidad de Administrador de sistemas.

Prácticas recomendadas

Le recomendamos que lea más sobre el pilar de seguridad del Marco de AWS Well-Architected y explore las opciones de cifrado y aplique las recomendaciones de seguridad de la sección Configuración del administrador de sesiones (documentación del Administrador de sistemas).

Epics

Configure la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree el rol de IAM.	Cree el rol de IAM para el agente de SSM. Siga las instrucciones de Creación de un rol para un servicio de AWS (documentación de IAM) y tenga en cuenta lo siguiente: 1. Para el servicio AWS, elija EC2. 2. Para las políticas de permisos, seleccione `AmazonSSMManagedInstanceCore` .	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	3. En Nombre del rol, escriba `EC2_SSM_Role` .	

Tarea	Descripción	Habilidades requeridas
Crear la instancia EC2.	1. Crear la instancia EC2. Siga las instrucciones de Lanzar una instancia (documentación de Amazon EC2) y tenga en cuenta lo siguiente: a. En la sección Nombre y etiquetas, seleccione Añadir etiquetas adicionales. En Key (Clave), escriba `Name` y, en Value (Valor), escriba `Production_Server_One` . b. Seleccione una AMI de Amazon Linux que tenga el agente SSM preinstalado. Para obtener una lista completa, consulte las AMI con el agente SSM preinstalado (documentación del Administrador de sistemas). c. En la sección de detalles avanzados, en el perfil de instancia de IAM, seleccione EC2_SSM_Role. 2. Abra la consola de Systems Manager en https://console.aws.amazon.com/systems-manager/.	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	3. En el panel de navegación, seleccione Administrador de flotas. 4. Compruebe que la instancia aparece en la lista de nodos administrados.	
Configurar el registro.	1. Cree un grupo de CloudWatch registros en Logs. Siga las instrucciones de Crear un grupo de CloudWatch registros (documentación de registros). Nombre el nuevo grupo de registros `SessionManager` . 2. Configure el registro para el administrador de sesiones. Siga las instrucciones de Registrar datos de sesión con Amazon CloudWatch Logs (documentación de Systems Manager) y tenga en cuenta lo siguiente: a. No selecciones Permitir solo grupos de CloudWatch registros cifrados. b. En Elija un grupo de registros de la lista, elija SessionManager.	Administrador de sistemas de AWS

Conectarse a la instancia

Tarea	Descripción	Habilidades requeridas
Conectarse a la instancia EC2.	1. Iniciar una sesión en la consola del Administrador de sistemas. Para recibir instrucciones, consulte Iniciar una sesión (documentación del Administrador de sistemas). En Instancias de destino, seleccione el botón de opción situado a la izquierda de la instancia de Production_Server_One. 2. Una vez realizada la conexión, ejecute varios comandos de bash. 3. En la consola del Administrador de sistemas, finalice la sesión. Para obtener instrucciones, consulte Finalizar una sesión (documentación del Administrador de sistemas).	Administrador de sistemas de AWS
Valide el registro.	1. En CloudWatch Registros, abra el flujo de registros del grupo de registros. Para obtener instrucciones, consulte Ver datos de registro (documentación de CloudWatch registros). 2. En los datos de registro, confirme que aparecen los	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	comandos que ejecutó en la historia anterior.	

Solución de problemas

Problema	Solución
Problemas con IAM	Para obtener asistencia, consulte Solución de problemas (documentación de IAM).

Recursos relacionados

- Requisitos previos completos de Session Manager (documentación del Administrador de sistemas)
- Diseño e implementación del registro y la supervisión con Amazon CloudWatch (AWS Prescriptive Guidance)

Cree una canalización en las regiones de AWS que no sean compatibles con AWS CodePipeline

Creado por Anand Krishna Varanasi (AWS)

Repositorio de código: invisible-codepipeline-unsupported-regions	Entorno: PoC o piloto	Tecnologías: infraestructura; DevOps
Servicios de AWS: AWS CodeBuild CodeCommit; AWS CodeDeploy; AWS CodePipeline		

Resumen

AWS CodePipeline es un servicio de organización de entrega continua (CD) que forma parte de un conjunto de DevOps herramientas de Amazon Web Services (AWS). Se integra con una gran variedad de fuentes (como sistemas de control de versiones y soluciones de almacenamiento), productos y servicios de integración continua (CI) de AWS y sus socios, y productos de código abierto para proporcionar un servicio de end-to-end flujo de trabajo que permita una implementación rápida de aplicaciones e infraestructuras.

Sin embargo, CodePipeline no es compatible en todas las regiones de AWS y es útil tener un orquestador invisible que conecte los servicios de CI/CD de AWS. Este patrón describe cómo implementar una canalización de end-to-end flujo de trabajo en las regiones de AWS en las que aún CodePipeline no se admite mediante el uso de servicios de CI/CD de AWS, como CodeCommit AWS CodeBuild, AWS y AWS. CodeDeploy

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- CLI del AWS Cloud Development Kit (AWS CDK) versión 2.28 o posterior

Arquitectura

Pila de tecnología de destino

En el siguiente diagrama se muestra una canalización que se creó en una región que no es compatible CodePipeline, como la región de África (Ciudad del Cabo). Un desarrollador envía los archivos de CodeDeploy configuración (también denominados scripts de enlace del ciclo de vida de despliegue) al repositorio de Git que aloja. CodeCommit (Consulta el GitHub repositorio que se proporciona con este patrón). Se inicia CodeBuild automáticamente una EventBridge regla de Amazon.

Los archivos CodeDeploy de configuración se obtienen CodeCommit como parte de la etapa de origen de la canalización y se transfieren a ella. CodeBuild

En la siguiente fase, CodeBuild realiza las siguientes tareas:

1. Descargue el archivo TAR del código fuente de la aplicación. Puede configurar el nombre de este archivo mediante Parameter Store, una capacidad de AWS Systems Manager.
2. Descarga los archivos CodeDeploy de configuración.
3. Crea un archivo combinado de código fuente de la aplicación y archivos de CodeDeploy configuración específicos del tipo de aplicación.
4. Inicia el CodeDeploy despliegue en una instancia de Amazon Elastic Compute Cloud (Amazon EC2) mediante el archivo combinado.

Herramientas

Servicios de AWS

- AWS CodeBuild es un servicio de compilación totalmente gestionado que le ayuda a compilar código fuente, ejecutar pruebas unitarias y producir artefactos listos para su implementación.
- AWS CodeCommit es un servicio de control de versiones que le ayuda a almacenar y gestionar repositorios de Git de forma privada, sin necesidad de gestionar su propio sistema de control de código fuente.
- AWS CodeDeploy automatiza las implementaciones en instancias locales o de Amazon EC2, funciones de AWS Lambda o servicios de Amazon Elastic Container Service (Amazon ECS).

- AWS le CodePipeline ayuda a modelar y configurar rápidamente las diferentes etapas de una versión de software y a automatizar los pasos necesarios para publicar cambios de software de forma continua.
- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura de la nube de AWS en código.

Código

El código de este patrón está disponible en el repositorio de regiones GitHub CodePipeline no compatibles.

Epics

Configurar la estación de trabajo de desarrollador

Tarea	Descripción	Habilidades requeridas
Instale la CLI de AWS CDK.	Para obtener instrucciones, consulte la documentación de AWS CDK.	AWS DevOps
Instalar un cliente Git.	Para crear confirmaciones, puedes usar un cliente Git instalado en tu computadora local y, a continuación, enviar tus confirmaciones al CodeCommit repositorio. Para configurarlo CodeCommit con tu cliente Git, consulta la CodeCommit documentación.	AWS DevOps
Instale npm.	Instale el administrador de paquetes npm. Para obtener más información, consulte la documentación npm.	AWS DevOps

Configurar la canalización

Tarea	Descripción	Habilidades requeridas
Clone el repositorio de código.	Clone el repositorio de Regions GitHub CodePipeline no compatibles en su máquina local ejecutando el siguiente comando. `git clone https://github.com/aws-samples/invisible-codepipeline-unsupported-regions`	DevOps ingeniero
Establezca los parámetros en cdk.json.	Abra el archivo `cdk.json` y proporcione valores para los siguientes parámetros: `"pipeline_account":"XXXXXXXXXXXX", "pipeline_region":"us-west-2", "repo_name": "app-dev-repo", "ec2_tag_key": "test-vm", "configName" : "cbdeployconfig", "deploymentGroupName": "cbdeploygroup", "applicationName" : "cbdeployapplication", "projectName" : "CodeBuildProject"` donde:	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	• `pipeline_account` es la cuenta de AWS en la que se creará la canalización. • `pipeline_region` es la región de AWS en la que se construirá la canalización. • `repo_name` es el nombre del CodeCommit repositorio. • `ec2_tag_key` es la etiqueta adjunta a la instancia EC2 en la que desea implementar el código. • `configName` es el nombre del archivo CodeDeploy de configuración. • `deploymentGroupNam e` es el nombre del grupo CodeDeploy de despliegue. • `applicationName` es el nombre CodeDeploy de la aplicación. • `projectName` es el nombre CodeBuild del proyecto.	

Tarea	Descripción	Habilidades requeridas
Configure la biblioteca de constructo de AWS CDK.	En el GitHub repositorio clonado, utilice los siguiente s comandos para instalar la biblioteca de construcción de AWS CDK, compilar la aplicación y sintetizar para generar la CloudFormation plantilla de AWS para la aplicación. `npm i aws-cdk-lib` `npm run build` `cdk synth`	AWS DevOps
Implementar la aplicación de AWS CDK de muestra	Implemente el código ejecutando el siguiente comando en una región no compatible (por ejemplo `af-south-1`). `cdk deploy`	AWS DevOps

Configure el CodeCommit repositorio para CodeDeploy

Tarea	Descripción	Habilidades requeridas
Configurar CI/CD para la aplicación.	Clone el CodeCommit repositorio que especificó en el `cdk.json` archivo (se denomina de forma `app-dev-repo` predeterminada) para configurar la canalización de CI/CD de la aplicación.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`git clone https://git-codecommit.us-west-2.amazonaws.com/v1/repos/app-dev-repo` donde el nombre y la región del repositorio dependen de los valores que haya proporcionado en el archivo `cdk.json`.	

Prueba la canalización

Tarea	Descripción	Habilidades requeridas
Pruebe la canalización con las instrucciones de implementación.	La `CodeDeploy_Files` carpeta del repositorio de regiones GitHub CodePipeline no compatibles incluye archivos de muestra que indican cómo CodeDeploy implementar la aplicación. El `appspec.yml` archivo es un archivo CodeDeploy de configuración que contiene enlaces para controlar el flujo de implementación de la aplicación. Puede usar los archivos de muestra `index.html` , `start_server.sh` , `stop_server.sh` y `install_dependencies.sh` para actualizar un sitio web alojado en Apache. Estos	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	son ejemplos: puede usar el código del GitHub repositor io para implementar cualquier tipo de aplicación. Cuando los archivos se envían al CodeCommit repositorio, la canalización invisible se inicia automáticamente. Para ver los resultados de la implementación, compruebe los resultados de las fases individuales en las CodeDeplo y consolas CodeBuild y consolas.	

Recursos relacionados

- Introducción (documentación de AWS CDK)
- Introducción al Cloud Development Kit (CDK) (AWS Workshop Studio)
- Taller sobre AWS CDK

Implementar un clúster de Cassandra en Amazon EC2 con IP estáticas privadas para evitar el reequilibrio

Creado por Dipin Jain (AWS)

Entorno: PoC o piloto	Origen: máquina virtual en las instalaciones	Destino: Amazon EC2
Tipo R: volver a alojar	Carga de trabajo: código abierto	Tecnologías: infraestructura; bases de datos; migración
Servicios de AWS: Amazon EC2		

Resumen

La IP privada de una instancia de Amazon Elastic Compute Cloud (Amazon EC2) se retiene durante todo su ciclo de vida. Sin embargo, la IP privada puede cambiar durante un bloqueo planificado o imprevisto del sistema; por ejemplo, durante una actualización de Imagen de máquina de Amazon (AMI). En algunos escenarios, retener una IP estática privada puede mejorar el rendimiento y el tiempo de recuperación de las cargas de trabajo. Por ejemplo, el uso de una IP estática para un nodo raíz de Apache Cassandra evita que el clúster incurra en una sobrecarga de reequilibrio.

Este patrón describe cómo conectar una interfaz de red elástica secundaria a las instancias de EC2 para mantener la IP estática durante el rehosting. El patrón se centra en los clústeres de Cassandra, pero puede usar esta implementación para cualquier arquitectura que se beneficie de IP estáticas privadas.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta activa de Amazon Web Services (AWS)

Versiones de producto

- DataStax versión 5.11.1
- Sistema operativo: Ubuntu 16.04.6 LTS

Arquitectura

Arquitectura de origen

La fuente podría ser un clúster de Cassandra en una máquina virtual (VM) en las instalaciones o en instancias de EC2 en la nube de AWS. En el siguiente diagrama se ilustra el segundo escenario. Este ejemplo incluye cuatro nodos en el clúster: tres nodos raíz y un nodo de administración. En la arquitectura de origen, cada nodo tiene una única interfaz de red conectada.

Arquitectura de destino

El clúster de destino se aloja en instancias de EC2 con una interfaz de red elástica secundaria conectada a cada nodo, como se muestra en el siguiente diagrama.

Automatizar y escalar

También puede automatizar la conexión de una segunda interfaz de red elástica a un grupo de escalado automático de EC2, tal y como se describe en un video del Centro de conocimientos de AWS.

Epics

Configurar un clúster de Cassandra en Amazon EC2

Tarea	Descripción	Habilidades requeridas
Lanzar los nodos de EC2 para alojar un clúster de Cassandra.	En la consola de Amazon EC2, lance cuatro instancias de EC2 para los nodos de Ubuntu de su cuenta de AWS. Se utilizan tres nodos (iniciales) para el clúster	Ingeniero de nube

Tarea	Descripción	Habilidades requeridas
	de Cassandra y el cuarto nodo actúa como nodo de administración de clústeres donde se instalará DataStax Enterprise (DSE). OpsCenter Para obtener instrucciones, consulte la documentación de Amazon EC2.	
Confirmar las comunicaciones de los nodos.	Asegúrese de que los cuatro nodos se puedan comunicar entre sí a través de los puertos de administración de la base de datos y el clúster.	Ingeniero de redes
Instale el DSE OpsCenter en el nodo de administración.	Instale DSE OpsCenter 6.1 desde el paquete Debian en el nodo de gestión. Para obtener instrucciones, consulte la DataStax documentación.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree una interfaz de red secundaria.	Cassandra genera un identificador único universal (UUID) para cada nodo en función de la dirección IP de la instancia de EC2 de dicho nodo. Este UUID se utiliza para distribuir los nodos virtuales (vnodes) en el anillo. Cuando Cassandra se implementa en instancias de EC2, las direcciones IP se asignan automáticamente a las instancias a medida que se crean. En caso de una interrupción planificada o imprevista, la dirección IP de la nueva instancia de EC2 cambia, la distribución de los datos cambia y todo el anillo debe reequilibrarse. Esta situación no es deseable. Para conservar la dirección IP asignada, utilice una interfaz de red elástica secundaria con una dirección IP fija. 1. En la consola de Amazon EC2, seleccione Interfaces de red, Crear interfaz de red. 2. Para Subred, seleccione la subred en la que creó la instancia de EC2.	Ingeniero de nube

Tarea	Descripción	Habilidades requeridas
	3. Para la dirección IPv4 privada, seleccione Asignación automática. 4. Para los Grupos de seguridad, seleccione un grupo de seguridad y, a continuación, seleccione Crear interfaz de red. Para obtener más información sobre cómo crear una interfaz de red, consulte la documentación de Amazon EC2.	
Conectar la interfaz de red secundaria a los nodos del clúster.	1. En la consola de Amazon EC2, seleccione Instancias. 2. Seleccione la casilla de verificación de la instancia de EC2 que creó anteriormente. 3. Elija Acciones, Redes, Conectar interfaz de red. 4. Seleccione la interfaz de red que creó en el paso anterior y, a continuación, seleccione Conectar. Para obtener más información sobre cómo conectar una interfaz de red, consulte la documentación de Amazon EC2.	Ingeniero de nube

Tarea	Descripción	Habilidades requeridas
Añadir rutas en Amazon EC2 para abordar el enrutamiento asimétrico.	Al conectar la segunda interfaz de red, es muy probable que la red realice un enrutamiento asimétrico. Para evitarlo, puede agregar rutas para las nuevas interfaces de red. Para obtener una explicaci ón detallada y corregir el enrutamiento asimétrico, consulte el vídeo del AWS Knowledge Center o Cómo superar el enrutamiento asimétrico en servidores multihogar (artículo publicado por Patrick en Linux Journal McManus, el 5 de abril de 2004).	Ingeniero de redes
Actualizar las entradas de DNS para que apunten a la IP de la interfaz de red secundari a.	Apunte el nombre de dominio completo (FQDN) del nodo a la IP de la interfaz de red secundaria.	Ingeniero de redes
Instale y configure el clúster de Cassandra mediante DSE. OpsCenter	Cuando los nodos del clúster estén listos con las interface s de red secundarias, podrá instalar y configurar el clúster de Cassandra.	Administrador de base de datos

Recuperar el clúster de un fallo de nodo

Tarea	Descripción	Habilidades requeridas
Crear una AMI para el nodo raíz del clúster.	Haga una copia de seguridad de los nodos para poder restaurarlos con los archivos binarios de la base de datos en caso de que fallen los nodos. Para obtener instrucciones, consulte Crear una AMI en la documentación de Amazon EC2.	Administrador de copias de seguridad
Recuperarse del fallo de un nodo.	Sustituya el nodo fallido por una nueva instancia de EC2 lanzada desde la AMI y conecte la interfaz de red secundaria del nodo fallido.	Administrador de copias de seguridad
Verificar que el clúster de Cassandra está en buen estado.	Cuando el nodo de reemplazo esté activo, compruebe el estado del clúster en DSE. OpsCenter	Administrador de base de datos

Recursos relacionados

- Instalación del DSE OpsCenter 6.1 desde el paquete Debian (DataStax documentación)
- Cómo hacer que una interfaz de red secundaria funcione en una instancia de EC2 de Ubuntu (video del Centro de conocimientos de AWS)
- Prácticas recomendadas para ejecutar Apache Cassandra en Amazon EC2 (entrada del Blog de AWS)

Amplíe las VRF a AWS mediante AWS Transit Gateway Connect

Entorno: PoC o piloto	Tecnologías: infraestructura; redes	Servicios de AWS: AWS Direct Connect; AWS Transit Gateway

Resumen

El enrutamiento y el reenvío virtuales (VRF) son una característica de las redes tradicionales. Utiliza dominios de enrutamiento lógico aislados, en forma de tablas de enrutamiento, para separar el tráfico de red dentro de la misma infraestructura física. Puede configurar AWS Transit Gateway para que admita el aislamiento de VRF al conectar su red en las instalaciones a AWS. Este patrón utiliza una arquitectura de ejemplo para conectar los VRF en las instalaciones a diferentes tablas de enrutamiento de las puertas de enlace de tránsito.

Este patrón utiliza interfaces virtuales de tránsito (VIF) en las conexiones de AWS Direct Connect y Transit Gateway Connect para ampliar los VRF. Un VIF de tránsito se utiliza para acceder a una o más puertas de enlace de tránsito de Amazon VPC asociadas a las puertas de enlace de Direct Connect. Una conexión de Transit Gateway Connect conecta una puerta de enlace de tránsito con un dispositivo virtual de terceros que se ejecuta en una VPC. Una conexión de Transit Gateway Connect admite el protocolo de túnel de encapsulación de enrutamiento genérico (GRE) para un alto rendimiento y el protocolo de puerta de enlace fronteriza (BGP) para el enrutamiento dinámico.

El enfoque descrito en este patrón tiene los siguientes beneficios:

- Con Transit Gateway Connect, puede anunciar hasta 1000 rutas en el dispositivo homólogo de Transit Gateway Connect y recibir hasta 5000 rutas de este. El uso de la característica VIF de tránsito Direct Connect sin Transit Gateway Connect está limitado a 20 prefijos por puerta de enlace.
- Puede mantener el aislamiento del tráfico y utilizar Transit Gateway Connect para proporcionar servicios con host en AWS, independientemente de los esquemas de direcciones IP que utilicen sus clientes.
- No es necesario que el tráfico de VRF atraviese una interfaz virtual pública. Esto facilita el cumplimiento de los requisitos de cumplimiento y seguridad en muchas organizaciones.

- Cada túnel de GRE admite hasta 5 Gbps y puede tener hasta cuatro túneles de GRE por cada conexión de Transit Gateway Connect. Es más rápido que muchos otros tipos de conexión, como las conexiones AWS Site-to-Site VPN, que admiten hasta 1,25 Gbps.

Requisitos previos y limitaciones

Requisitos previos

- Se han creado las cuentas de AWS necesarias (consulte la arquitectura para obtener más información)
- Permisos para asumir un rol de AWS Identity and Access Management (IAM) en cada cuenta.
- Los roles de IAM de cada cuenta deben tener permisos para aprovisionar los recursos de AWS Transit Gateway y AWS Direct Connect. Para obtener más información, consulte Autenticación y control de acceso para sus puertas de enlace y Administración de identidad y acceso para Direct Connect.
- Las conexiones Direct Connect se crearon correctamente. Para obtener más información, consulte Creación de una conexión mediante el asistente de conexión.

Limitaciones

- Hay límites para las conexiones de puerta de enlace de tránsito a las VPC en las cuentas de producción, control de calidad y desarrollo. Para obtener más información, consulte Conexión de puerta de enlace de tránsito a una VPC.
- Existen límites para la creación y el uso de gateways de Direct Connect. Para obtener más información, consulte Cuotas AWS Direct Connect.

Arquitectura

Arquitectura de destino

El siguiente ejemplo de arquitectura proporciona una solución reutilizable para implementar VIF de tránsito con conexiones de Transit Gateway Connect. Esta arquitectura proporciona resiliencia mediante el uso de varias ubicaciones de Direct Connect. Para obtener más información, consulte Resiliencia máxima en la documentación de Direct Connect. La red en las instalaciones tiene VRF de producción, control de calidad y desarrollo que se extienden a AWS y se aíslan mediante tablas de enrutamiento específicas.

En el entorno de AWS, hay dos cuentas dedicadas a ampliar los VRF: una cuenta de Direct Connect y una cuenta del hub de red. La cuenta Direct Connect contiene la conexión y los VIF de tránsito de cada router. Los VIF de tránsito se crean desde la cuenta de Direct Connect, pero se implementan en la cuenta del hub de red para poder asociarlos a la puerta de enlace de Direct Connect en la cuenta del concentrador de red. La cuenta del hub de red contiene la puerta de enlace de Direct Connect y la puerta de enlace de tránsito. Los recursos de AWS están conectados de la siguiente manera:

1. Los VIF de tránsito conectan los enrutadores de las ubicaciones de Direct Connect con AWS Direct Connect en la cuenta de Direct Connect.
2. Un VIF de tránsito conecta Direct Connect con la puerta de enlace Direct Connect de la cuenta del hub de red.
3. Una asociación de puertas de enlace de tránsito conecta la puerta de enlace Direct Connect con la puerta de enlace de tránsito de la cuenta del hub de red.
4. Las conexiones Transit Gateway Connect conectan la puerta de enlace de tránsito con las VPC de las cuentas de producción, control de calidad y desarrollo.

Arquitectura Transit VIF

El siguiente diagrama muestra los detalles de configuración de los VIF de tránsito. En este ejemplo de arquitectura se utiliza una VLAN para la fuente del túnel, pero también se puede utilizar un bucle invertido.

A continuación, se muestran los detalles de configuración, como los números de sistema autónomo (ASN), de las VIF de tránsito.

Recurso	Elemento	Detalle
router-01	ASN	65534
router-02	ASN	65534
router-03	ASN	65534
router-04	ASN	65534

Gateway de Direct Connect	ASN	64601
Puerta de enlace de tránsito	ASN	64600
	Bloque CIDR	10,100,254,0/24

Arquitectura Transit Gateway Connect

El diagrama y las tablas siguientes describen cómo configurar un VRF único a través de una conexión Transit Gateway Connect. Para VRFs adicionales, asigne IDs de túnel únicos, direcciones IP GRE de puerta de enlace de tránsito y BGP dentro de los bloques CIDR. La dirección IP GRE homóloga coincide con la dirección IP homóloga del router del VIF de tránsito.

La siguiente tabla contiene detalles de configuración del enrutador.

Enrutador	Túnel	Dirección IP	Origen	Destino
router-01	Túnel 1	169,254101,17	VLAN 60	10,100,254.1
			169,254,1001	
router-02	Túnel 11	169,254,101,81	VLAN 61	10,100254,11
			169,254,1005	
router-03	Túnel 21	169,254,101,145	VLAN 62	10,100254,21
			169,254,1009	
router-04	Túnel 31	169,254,101,209	VLAN 63	10,100254,31
			169,254100,13	

La siguiente tabla contiene detalles de la puerta de enlace de tránsito.

Túnel	Dirección IP GRE de puerta de enlace	Direcciones IP GRE del mismo nivel	BGP dentro de los bloques CIDR

Túnel 1	10,100254.1	VLAN 60 169,254,1001	169,254,101,16/29
Túnel 11	10,100254,11	VLAN 61 169,254,1005	169,254,101,80/29
Túnel 21	10,100254,21	VLAN 62 169,254,1009	169,254.101.144/29
Túnel 31	10,100254,31	VLAN 63 169,254100,13	169,254,101.208/29

Implementación

La sección Epics describe cómo implementar un ejemplo de configuración para un único VRF en varios enrutadores de clientes. Una vez completados los pasos 1 a 5, puede crear nuevas conexiones de Transit Gateway Connect siguiendo los pasos 6 y 7 para cada VRF nuevo que extienda a AWS:

1. Cree la puerta de enlace de tránsito.
2. Crear una tabla de enrutamiento de la puerta de enlace de tránsito para cada VRF.
3. Cree las interfaces virtuales de tránsito.
4. Cree una puerta de enlace Direct Connect.
5. Cree la interfaz virtual de la puerta de enlace Direct Connect y las asociaciones de puerta de enlace con los prefijos permitidos.
6. Cree una conexión de Connect de puerta de enlace de tránsito.
7. Crear pares de Transit Gateway Connect.
8. Asocie las conexiones de Transit Gateway Connect con la tabla de enrutamiento.
9. Anuncie las rutas a los enrutadores.

Herramientas

Servicios de AWS

- AWS Direct Connect vincula su red interna con una ubicación de Direct Connect a través de un cable estándar Ethernet de fibra óptica. Con esta conexión, puede crear interfaces virtuales directamente en servicios públicos de AWS omitiendo a los proveedores de servicios de Internet en su ruta de acceso a la red.
- AWS Transit Gateway es un hub central que conecta las nubes privadas virtuales (VPC) y las redes en las instalaciones.
- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esta red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Epics

Planifique la arquitectura

Tarea	Descripción	Habilidades requeridas
Cree diagramas de arquitectura personalizados.	1. En la sección Attachments (Conexiones), descargue la plantilla de diagrama. 2. Abra el diagrama adjunto en Microsoft Office PowerPoint. 3. En la diapositiva Architecture overview (Descripción general de la arquitectura), personalice el diagrama de arquitectura para su entorno. Identifique los VRF en las instalaciones que deben extenderse a su entorno de AWS. 4. En la diapositiva Transit VIF (VIF de tránsito), personalice el diagrama de arquitectura. Identifique los números	Arquitecto de la nube, administrador de redes

Tarea	Descripción	Habilidades requeridas
	de AS de los enrutador es, la puerta de enlace de Direct Connect y la puerta de enlace de tránsito. Identifique las direcciones IP en cada extremo del VIF de tránsito. 5. En la diapositiva Transit Gateway Connect, personalice un diagrama de arquitectura para cada VRF. Identifique todas las direcciones IP necesaria s para configurar los enrutadores y los pares de Transit Gateway Connect.	

Cree los recursos de la puerta de enlace de tránsito.

Tarea	Descripción	Habilidades requeridas
Cree la puerta de enlace de tránsito.	1. Inicie sesión en la cuenta del hub de red. 2. Siga las instrucciones de Crear una puerta de enlace de tránsito. Tenga en cuenta lo siguiente para este patrón: • En Amazon side Autonomous System Number (ASN) (Número de sistema autónomo (ASN) de Amazon), ingrese el ASN único.	Administrador de redes, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	A los efectos de este ejemplo, el ASN es `64600`. • Seleccione DNS support (Compatibilidad de DNS). • Para este ejemplo de arquitectura, no se requieren la compatibilidad con ECMP de VPN, la Asociación de tablas de enrutamiento predeterminada, la Prórroga de la tabla de enrutamiento predeterminada ni la Compatibilidad con multidifusión. • En los bloques CIDR de Transit Gateway, introduzca los bloques CIDR IPv4 para su puerta de enlace de tránsito. A los efectos de este ejemplo, el bloque de CIDR es `10.100.254.0/24` .	

Tarea	Descripción	Habilidades requeridas
Cree una tabla de enrutamiento para la puerta de enlace de tránsito.	Siga las instrucciones de Crear una tabla de enrutamiento para la puerta de enlace de tránsito. Tenga en cuenta lo siguiente para este patrón: • En Name tag (Nombre de la etiqueta), escriba un nombre para la tabla de enrutamiento de la puerta de enlace de tránsito. Recomendamos usar un nombre que corresponda al VRF, como `routetable-dev-vrf` . • En Transit Gateway ID (ID de gateway de tránsito), elija la puerta de enlace de tránsito que creó.	Arquitecto de la nube, administrador de redes

Cree las interfaces virtuales de tránsito

Tarea	Descripción	Habilidades requeridas
Cree las interfaces virtuales de tránsito.	1. Inicie sesión en la cuenta Direct Connect. 2. Siga las instrucciones para Crear una interfaz virtual de tránsito en la puerta de enlace de Direct Connect. Tenga en cuenta lo siguiente para este patrón:	Arquitecto de la nube, administrador de redes

Tarea	Descripción	Habilidades requeridas
	• En Virtual interface name (Nombre de la interfaz virtual), escriba un nombre para la interfaz virtual. Recomendamos usar un nombre que corresponda al enrutador, como `transit-vif-router01` . • En Connection (Conexión), seleccione el enrutador, por ejemplo `router-01` . • Para el Virtual interface owner (Propietario de la interfaz virtual), introduzca el ID de cuenta de la cuenta del hub de red. Para obtener instrucciones, consulte Ver el ID de su cuenta de AWS. • Para la puerta de enlace Direct Connect, no haga ninguna selección. La puerta de enlace Direct Connect se conecta en un paso posterior. • Para la VLAN, introduzca la VLAN del enrutador, por ejemplo `60`. • Para ASN BGP, introduzca el ASN del enrutador, por ejemplo `65534`.	

Tarea	Descripción	Habilidades requeridas
	• En Additional Settings (Configuración adicional), haga lo siguiente: • Elija IPv4. • Para la IP homóloga de su enrutador, introduzca la dirección IP homóloga del enrutador, por ejemplo `169.254.100.1` . • Para la IP homóloga del enrutador Amazon, introduzca la dirección IP homóloga del enrutador de Amazon, por ejemplo `169.254.100.2` . • Para la clave de autenticación BGP, se requiere una contraseña. Si se deja en blanco, AWS crea una clave a la que solo se puede acceder en esta cuenta. 3. Repita estas instrucciones para crear todos los VIF de tránsito para el VRF.	

Cree los recursos de Direct Connect

Tarea	Descripción	Habilidades requeridas
Cree una gateway de Direct Connect.	1. Inicie sesión en la cuenta del hub de red. 2. Siga las instrucciones de Creación de una puerta de enlace de Direct Connect. Tenga en cuenta lo siguiente para este patrón: • Para el ASN de Amazon, introduzca el ASN de la puerta de enlace Direct Connect, como `64601`. • No elija una puerta de enlace privada virtual.	Arquitecto de la nube, administrador de redes
Conecte la puerta de enlace Direct Connect a los VIF de tránsito.	1. En la cuenta del hub de red, abra la consola de AWS Direct Connect en https://console.aws.amazon.com/directconnect/v2/. 2. En el panel de navegación, elija Virtual Interfaces. 3. Seleccione un nuevo VIF de tránsito y, a continuación, elija Accept (Aceptar). 4. Elija la puerta de enlace Direct Connect que creó. 5. Repita estas instrucciones para cada VIF de tránsito.	Arquitecto de la nube, administrador de redes
Cree las asociaciones de puerta de enlace Direct	En la cuenta del hub de red, siga las instrucciones de Para asociar una puerta de enlace	Arquitecto de la nube, administrador de redes

Tarea	Descripción	Habilidades requeridas
Connect con los prefijos permitidos.	de tránsito. Tenga en cuenta lo siguiente para este patrón: • En Transit Gateway ID (ID de puerta de enlace de tránsito), elija la puerta de enlace de tránsito que creó. • En Allowed prefixes (Prefijos permitidos), introduzca el bloque CIDR asignado a la puerta de enlace de tránsito, por ejemplo `10.100.254.0/24` . Al crear esta asociación, se crea automáticamente una conexión de puerta de enlace de tránsito que tiene un tipo de recurso Direct Connect Gateway. No es necesario que esta conexión esté asociada a una tabla de enrutamiento de puerta de enlace de tránsito.	

Tarea	Descripción	Habilidades requeridas
Cree una conexión de Connect de puerta de enlace de tránsito.	1. En la cuenta del hub de red, abra la consola de AWS VPC en https://console.aws.amazon.com/vpc/. 2. En el panel de navegación, elija Transit gateway attachments (Conexiones de puerta de enlace de tránsito). 3. Elija Create transit gateway attachment (Crear conexión de puerta de enlace de tránsito). 4. En Name (Nombre), escriba un nombre para la conexión. Recomendamos usar un nombre que corresponda al VRF, como `PROD-VRF`. 5. En Transit Gateway ID (ID de puerta de enlace de tránsito), elija la puerta de enlace de tránsito que creó. 6. En Attachment type (Tipo de conexión), elija Connect. 7. Para el Transport attachment ID (ID de conexión de transporte), elija la puerta de enlace de Direct Connect que creó anteriormente. 8. Elija Create transit gateway attachment (Crear conexión	Arquitecto de la nube, administrador de redes

Tarea	Descripción	Habilidades requeridas
	de puerta de enlace de tránsito). 9. Repita este paso para cada VRF que vaya a ampliar.	

Tarea	Descripción	Habilidades requeridas
Crear pares de Transit Gateway Connect.	1. En la cuenta del hub de red, siga las instrucciones de Crear un homólogo de Transit Gateway Connect (túnel de GRE). Tenga en cuenta lo siguiente para este patrón: • En Name tag (Nombre de la etiqueta), puede escribir un nombre para la puerta de enlace de tránsito. Recomendamos usar un nombre que corresponda al enrutador, como `connectpeer-router01` . • Para la dirección GRE de Transit Gateway, introduzca la dirección IP asignada desde el bloque CIDR, por ejemplo `10.100.254.1` . • Para la dirección GRE homóloga, introduzca la dirección IP asignada a la VLAN creada en el enrutador para el VIF de tránsito, por ejemplo `169.254.100.1` . Siempre que AWS pueda acceder a la dirección IP, puede utilizar cualquier interfaz, como VLAN	

Tarea	Descripción	Habilidades requeridas
	o Loopback, para la dirección GRE homóloga. • Para el BGP dentro de los bloques CIDR (IPv4), introduzca la dirección IP del BGP dentro del bloque CIDR, por ejemplo `169.254.101.16/29` . • Para ASN homólogo, introduzca el ASN del enrutador, por ejemplo `65534`. 2. Repita estas instrucciones para crear un túnel de GRE para cada enrutador.	

Anuncie las rutas a los enrutadores.

Tarea	Descripción	Habilidades requeridas
Anuncie las rutas.	Asocie la nueva conexión de puerta de enlace de Connect a la tabla de enrutamiento que creó anteriormente para este VRF. Por ejemplo, asocie las conexiones de Transit Gateway Connect de producción con la tabla de enrutamiento `Production-VRF`. Cree una ruta estática para el prefijo que se anuncia en los enrutadores.	Administrador de redes, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	1. Inicie sesión en la cuenta del hub de red. 2. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/. 3. En el panel de navegación, bajo Transit Gateways (Puertas de enlace de tránsito) elija Transit gateway route tables (Tablas de enrutamiento de puerta de enlace de tránsito). 4. Seleccione la tabla de enrutamiento de la `Production-VRF` . 5. En el menú Actions (Acciones), elija Create static route (Crear ruta estática). 6. Para CIDR, introduzca el bloque CIDR para la ruta anunciada a la conexión de puerta de enlace de tránsito en la VPC de destino, como `10.100.1.0/24` . 7. En Choose Attachment (Elegir conexión), seleccione la conexión de Transit Gateway Connect correspondiente.	

Tarea	Descripción	Habilidades requeridas
	8. Elija Create static route (Crear ruta estática).	

Recursos relacionados

Documentación de AWS

- Documentación de Direct Connect
  - Uso de puertas de enlace de Direct Connect
  - Asociaciones de la puerta de enlace de tránsito
  - Interfaces virtuales de AWS Direct Connect
- Documentación de Transit Gateway
  - Usar puertas de enlace de tránsito
  - Conexiones de puertas de enlace de tránsito a una puerta de enlace de Direct Connect
  - Conexiones de puertas de enlace de tránsito y pares de Transit Gateway Connect
  - Crear una conexión Transit gateway Connect

Publicaciones del blog de AWS

- Segmentación de redes híbridas con AWS Transit Gateway Connect
- Uso de AWS Transit Gateway Connect para ampliar los VRF y aumentar el anuncio de prefijos de IP

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Reciba notificaciones de Amazon SNS cuando cambie el estado de clave de una clave de AWS KMS

Creado por Shubham Harsora (AWS), Aromal Raj Jayarajan (AWS) y Navdeep Pareek (AWS)

Repositorio de códigos: aws-kms-deletion-notification	Entorno: PoC o piloto	Tecnologías: infraestructura; nativa de la nube DevOps; seguridad, identidad y cumplimiento
Carga de trabajo: todas las demás cargas de trabajo	Servicios de AWS: Amazon EventBridge; AWS KMS; Amazon SNS	

Resumen

Los datos y los metadatos asociados con una clave de AWS Key Management Service (AWS KMS) se pierden al eliminarla. Esta eliminación es irreversible, y no se pueden recuperar los datos perdidos (incluidos los datos cifrados). Puede evitar la pérdida de datos configurando un sistema de notificaciones que le avise de los cambios de estado en los estados de clave de sus claves de AWS KMS.

Este patrón le muestra cómo supervisar los cambios de estado en las claves de AWS KMS mediante Amazon EventBridge y Amazon Simple Notification Service (Amazon SNS) para emitir notificaciones automáticas siempre que el estado clave de una clave de AWS KMS cambie a o. `Disabled` `PendingDeletion` Por ejemplo, si un usuario intenta deshabilitar o eliminar una clave de AWS KMS, recibirá una notificación por correo electrónico con detalles sobre el intento de cambio de estado. También puede usar este patrón para programar la eliminación de las claves de AWS KMS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS con un usuario de AWS Identity and Access Management (IAM)
- Una clave de AWS KMS

Arquitectura

Pila de tecnología

- Amazon EventBridge
- AWS Key Management Service (AWS KMS)
- Amazon Simple Notification Service (Amazon SNS)

Arquitectura de destino

El siguiente diagrama muestra una arquitectura para crear un proceso automatizado de supervisión y notificación que detecta cualquier cambio en el estado de una clave de AWS KMS.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un usuario deshabilita o programa la eliminación de una clave de AWS KMS.
2. Una EventBridge regla evalúa la programación `Disabled` o el `PendingDeletion` evento.
3. La EventBridge regla invoca el tema Amazon SNS.
4. Amazon SNS envía un mensaje de notificación por correo electrónico a los usuarios.

Nota: Puede personalizar el mensaje de correo electrónico para adaptarlo a las necesidades de su organización. Recomendamos incluir información sobre las entidades en las que se usa la clave de AWS KMS. Esto puede ayudar a los usuarios a comprender el impacto de eliminar la clave de AWS KMS. También puede programar una notificación de recordatorio por correo electrónico que se envíe uno o dos días antes de eliminar la clave de AWS KMS.

Automatizar y escalar

La CloudFormation pila de AWS implementa todos los recursos y servicios necesarios para que este patrón funcione. Puede implementar el patrón de forma independiente en una sola cuenta o mediante AWS CloudFormation StackSets para varias cuentas o unidades organizativas independientes en AWS Organizations.

Herramientas

- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS. La CloudFormation plantilla de este patrón describe todos los recursos de AWS que desee y los CloudFormation aprovisiona y configura automáticamente.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. EventBridge ofrece un flujo de datos en tiempo real desde sus propias aplicaciones y servicios de AWS, y dirige esos datos a objetivos como AWS Lambda. EventBridge simplifica el proceso de creación de arquitecturas basadas en eventos.
- AWS Key Management Service (AWS KMS) facilita poder crear y controlar claves criptográficas para proteger los datos.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.

Código

El código de este patrón está disponible en el repositorio GitHub Monitor AWS KMS Keys Disable and Scheduled Delete.

Epics

Implemente la CloudFormation plantilla

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Clone el repositorio de claves, deshabilitación y eliminación programada de claves de AWS KMS de GitHub Monitor en su máquina local ejecutando el siguiente comando: `git clone https://github.com/aws-samp`	Administrador de AWS, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	`les/aws-kms-deleti on-notification`	
Actualice los parámetros de la plantilla.	En un editor de código, abra la `Alerting-KMS-Event s.yaml` CloudFormation plantilla que ha clonado del repositorio y, a continuac ión, actualice los siguientes parámetros: • En `Destinati onEmailAddress` , introduzca la dirección de correo electrónico activa en la que desee recibir la notificación de SNS. • Para `SNSTopicName` , ingrese un nombre para su tema SNS.	Administrador de AWS, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation plantilla.	1. Inicie sesión en la consola de administración de AWS y abra la consola de CloudFormation . 2. En el panel de navegación, seleccione Crear pila y, a continuación, seleccione Con nuevos recursos (estándar). 3. En la página Identificar recursos, seleccione Siguiente. 4. En la página Especificar plantilla, en Origen de la plantilla, seleccione Cargar un archivo de plantilla. 5. Elija Elegir archivo, seleccione el `Alerting-KMS-Events.yaml` archivo del GitHub repositorio clonado y, a continuación, elija Siguiente. 6. En Nombre de la pila, introduzca el nombre de la pila. 7. Seleccione Enviar.	Administrador de AWS, arquitecto de la nube

Confirmar la suscripción

Tarea	Descripción	Habilidades requeridas
Confirme la suscripción por correo electrónico.	Una vez que la CloudFormation plantilla se haya	Administrador de AWS, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	implementado correctamente, Amazon SNS envía un mensaje de confirmación de suscripción a la dirección de correo electrónico que proporcionó en CloudFormation la plantilla. Debe confirmar esta suscripción de correo electrónico para recibir notificaciones. Para obtener más información, consulte Cómo confirmar la suscripción en la Guía para desarrolladores de Amazon SNS.	

Pruebe la notificación de la suscripción

Tarea	Descripción	Habilidades requeridas
Deshabilite las claves de AWS KMS.	1. Inicie sesión en la consola de administración de AWS y abra la consola de AWS KMS. 2. Para cambiar la región, elija el nombre de la región que se muestra actualmente y, a continuación, seleccione la región a la que desee cambiar. 3. En el panel de navegación, elija Claves administradas por el cliente.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	4. Seleccione la casilla de verificación de las claves de AWS KMS que quiere habilitar o deshabilitar. 5. Para deshabilitar una clave de AWS KMS, seleccione Key actions (Acciones de claves), y posteriormente, Disable (Deshabilitar).	
Valide la suscripción.	Confirme que ha recibido la notificación de Amazon SNS por correo electrónico.	Administrador de AWS

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Elimine la pila CloudFormation .	1. Inicie sesión en la consola de administración de AWS y abra la consola de CloudFormation . 2. En el panel de navegación, seleccione Stacks (Pilas). 3. Seleccione la pila que creó anteriormente y, a continuación, seleccione Eliminar.	Administrador de AWS

Recursos relacionados

- AWS CloudFormation (documentación de AWS)

- Creación de una pila en la CloudFormation consola de AWS (CloudFormation documentación de AWS)
- Creación de arquitecturas basadas en eventos en AWS (documentación de AWS Workshop Studio)
- Prácticas recomendadas de AWS Key Management Service (documento técnico de AWS)
- Prácticas recomendadas de seguridad para AWS Key Management Service (AWS KMS) (Guía del desarrollador de AWS KMS)

Información adicional

Amazon SQS proporciona cifrado en tránsito de forma predeterminada. Para satisfacer las prácticas recomendadas de seguridad, también puede habilitar el cifrado en el servidor para Amazon SNS mediante una clave de AWS KMS gestionada por el cliente.

Modernización del mainframe: DevOps en AWS con Micro Focus

Creado por Kevin Yung (AWS)

Origen: Mainframe de IBM z/OS	Destino: AWS	Tipo R: N/D
Entorno: PoC o piloto	Tecnologías: DevOps Infraestructura	Servicios de AWS: Amazon EC2; CloudFormation AWS; CodeBuild AWS; CodeCommit AWS CodeDeploy; AWS Systems Manager; AWS CodePipeline

Resumen

Desafíos de los clientes

Las organizaciones que ejecutan aplicaciones principales en hardware de mainframe suelen enfrentarse a algunos desafíos cuando el hardware necesita escalar verticalmente para satisfacer las demandas de las innovaciones digitales. Estos desafíos incluyen las siguientes limitaciones.

- Los entornos de desarrollo y prueba de los mainframe no se pueden escalar debido a la inflexibilidad de los componentes de hardware de los mainframes y al elevado costo que supone cambiarlos.
- El desarrollo de mainframes se enfrenta a una escasez de personal cualificado, ya que los nuevos desarrolladores no están familiarizados con las herramientas tradicionales de desarrollo de mainframes ni están interesados en ellas. Las tecnologías modernas, como los contenedores, las canalizaciones de integración y entrega continuas (CI/CD) y los marcos de pruebas modernos, no están disponibles para el desarrollo de mainframes.

Resultados del patrón

Para abordar estos desafíos, Amazon Web Services (AWS) y Micro Focus, un socio de la red de socios de AWS (APN), han colaborado para crear este patrón. La solución está diseñada para ayudarle a lograr los siguientes resultados.

- Mejora de la productividad de los desarrolladores. Los desarrolladores pueden disponer de nuevas instancias de desarrollo de mainframe en cuestión de minutos.
- Uso de la nube de AWS para crear nuevos entornos de prueba de mainframe con una capacidad prácticamente ilimitada.
- Aprovisionamiento rápido de una nueva infraestructura de CI/CD de mainframe. El aprovisionamiento en AWS se puede completar en una hora mediante AWS CloudFormation y AWS Systems Manager.
- Uso nativo de DevOps las herramientas de AWS para el desarrollo de mainframes, incluidas AWS CodeBuild, AWS CodeCommit CodePipeline CodeDeploy, AWS y Amazon Elastic Container Registry (Amazon ECR).
- Transforme el desarrollo tradicional en cascada en un desarrollo ágil en proyectos de mainframe.

Resumen de tecnologías

En este patrón, la pila de destino contiene los siguientes componentes.

Componentes lógicos	Soluciones de implementación	Descripción
Repositorios de código fuente	AccuRev Servidor Micro Focus CodeCommit, Amazon ECR	Administración del código fuente – La solución utiliza dos tipos de código fuente. • Código fuente de mainframe , por ejemplo COBOL, JCL, etc. • Plantillas de infraestructura y scripts de automatización de AWS Ambos tipos de código fuente necesitan control de versiones , pero se administran en diferentes SCM. El código fuente implementado en el mainframe o en los servidore s Micro Focus Enterprise se

		administra en Micro Focus AccuRev Server. Las plantillas y los scripts de automatización de AWS se administran en CodeCommit. Amazon ECR se utiliza para los repositorios de imágenes de Docker.
Instancias de desarrolladores empresariales	Amazon Elastic Compute Cloud (Amazon EC2), desarrollador Enterprise Micro Focus para Eclipse	Los desarrolladores de mainframe pueden desarroll ar código en Amazon EC2 mediante Micro Focus Enterprise Developer para Eclipse. Esto elimina la necesidad de depender del hardware del mainframe para escribir y probar el código.
Administración de licencias de Micro Focus	Administrador de licencias de Micro Focus	Para la gestión y el gobierno centralizados de las licencias de Micro Focus, la solución utiliza Micro Focus License Manager para alojar la licencia requerida.
Canalización de CI/CD	CodePipeline,, CodeBuild CodeDeploy, Micro Focus Enterprise Developer en un contenedor, Micro Focus Enterprise Test Server en un contenedor, Micro Focus Enterprise Server	Los equipos de desarrollo de mainframe necesitan canalizac iones de CI/CD para realizar la compilación de código, las pruebas de integración y las pruebas de regresión . En AWS, CodePipeline y CodeBuild puede funcionar con Micro Focus Enterprise Developer y Enterprise Test Server en un contenedor de forma nativa.

Requisitos previos y limitaciones

Requisitos previos

Nombre	Descripción
py3270	py3270 es una interfaz de Python para x3270, un emulador de terminal IBM 3270. Proporcio na una API para un subproceso x3270 o s3270.
x3270	x3270 es un emulador de terminal IBM 3270 para el sistema X Window y Windows. El desarrollador lo puede utilizar para realizar pruebas unitarias a nivel local.
Robot-Framework-Mainframe-3270-Library	Mainframe3270 es una biblioteca para Robot Framework basada en el proyecto py3270.
Micro Focus Verastream	Micro Focus Verastream es una plataforma de integración que permite probar los activos del mainframe del mismo modo que se prueban las aplicaciones móviles, las aplicaciones web y los servicios web SOA.
Instalador y licencia de Micro Focus Unified Functional Testing (UFT)	Micro Focus Unified Functional Testing es un software que automatiza las pruebas funcional es y de regresión para aplicaciones y entornos de software.
Instalador y licencia de Micro Focus Enterprise Server	Enterprise Server proporciona el tiempo de ejecución para las aplicaciones de mainframe.
Instalador y licencia de Micro Focus Enterprise Test Server	Micro Focus Enterprise Test Server es un entorno de prueba de aplicaciones de mainframe de IBM
AccuRev Instalador y licencia de Micro Focus para servidores, e AccuRev instalado	AccuRev proporciona administración de código fuente (SCM). El AccuRev sistema está diseñado para que lo utilice un equipo de

r y licencia de Micro Focus para sistemas operativos Windows y Linux	personas que están desarrollando un conjunto de archivos.
Instalador, parche y licencia de Micro Focus Enterprise Developer para Eclipse	Enterprise Developer proporciona a los desarrolladores de mainframe una plataform a para desarrollar y mantener las principales aplicaciones de mainframe en línea y por lotes.

Limitaciones

- No se admite la creación de una imagen de Docker de Windows en CodeBuild. Este problema notificado necesita el apoyo de los equipos de Kernel/HCS y Docker de Windows. La solución alternativa consiste en crear un manual de procedimientos de imágenes de Docker mediante Systems Manager. Este patrón utiliza la solución alternativa para compilar imágenes de contenedor de Micro Focus Enterprise Developer para Eclipse y Micro Focus Enterprise Test Server.
- Windows aún no admite la conectividad de nube privada virtual (VPC) desde, por lo que el patrón no CodeBuild utiliza Micro Focus License Manager para administrar las licencias en los contenedores Micro Focus Enterprise Developer y Micro Focus Enterprise Test Server.

Versiones de producto

- Micro Focus Enterprise Developer 5.5 o posterior
- Micro Focus Enterprise Test Server 5.5 o posterior
- Micro Focus Enterprise Server 5.5 o posterior
- Micro Focus AccuRev 7.x o posterior
- Imagen base de Windows Docker para Micro Focus Enterprise Developer y Enterprise Test Server: microsoft/dotnet-framework-4.7.2-runtime
- Imagen base de Linux Docker para el AccuRev cliente: amazonlinux:2

Arquitectura

Entorno de mainframe

En el desarrollo de mainframe convencional, los desarrolladores necesitan usar hardware de mainframe para desarrollar y probar programas. Se enfrentan a limitaciones de capacidad,

por ejemplo, la restricción de millones de instrucciones por segundo (MIPS) para el entorno de desarrollo/pruebas, y deben confiar en las herramientas disponibles en las computadoras mainframe.

En muchas organizaciones, el desarrollo de mainframes sigue la metodología de desarrollo en cascada, y los equipos utilizan ciclos largos para publicar los cambios. Estos ciclos de lanzamiento suelen ser más largos que los del desarrollo de productos digitales.

El siguiente diagrama muestra varios proyectos de mainframe que comparten el hardware de mainframe para su desarrollo. En el caso del hardware de mainframe, resulta caro escalar horizontalmente un entorno de desarrollo y pruebas para más proyectos.

Arquitectura de AWS

Este patrón extiende el desarrollo de mainframe a la nube de AWS. En primer lugar, utiliza Micro Focus AccuRev SCM para alojar el código fuente del mainframe en AWS. Luego, permite que Micro Focus Enterprise Developer y Micro Focus Enterprise Test Server estén disponibles para compilar y probar el código del mainframe en AWS.

En las siguientes secciones se describen los tres componentes principales del patrón.

1. SCM

En AWS, el patrón utiliza Micro Focus AccuRev para crear un conjunto de espacios de trabajo SCM y control de versiones para el código fuente del mainframe. Su arquitectura basada en flujos permite el desarrollo de mainframes paralelos para varios equipos. Para combinar un cambio, AccuRev utiliza el concepto de promoción. Para añadir ese cambio a otros espacios de trabajo, AccuRev utiliza el concepto de actualización.

A nivel de proyecto, cada equipo puede crear una o más secuencias para realizar un seguimiento de los cambios AccuRev a nivel de proyecto. Se denominan flujos de proyectos. Estos flujos del proyecto se heredan del mismo flujo principal. El flujo principal se usa para combinar los cambios de los diferentes flujos del proyecto.

Cada flujo de proyectos puede promover el código y se ha configurado un activador de promoción posterior para iniciar la canalización de CI/CD de AWS. AccuRev La versión correcta para el

cambio de flujo de un proyecto se puede convertir en su flujo principal para realizar más pruebas de regresión.

Por lo general, el flujo principal se denomina flujo de integración del sistema. Cuando hay un ascenso de un flujo de proyectos a una secuencia de integración de sistemas, una activación posterior a la promoción inicia otra canalización de CI/CD para ejecutar pruebas de regresión.

Además del código de mainframe, este patrón incluye CloudFormation plantillas de AWS, documentos de Systems Manager Automation y scripts. Siguiendo las prácticas infrastructure-as-code recomendadas, están controladas por versiones en AWS. CodeCommit

Si necesita volver a sincronizar el código del mainframe con un entorno de mainframe para su implementación, Micro Focus proporciona la solución Enterprise Sync, que sincroniza el código del SCM con el AccuRev SCM del mainframe.

2. Entornos de desarrollo y pruebas

En una organización grande, escalar más de cien o incluso más de mil desarrolladores de mainframe es todo un desafío. Para abordar esta restricción, el patrón utiliza instancias Windows de Amazon EC2 para el desarrollo. En las instancias, están instaladas las herramientas Micro Focus Enterprise Developer para Eclipse. El desarrollador puede realizar todas las pruebas y depuraciones del código del mainframe de forma local en la instancia.

Los documentos de AWS Systems Manager, State Manager y Automation se utilizan para automatizar el aprovisionamiento de instancias para desarrolladores. El tiempo medio para crear una instancia de desarrollador es de 15 minutos. Se han preparado el software y las configuraciones siguientes.

- AccuRev Cliente de Windows para comprobar y guardar el código fuente AccuRev
- Herramienta Micro Focus Enterprise Developers para Eclipse, para escribir, probar y depurar el código de mainframe de forma local
- Marcos de pruebas de código abierto, pruebas de desarrollo impulsado por el comportamiento (BDD) de Python, marco de prueba Behave, py3270 y el emulador x3270 para crear scripts para probar aplicaciones
- Una herramienta de desarrollo de Docker para crear la imagen de Docker de Enterprise Test Server y probar la aplicación en el contenedor de Docker de Enterprise Test Server

En el ciclo de desarrollo, los desarrolladores utilizan la instancia EC2 para desarrollar y probar el código del mainframe de forma local. Cuando los cambios locales se prueban correctamente, los desarrolladores promueven el cambio en el AccuRev servidor.

3. Canalización de CI/CD

En este patrón, las canalizaciones de CI/CD se utilizan para las pruebas de integración y las pruebas de regresión antes de la implementación en el entorno de producción.

Como se explica en la sección SCM, AccuRev utiliza dos tipos de flujos: un flujo de proyecto y un flujo de integración. Cada flujo está enlazado con canalizaciones de CI/CD. Para realizar la integración entre el AccuRev servidor y AWS CodePipeline, el patrón utiliza un script AccuRev posterior a la promoción para crear un evento que inicie la CI/CD.

Por ejemplo, cuando un desarrollador promueve un cambio en la transmisión de un proyecto AccuRev, inicia un guion posterior a la promoción para que se ejecute en Server. AccuRev A continuación, el script carga los metadatos del cambio a un bucket de Amazon Simple Storage Service (Amazon S3) para crear un evento de Amazon S3. Este evento iniciará la ejecución de una canalización CodePipeline configurada.

El mismo mecanismo de inicio de eventos se utiliza para el flujo de integración y sus canalizaciones asociadas.

En la canalización de CI/CD, se CodePipeline utiliza CodeBuild con el contenedor de clientes AccuRev Linux de Micro Focus para extraer el código más reciente de las AccuRev transmisiones. A continuación, se empieza CodeBuild a utilizar el contenedor de Windows para desarrolladores de Micro Focus Enterprise para compilar el código fuente y a utilizar el contenedor de Windows de Micro Focus Enterprise Test Server CodeBuild para probar las aplicaciones de mainframe.

Las canalizaciones de CI/CD se crean con CloudFormation plantillas de AWS y el plano se utilizará para nuevos proyectos. Al usar las plantillas, un proyecto tarda menos de una hora en crear una nueva canalización de CI/CD en AWS.

Para escalar la capacidad de pruebas de mainframe en AWS, el patrón crea el conjunto de DevOps pruebas Micro Focus, Micro Focus Verastream y el servidor Micro Focus UFT. Con las DevOps herramientas modernas, puede ejecutar tantas pruebas en AWS como necesite.

En el siguiente diagrama se muestra un ejemplo de entorno de desarrollo de mainframe con Micro Focus en AWS.

Pila de tecnología de destino

En esta sección se ofrece una visión más detallada de la arquitectura de cada componente del patrón.

1. Repositorio de código fuente: AccuRev SCM

Micro Focus AccuRev SCM está configurado para gestionar las versiones del código fuente del mainframe. Para una alta disponibilidad, AccuRev admite los modos principal y de réplica. Los operadores pueden realizar una conmutación por error a la réplica cuando realizan tareas de mantenimiento en el nodo principal.

Para acelerar la respuesta de la canalización de CI/CD, el patrón utiliza Amazon CloudWatch Events para detectar los cambios en el código fuente e iniciar el inicio de la canalización.

1. CodePipeline Está configurado para usar una fuente de Amazon S3.
2. Se configura una regla de CloudWatch eventos para capturar los eventos de S3 de un bucket de S3 de origen.
3. La regla de CloudWatch eventos establece un objetivo para la canalización.
4. AccuRev SCM está configurado para ejecutar un script posterior a la promoción de forma local una vez finalizada la promoción.
5. AccuRev SCM genera un archivo XML que contiene los metadatos de la promoción y el script carga el archivo XML en el depósito S3 de origen.
6. Tras la carga, el bucket de S3 de origen envía los eventos para que coincidan con la regla de CloudWatch eventos y la regla de CloudWatch eventos inicia la CodePipeline ejecución.

Cuando la canalización se ejecuta, inicia un CodeBuild proyecto para utilizar un contenedor cliente de AccuRev Linux para extraer el código más reciente del mainframe de una transmisión asociada. AccuRev

El siguiente diagrama muestra la configuración de un AccuRev servidor.

2. Plantilla para desarrolladores empresariales

El patrón utiliza plantillas de Amazon EC2 para simplificar la creación de la instancia de desarrollador. Al utilizar State Manager, puede aplicar la configuración de software y licencia a las instancias EC2 de forma coherente.

La plantilla Amazon EC2 incluye su configuración de contexto de VPC y su configuración de instancia predeterminada, y cumple con los requisitos de etiquetado empresarial. Al usar una plantilla, un equipo puede crear sus propias instancias de desarrollo nuevas.

Cuando se inicia una instancia de desarrollador, mediante la asociación con etiquetas, Systems Manager usa State Manager para aplicar la automatización. La automatización incluye los siguientes pasos generales.

1. Instale el software Micro Focus Enterprise Developer e instale los parches.
2. Instale el AccuRev cliente Micro Focus para Windows.
3. Instale el script preconfigurado para que los desarrolladores se unan a la AccuRev transmisión. Inicialice los espacios de trabajo de Eclipse.
4. Instale las herramientas de desarrollo, incluidas x3270, py3270 y Docker.
5. Configure los ajustes de la licencia para que apunten a un equilibrador de carga de Micro Focus License Manager.

El siguiente diagrama muestra una instancia de desarrollador empresarial creada por la plantilla Amazon EC2, con el software y la configuración aplicados a la instancia por State Manager. Las instancias de desarrolladores empresariales se conectan a Micro Focus License Manager para activar su licencia.

3. Canalización de CI/CD

Como se explica en la sección de arquitectura de AWS, en el patrón hay canalizaciones de CI/CD a nivel de proyecto y canalizaciones de integración de sistemas. Cada equipo de proyecto de mainframe crea una o varias canalizaciones de CI/CD para compilar los programas que está desarrollando en un proyecto. Estas canalizaciones de CI/CD de proyectos extraen el código fuente de una transmisión asociada. AccuRev

En un equipo de proyecto, los desarrolladores promocionan su código en la transmisión asociada. AccuRev A continuación, la promoción inicia la cartera de proyectos para crear el código y ejecutar las pruebas de integración.

Cada canalización de CI/CD de CodeBuild proyectos utiliza proyectos con la imagen Amazon ECR de la herramienta para desarrolladores de Micro Focus Enterprise y la imagen Amazon ECR de la herramienta Micro Focus Enterprise Test Server.

CodePipeline y CodeBuild se utilizan para crear las canalizaciones de CI/CDS. Como CodeBuild no CodePipeline hay comisiones ni compromisos por adelantado, solo pagas por lo que utilizas. En comparación con el hardware de mainframe, la solución de AWS reduce considerablemente el tiempo de entrega del aprovisionamiento de hardware y reduce el costo del entorno de pruebas.

En el desarrollo moderno, se utilizan múltiples metodologías de prueba. Por ejemplo, el desarrollo basado en pruebas (TDD), el BDD y Robot Framework. Con este patrón, los desarrolladores pueden usar estas herramientas modernas para realizar pruebas de mainframe. Por ejemplo, si utiliza x3270, py3270 y la herramienta de prueba Behave python, puede definir el comportamiento de una aplicación en línea. También puede utilizar una compilación para mainframe de 3270 Robot Framework en estas canalizaciones de CI/CD.

En el siguiente diagrama se muestra la canalización de CI/CD de flujo de equipo.

El siguiente diagrama muestra el informe de prueba de CI/CD del proyecto elaborado por Mainframe3270 Robot CodePipeline Framework.

El siguiente diagrama muestra el informe de prueba de CI/CD del proyecto elaborado por Py3270 y Behave BDD. CodePipeline

Una vez superadas las pruebas a nivel de proyecto, el código probado se transfiere manualmente al flujo de integración de SCM. AccuRev Puede automatizar este paso una vez que los equipos confíen en la cobertura de las pruebas de su cartera de proyectos.

Cuando se promueve el código, la canalización de CI/CD de integración del sistema comprueba el código fusionado y realiza pruebas de regresión. El código fusionado se promueve desde todos los flujos de proyectos paralelos.

En función de lo preciso que sea necesario el entorno de prueba, los clientes pueden disponer de más canalizaciones de CI/CD de integración de sistemas en distintos entornos, por ejemplo, UAT o preproducción.

Por lo general, las herramientas utilizadas en el proceso de integración de sistemas son Micro Focus Enterprise Test Server, Micro Focus UFT Server y Micro Focus Verastream. Todas estas herramientas se pueden implementar en el contenedor de Docker y usarse con ellas. CodeBuild

Tras probar satisfactoriamente los programas del mainframe, el artefacto se almacena, con el control de versiones, en un bucket de S3.

En el siguiente diagrama se muestra una canalización de CI/CD de integración de sistemas.

Una vez que el artefacto se haya probado correctamente en las canalizaciones de CI/CD de integración del sistema, podrá promocionarse para su implementación en producción.

Si necesita volver a implementar el código fuente en el mainframe, Micro Focus ofrece la solución Enterprise Sync para sincronizar el código fuente desde el mainframe AccuRev Endeavour.

El siguiente diagrama muestra una canalización de CI/CD de producción que implementa el artefacto en los servidores empresariales de Micro Focus. En este ejemplo, CodeDeploy organiza el despliegue del artefacto de mainframe probado en Micro Focus Enterprise Server.

Además del tutorial sobre la arquitectura de la canalización de CI/CD, también puede leer la entrada del DevOps blog de AWS Automatice miles de pruebas de mainframe en AWS con Micro Focus Enterprise Suite para obtener más información sobre las pruebas de aplicaciones de mainframe en y. CodeBuild CodePipeline Consulte la entrada del blog para conocer las prácticas recomendadas y los detalles sobre la realización de pruebas de mainframe en AWS.

Herramientas

Herramientas

Herramientas de automatización de AWS

- AWS CloudFormation

- CloudWatch Eventos de Amazon
- AWS CodeBuild
- AWS CodeDeploy
- AWS CodePipeline
- Amazon ECR
- Amazon S3
- AWS Secrets Manager
- AWS Systems Manager

Herramientas de Micro Focus

- Desarrollador empresarial de Micro Focus para Eclipse
- Servidor de pruebas Micro Focus Enterprise
- Servidor empresarial de Micro Focus (implementación en producción)
- Micro Focus AccuRev
- Administrador de licencias de Micro Focus
- Integrador de host de Micro Focus Verastream
- Micro Focus UFT One

Otras herramientas

- x3270
- py3270
- Robot-Framework-Mainframe-3270-Library

Epics

Cree la infraestructura AccuRev SCM

Tarea	Descripción	Habilidades requeridas
Implemente un servidor AccuRev SCM principal		AWS CloudFormation

Tarea	Descripción	Habilidades requeridas
mediante AWS CloudForm ation.		
Cree el usuario AccuRev administrador.	Inicie sesión en el servidor AccuRev SCM y ejecute el comando CLI para crear un usuario administrador.	AccuRev Administrador del servidor SCM
Crea AccuRev transmisiones.	Cree AccuRev flujos que hereden de los flujos superiore s en secuencia: flujos de producción, integración de sistemas y equipos.	AccuRev Administrador de SCM
Cree las cuentas de inicio de AccuRev sesión del desarroll ador.	Utilice los comandos CLI de AccuRev SCM para crear cuentas de inicio de sesión de AccuRev usuarios para desarrolladores de mainframe.	AccuRev Administrador de SCM

Crear la plantilla de lanzamiento de Enterprise Developer para Amazon EC2

Tarea	Descripción	Habilidades requeridas
Implemente la plantilla de lanzamiento de Amazon EC2 mediante AWS. CloudForm ation	Utilice AWS CloudFormation para implementar una plantilla de lanzamiento de Amazon EC2 para las instancias de Micro Focus Enterprise Developer. La plantilla incluye un documento de automatiz ación de Systems Manager para la instancia de Micro Focus Enterprise Developer.	AWS CloudFormation

Tarea	Descripción	Habilidades requeridas
Cree la instancia Enterpris e Developer a partir de la plantilla de Amazon EC2.		Habilidades de desarrollador de mainframe y inicio de sesión en la consola de AWS

Crear la imagen de Docker de la herramienta para desarrolladores empresariales de Micro Focus

Tarea	Descripción	Habilidades requeridas
Cree la imagen de Docker de la herramienta para desarroll adores empresariales de Micro Focus.	Utilice el comando de Docker y la herramienta Dockerfil e de la herramienta para desarrolladores de Micro Focus Enterprise para crear la imagen de Docker.	Docker
Cree el repositorio de Docker en Amazon ECR.	En la consola de Amazon ECR, cree el repositorio para la imagen de Docker para desarrolladores de Micro Focus Enterprise.	Amazon ECR
Envíe la imagen de Docker de Micro Focus Enterprise Developer a Amazon ECR.	Ejecute el comando push de Docker para enviar la imagen de Docker de la herramien ta para desarrolladores empresariales y guardarla en el repositorio de Docker de Amazon ECR.	Docker

Crear la imagen de Docker de Micro Focus Enterprise Test Server

Tarea	Descripción	Habilidades requeridas
Cree la imagen de Docker de Micro Focus Enterprise Test Server.	Utilice el comando de Docker y el Dockerfile de Micro Focus Enterprise Test Server para crear la imagen de Docker.	Docker
Cree el repositorio de Docker en Amazon ECR.	En la consola de Amazon ECR, cree el repositorio de Amazon ECR para la imagen de Docker del servidor de pruebas de Micro Focus Enterprise.	Amazon ECR
Envíe la imagen de Docker del Micro Focus Enterprise Test Server a Amazon ECR.	Ejecute el comando push de Docker para enviar y guardar la imagen de Docker del Enterprise Test Server en Amazon ECR.	Docker

Crear la canalización de CI/CD de flujo de equipo

Tarea	Descripción	Habilidades requeridas
Cree el CodeCommit repositorio de AWS.	En la CodeCommit consola, cree un repositorio basado en Git para la infraestructura y el CloudFormation código de AWS.	AWS CodeCommit
Cargue la CloudFormation plantilla de AWS y el código de automatización en el CodeCommit repositorio.	Ejecute el comando Git push para cargar la CloudFormation plantilla de AWS y el código de automatización en el repositorio.	Git

Tarea	Descripción	Habilidades requeridas
Implemente la canalización de CI/CD en equipo mediante. CloudFormation	Utilice la CloudFormation plantilla de AWS preparada para implementar una canalización de CI/CD para streaming en equipo.	AWS CloudFormation

Crear la canalización de CI/CD de integración del sistema

Tarea	Descripción	Habilidades requeridas
Cree la imagen de Docker UFT de Micro Focus.	Utilice el comando Docker y el Dockerfile UFT de Micro Focus para crear la imagen de Docker de Micro Focus.	Docker
Cree el repositorio de Docker en Amazon ECR para la imagen UFT de Micro Focus.	En la consola Amazon ECR, cree el repositorio de Docker para la imagen UFT de Micro Focus.	Amazon ECR
Envíe la imagen de Docker de Micro Focus UFT a Amazon ECR.	Ejecute el comando push de Docker para enviar y guardar la imagen de Docker del Enterprise Test Server en Amazon ECR.	Docker
Cree la imagen de Docker Verastream de Micro Focus.	Utilice el comando de Docker y el Dockerfile Verastream de Micro Focus para crear la imagen de Docker.	Docker
Cree el repositorio de Docker en Amazon ECR para la imagen Verastream de Micro Focus.	En la consola Amazon ECR, cree el repositorio de Docker para la imagen Verastream de Micro Focus.	Amazon ECR

Tarea	Descripción	Habilidades requeridas
Implemente la canalizac ión de CI/CD de integraci ón de sistemas mediante. CloudFormation	Utilice la CloudFormation plantilla de AWS preparada para implementar una canalización de CI/CD de integración de sistemas.	AWS CloudFormation

Crear canalización de CI/CD para implementación de producción

Tarea	Descripción	Habilidades requeridas
Implemente Micro Focus Enterprise Server mediante AWS Quick Start.	Para implementar Micro Focus Enterprise Server mediante AWS CloudFormation, inicie Micro Focus Enterprise Server en AWS Quick Start.	AWS CloudFormation
Implemente un canalización de CI/CD para una implement ación de producción.	En la CloudFormation consola de AWS, utilice la CloudForm ation plantilla de AWS para implementar una canalización de CI/CD para una implement ación de producción.	AWS CloudFormation

Recursos relacionados

Referencias

- DevOps Blog de AWS: Automatice miles de pruebas de mainframe en AWS con la suite Micro Focus Enterprise
- repositorio py3270/py3270 GitHub
- Repositorio de bibliotecas GitHub Altran-PT-GDC/Robot-Framework-Mainframe-3270
- ¡Bienvenido a Behave!
- Blog de socios de APN - Etiqueta: Micro Focus

- Lanzamiento de una instancia desde una plantilla de lanzamiento

AWS Marketplace

- Micro Focus UFT One

AWS Quick Start

- Micro Focus Enterprise Server en AWS

Preserve el espacio IP enrutable en los diseños de VPC de varias cuentas para subredes que no son de carga de trabajo

Creado por Adam Spicer (AWS)

Repositorio de código: patrón CIDR secundario no enrutable	Entorno: producción	Tecnologías: infraestructura DevOps; gestión y gobierno; redes
Servicios de AWS: AWS Transit Gateway; Amazon VPC; Elastic Load Balancing (ELB)		

Resumen

Amazon Web Services (AWS) ha publicado prácticas recomendadas que animan a usar subredes dedicadas en una nube privada virtual (VPC) tanto para conexiones de puerta de enlace de tránsito como para los puntos de conexión del equilibrador de carga de la puerta de enlace (para admitir AWS Network Firewall o dispositivos de terceros). Estas subredes se utilizan para contener interfaces de red elásticas para estos servicios. Si utiliza AWS Transit Gateway y una puerta de enlace de equilibrador de carga, se crean dos subredes en cada zona de disponibilidad para la VPC. Debido a la forma en que están diseñadas las VPC, estas subredes adicionales no pueden ser más pequeñas que una máscara de /28 y pueden consumir un valioso espacio IP enrutable que, de otro modo, podría usarse para cargas de trabajo enrutables. Este patrón muestra cómo se puede utilizar un rango de enrutamiento entre dominios sin clase (CIDR) secundario y no enrutable para estas subredes dedicadas a fin de ayudar a preservar el espacio IP enrutable.

Requisitos previos y limitaciones

Requisitos previos

- Estrategia de múltiples VPC para un espacio IP enrutable
- Un rango de CIDR no enrutable para los servicios que está utilizando (conexión de puerta de enlace de tránsito y conexiones al equilibrador de carga de la puerta de enlace o puntos de conexión de Network Firewall)

Arquitectura

Arquitectura de destino

Este patrón incluye dos arquitecturas de referencia: una arquitectura tiene subredes para la conexión de puerta de enlace de tránsito (TGW) y un punto de conexión de equilibrador de carga de la puerta de enlace (GWLbE), y la segunda arquitectura tiene subredes solo para las conexiones de la TGW.

Arquitectura 1: VPC conectada a TGW-con enrutamiento de entrada a un dispositivo

El siguiente diagrama representa una arquitectura de referencia para una VPC que abarca dos zonas de disponibilidad. Al entrar, la VPC utiliza un patrón de enrutamiento de entrada para dirigir el tráfico destinado a la subred pública a bump-in-the-wire un dispositivo para inspeccionar el firewall. Un adjunto de TGW admite la salida de las subredes privadas a una VPC independiente.

Este patrón utiliza un rango CIDR no enrutable para la subred adjunta de TGW y la subred GWLbE. En la tabla de enrutamiento de TGW, este CIDR no enrutable se configura con una ruta de agujero negro (estática) mediante un conjunto de rutas más específicas. Si las rutas se propagaran a la tabla de enrutamiento de TGW, se aplicarían estas rutas de agujero negro más específicas.

En este ejemplo, el CIDR enrutable /23 se divide y se asigna completamente a las subredes enrutables.

Arquitectura 2: VPC adjunta a TGW

El siguiente diagrama representa otra arquitectura de referencia para una VPC que abarca dos zonas de disponibilidad. Una conexión de TGW admite el tráfico de salida (egreso) de las subredes privadas a una VPC independiente. Utiliza un rango CIDR no enrutable solo para la subred de conexión de TGW. En la tabla de enrutamiento de TGW, este CIDR no enrutable se configura con una ruta de agujero negro mediante un conjunto de rutas más específicas. Si las rutas se propagaran a la tabla de enrutamiento de TGW, se aplicarían estas rutas de agujero negro más específicas.

En este ejemplo, el CIDR enrutable /23 se divide y se asigna completamente a las subredes enrutables.

Herramientas

Servicios y recursos de AWS

- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esta red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS. En este patrón, los CIDR secundarios de VPC se utilizan para preservar el espacio IP enrutable en los CIDR de carga de trabajo.
- El enrutamiento de ingreso de la puerta de enlace de Internet (asociaciones de periferia) se puede utilizar junto con los puntos de conexión del equilibrador de carga de la puerta de enlace para subredes dedicadas no enrutables.
- AWS Transit Gateway es un concentrador central que conecta las VPC y las redes en las instalaciones. En este patrón, las VPC se conectan centralmente a una puerta de enlace de tránsito y las conexiones de puerta de enlace de tránsito se encuentran en una subred dedicada no enrutable.
- Los equilibradores de carga de la puerta de enlace permiten implementar, escalar y administrar dispositivos virtuales, como firewalls, sistemas de prevención y detección de intrusiones así como sistemas de inspección profunda de paquetes. La puerta de enlace sirve como punto único de entrada y salida para todo el tráfico. En este patrón, los puntos de conexión de un equilibrador de carga de puerta de enlace se pueden usar en una subred dedicada no enrutable.
- AWS Network Firewall es un servicio de detección y prevención de intrusiones y de firewall de red con estado y administrado para nubes privadas virtuales (VPC) en la nube de AWS. En este patrón, los puntos de conexión de un firewall se pueden usar en una subred dedicada no enrutable.

Repositorio de código

En el repositorio de patrones CIDR secundarios GitHub no enrutables hay un manual y CloudFormation plantillas de AWS para este patrón. Puede usar los archivos de muestra para configurar un laboratorio de trabajo en su entorno.

Prácticas recomendadas

AWS Transit Gateway

- Utilice una subred independiente para cada archivo asociado a la VPC de la puerta de enlace de tránsito.
- Asigne una subred /28 del rango CIDR secundario no enrutable para las subredes de conexión de puerta de enlace de tránsito.

- En cada tabla de enrutamiento de la puerta de enlace de tránsito, añada una ruta estática más específica para el rango CIDR no enrutable como agujero negro.

Equilibrador de carga de puerta de enlace y enrutamiento de ingreso

- Utilice el enrutamiento de ingreso para dirigir el tráfico de Internet a los puntos de conexión del equilibrador de carga de puerta de enlace.
- Utilice una subred independiente para cada punto de conexión del equilibrador de carga de puerta de enlace.
- Asigne una subred /28 del rango CIDR secundario no enrutable para las subredes de punto de conexión de puerta de enlace del equilibrador de carga.

Epics

Creación de VPCs

Tarea	Descripción	Habilidades requeridas
Determine el rango CIDR no enrutable.	Determine un rango CIDR no enrutable que se utilizará para la subred de conexión de puerta de enlace de tránsito y (opcionalmente) para cualquier subred de punto de conexión de equilibrador de carga de puerta de enlace o Network Firewall. Este rango de CIDR se utilizará como CIDR secundario para la VPC. No debe poder enrutarse desde el rango CIDR principal de la VPC ni desde la red más amplia.	Arquitecto de la nube
Determine los rangos CIDR enrutables para las VPC.	Determine un conjunto de rangos CIDR enrutables que	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	se utilizarán para sus VPC. Este rango CIDR se utilizará como el CIDR principal de sus VPC.	
Cree VPCs.	Cree las VPC y conéctela s a la puerta de enlace de tránsito. Cada VPC debe tener un rango CIDR principal que se pueda enrutar y un rango CIDR secundario que no se pueda enrutar, según los rangos que haya determinado en los dos pasos anteriores.	Arquitecto de la nube

Configuración de las rutas de agujeros negros de puerta de enlace de tránsito

Tarea	Descripción	Habilidades requeridas
Cree CIDR no enrutables más específicos como agujeros negros.	Cada tabla de enrutamie nto de las puerta de enlace de tránsito debe tener un conjunto de rutas de agujeros negros creadas para los CIDR no enrutables. Están configurados para garantiza r que el tráfico del CIDR de la VPC secundaria no se pueda enrutar y no se filtre a la red más amplia. Estas rutas deben ser más específicas que el CIDR no enrutable que se establece como el CIDR secundario en la VPC. Por ejemplo, si el CIDR secundari	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	o no enrutable es 100.64.0.0/26, las rutas de agujero negro de la tabla de enrutamiento de la puerta de enlace de tránsito deberían ser 100.64.0.0/27 y 100.64.0.32/27.	

Recursos relacionados

- Prácticas recomendadas para implementar el Equilibrador de carga de puerta de enlace
- Arquitecturas de inspección distribuida con el Equilibrador de carga de puerta de enlace
- Día de inmersión en redes: laboratorio de firewall de Internet a VPC
- Prácticas recomendadas de diseño de una puerta de enlace de tránsito

Información adicional

El rango CIDR secundario no enrutable también puede resultar útil cuando se trabaja con implementaciones de contenedores de mayor escala que requieren un gran conjunto de direcciones IP. Puede utilizar este patrón con una puerta de enlace NAT privada para utilizar una subred no enrutable para alojar las implementaciones de contenedores. Para obtener más información, consulte la entrada de blog sobre cómo resolver el agotamiento de la IP privada con una solución de NAT privada.

Aprovisione un producto Terraform en AWS Service Catalog mediante un repositorio de código

Creado por el Dr. Rahul Sharad Gaikwad (AWS) y Tamilselvan (AWS)

Entorno: PoC o piloto	Tecnologías: infraestructura; DevOps	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: AWS Service Catalog; Amazon EC2		

Resumen

AWS Service Catalog admite el aprovisionamiento de autoservicio con gobernanza para sus configuraciones de HashiCorp Terraform. Si usa Terraform, puede usar Service Catalog como la única herramienta para organizar, gobernar y distribuir sus configuraciones de Terraform en AWS a escala. Puede acceder a las funciones clave de Service Catalog, como la catalogación de plantillas de infraestructura como código (IaC) estandarizadas y previamente aprobadas, el control de acceso, el aprovisionamiento de recursos en la nube con el acceso más mínimo, el control de versiones, el uso compartido con miles de cuentas de AWS y el etiquetado. Los usuarios finales, como ingenieros, administradores de bases de datos y científicos de datos, consultan una lista de productos y versiones a los que tienen acceso y pueden implementarlos con una sola acción.

Este patrón le ayuda a implementar los recursos de AWS mediante el código de Terraform. Se accede al código de Terraform del GitHub repositorio a través de Service Catalog. Con este enfoque, usted integra los productos con sus flujos de trabajo de Terraform existentes. Los administradores pueden crear carteras de Service Catalog y añadirles productos de AWS Launch Wizard mediante Terraform.

Los beneficios de esta solución son los siguientes:

- Gracias a la función de reversión de Service Catalog, si se produce algún problema durante la implementación, puede revertir el producto a una versión anterior.
- Puede identificar fácilmente las diferencias entre las versiones del producto. Esto le ayuda a resolver los problemas durante la implementación.

- Puede configurar una conexión a un repositorio en el catálogo de servicios, por ejemplo GitHub GitLab, a o AWS CodeCommit. Puede realizar cambios en el producto directamente a través del repositorio.

Para obtener información sobre las ventajas generales de AWS Service Catalog, consulte Qué es Service Catalog.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Un GitHub repositorio u otro que contenga archivos de configuración de Terraform en formato ZIP. BitBucket
- Interfaz de línea de comandos del modelo de aplicaciones sin servidor de AWS (AWS SAM CLI), instalada.
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada.
- Vamos, instalado.
- Python versión 3.9, instalada. La AWS SAM CLI requiere esta versión de Python.
- Permisos para escribir y ejecutar funciones de AWS Lambda y permisos para acceder a los productos y carteras de Service Catalog y administrarlos.

Arquitectura

Pila de tecnología de destino

- AWS Service Catalog
- AWS Lambda

Arquitectura de destino

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Cuando la configuración de Terraform está lista, un desarrollador crea un archivo.zip que contiene todo el código de Terraform. El desarrollador carga el archivo.zip en el repositorio de código que está conectado a Service Catalog.
2. Un administrador asocia el producto Terraform a una cartera de Service Catalog. El administrador también crea una restricción de lanzamiento que permite a los usuarios finales aprovisionar el producto.
3. En Service Catalog, los usuarios finales lanzan los recursos de AWS mediante la configuración de Terraform. Pueden elegir la versión del producto que desean implementar.

Herramientas

Servicios y herramientas de AWS

- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Service Catalog le ayuda a administrar de forma centralizada los catálogos de servicios de TI aprobados para AWS. Los usuarios finales pueden implementar rápidamente solo los servicios de TI aprobados que necesitan, de acuerdo con las limitaciones establecidas por su organización.

Otros servicios

- Go es un lenguaje de programación de código abierto compatible con Google.
- Python es un lenguaje de programación informático de uso general.

Repositorio de código

Si necesita ejemplos de configuraciones de Terraform que pueda implementar a través de Service Catalog, puede usar las configuraciones del repositorio GitHub Amazon Macie Organization Setup Using Terraform. No es necesario utilizar los ejemplos de código de este repositorio.

Prácticas recomendadas

- En lugar de proporcionar los valores de las variables en el archivo de configuración de Terraform (`terraform.tfvars`), configure los valores de las variables al lanzar el producto a través de Service Catalog.
- Conceda acceso a la cartera solo a usuarios o administradores específicos.
- Siga el principio de privilegios mínimos y conceda los permisos mínimos necesarios para realizar una tarea. Para obtener más información, consulte Otorgar privilegio mínimo y Prácticas recomendadas de seguridad en la documentación de IAM.

Epics

Configure su equipo de trabajo local

Tarea	Descripción	Habilidades requeridas
(Opcional) Instale Docker.	Si desea ejecutar las funciones de AWS Lambda en su entorno de desarroll o, instale Docker. Para ver instrucciones, consulte Install Docker Engine (Instalar motor de Docker) en la documenta ción de Docker.	DevOps ingeniero
Instale el motor de AWS Service Catalog para Terraform.	1. Introduzca el siguiente comando para clonar el repositorio AWS Service Catalog Engine for Terraform. `git clone https://g ithub.com/aws-samp les/service-catalo g-engine-for-terra form-os.git`	DevOps ingeniero, administr ador de AWS

Tarea	Descripción	Habilidades requeridas
	2. Navegue hasta el directorio raíz del repositorio clonado. 3. Escriba el siguiente comando. Esto instala el motor. `run ./bin/bash/deploy-tre.sh -r` La región de AWS establecida en su perfil predeterminado no se utiliza durante la instalación automática. En su lugar, debe proporcionar la región al ejecutar este comando.	

Conectar el GitHub repositorio

Tarea	Descripción	Habilidades requeridas
Cree una conexión con el GitHub repositorio.	1. Inicie sesión en la consola de administración de AWS y, a continuación, abra la consola de herramientas para desarrolladores. Para acceder a la consola de herramientas para desarrolladores, elija un servicio como AWS CodePipeline CodeCommit, AWS o AWS CodeDeploy. 2. En el panel de navegación izquierdo, seleccion	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	a Configuración y, a continuación, selecciona Conexiones. 3. Seleccione Crear conexión. 4. Seleccione el repositor io en el que mantiene el código fuente de Terraform . Por ejemplo, puede elegir Bitbucket o GitHub Enterprise Server. GitHub 5. Introduzca un nombre para la conexión y, a continuac ión, seleccione Connect. 6. Cuando se le pida, autentique el repositorio. Una vez completada la autenticación, se crea la conexión y el estado cambia a activo.	

Cree un producto de Terraform en Service Catalog

Tarea	Descripción	Habilidades requeridas
Cree el producto Service Catalog.	1. Abra la consola de AWS Service Catalog. 2. Vaya a la sección de Administración y, a continuación, seleccione Lista de productos. 3. Seleccione Crear producto.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	4. En la página Crear producto, en la sección Detalles del producto, elija el tipo de producto externo. Service Catalog utiliza este tipo de producto para respaldar los productos de Terraform Community Edition. 5. Introduzca un nombre y un propietario para el producto Service Catalog. 6. Seleccione Especifique su repositorio de códigos mediante un CodeStar proveedor. 7. Introduce la siguiente información para tu repositorio: • Conéctese a su proveedor mediante AWS CodeConnections: seleccione la conexión que creó anteriormente. • Repositorio: seleccione el repositorio. • Sucursal: seleccione la rama. • Ruta del archivo de plantilla: elija la ruta en la que se almacena el archivo de plantilla de código. El nombre del	

Tarea	Descripción	Habilidades requeridas
	archivo debe terminar `portar.gz`. 8. En Nombre y descripción de la versión, proporciona información sobre la versión del producto. 9. Seleccione Crear producto.	
Cree una cartera.	1. Abra la consola de AWS Service Catalog. 2. Vaya a la sección Administración y, a continuación, elija Portafolios. 3. Selecciona Crear cartera 4. Escriba los siguientes valores: • Portfolio name: `Sample terraform` • Descripción de la cartera – `Sample portfolio for Terraform configurations` • Propietario: tu información de contacto, como el correo electrónico 5. Seleccione Crear.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Agregue el producto Terraform a la cartera.	1. Abra la consola de AWS Service Catalog. 2. Vaya a la sección de Administración y, a continuación, seleccione Lista de productos. 3. Seleccione el producto Terraform que creó anteriormente. 4. Elija Acciones y, a continuación, elija Agregar producto a la cartera. 5. Elige la `Sample terraform` cartera. 6. Seleccione Añadir producto a la cartera.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Cree la política de acceso.	1. Abra la consola de AWS Identity and Access Management (IAM). 2. En el panel de navegación, seleccione Políticas. 3. En el panel de contenido , elija Create policy (Crear política). 4. Elija la opción JSON. 5. Introduzca el ejemplo de política de JSON en la política de acceso, en la sección de información adicional de este patrón. 6. Elija Siguiente. 7. En la página Revisar y crear, en el cuadro Nombre de la política, escriba`TerraformResourceCreationAndArtifactAccessPolicy` . 8. Elija Crear política.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Cree una política de confianza personalizada.	1. Abra la consola de AWS Identity and Access Management (IAM). 2. Seleccione Roles en el panel de navegación. 3. Elija Crear rol. 4. En Tipo de entidad de confianza, elija Política de confianza personalizada. 5. En el editor de políticas de JSON, introduce el ejemplo de política de JSON en Política de confianza en la sección de información adicional de este patrón. 6. Elija Siguiente. 7. En Políticas de permisos, elige la `TerraformResourceCreationAndArtifactAccessPolicy` que hayas creado anteriormente. 8. Elija Siguiente. 9. En Detalles del rol, en el cuadro Nombre del rol, escriba `SCLaunch-product` . Importante: El nombre del rol debe empezar por `SCLaunch`. 10. Seleccione Crear rol.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Añada una restricción de lanzamiento al producto Service Catalog.	1. Inicie sesión en la consola de administración de AWS como usuario con permisos administrativos. 2. Abra la consola de AWS Service Catalog. 3. En el panel de navegación, elija Portfolios. 4. Elija la cartera que creó anteriormente. 5. En la página Detalles de la cartera, elija la pestaña Restricciones y, a continuación, elija Crear restricción. 6. En Producto, selecciona el producto Terraform que creaste anteriormente. 7. En Restricción de lanzamiento, en Método, elija Introducir el nombre del rol. 8. En el cuadro Nombre del rol, escriba `SCLaunch-product` . 9. Seleccione Crear.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Conceda acceso al producto.	1. Abra la consola de AWS Service Catalog. 2. En el panel de navegación, elija Portfolios. 3. Elija la cartera que creó anteriormente. 4. Seleccione la pestaña Acceso y, a continuación, elija Conceder acceso. 5. Elija la pestaña Funciones y, a continuación, seleccione la función a la que debe tener acceso para implementar este producto. 6. Elija Grant access (Conceder acceso).	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Lance el producto.	1. Inicie sesión en la consola de administración de AWS como usuario con permisos para implement ar el producto Service Catalog. 2. Abra la consola de AWS Service Catalog. 3. En el panel de navegación, elija Productos. 4. Elija el producto que creó anteriormente y, a continuación, elija Lanzar producto. 5. Introduzca un nombre de producto y defina los parámetros necesarios. 6. Seleccione Lanzar producto.	DevOps ingeniero

Verifique la implementación

Tarea	Descripción	Habilidades requeridas
Valide la implementación.	Existen dos máquinas de estados de AWS Step Functions para el flujo de trabajo de aprovisionamiento de Service Catalog: • `ManageProvisionedP roductStateMachine` —Service Catalog invoca	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	esta máquina de estados al aprovisionar un nuevo producto de Terraform y al actualizar un producto aprovisionado de Terraform existente. • `TerminateProvisionedProductStateMachine` —Service Catalog invoca esta máquina de estados al cancelar un producto aprovisionado por Terraform existente. Se comprueban los registros de la máquina de `ManageProvisionedProductStateMachine` estados para confirmar que el producto se ha aprovisionado. 1. Inicie sesión en la consola de administración de AWS y, a continuación, abra la consola AWS Step Functions. 2. En el panel de navegación izquierdo, elija State machines. 3. Elija `ManageProvisionedProductStateMachine` . 4. En la lista de ejecuciones, introduzca el ID del	

Tarea	Descripción	Habilidades requeridas
	producto aprovisionado para localizar la ejecución. Nota: Los nombres de los buckets de backend de los archivos de estado comienzan por. `sc-terraform-engine-state-` 5. Valide que se hayan creado todos los recursos necesarios en la cuenta.	

Limpiar la infraestructura

Tarea	Descripción	Habilidades requeridas
Elimine los productos aprovisionados.	1. Inicie sesión en la consola de administración de AWS como usuario con permisos para implement ar el producto Service Catalog. 2. Abra la consola de AWS Service Catalog. 3. En el menú de navegació n de la izquierda, elija Productos aprovisionados. 4. Seleccione el producto que ha creado. 5. En la lista de acciones, elija Finalizar.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	6. En el cuadro de texto de confirmación, introduzca `yterminate` , a continuación, seleccione Finalizar el producto aprovisionado. 7. Repita estos pasos para cancelar todos los productos aprovisionados.	

Tarea	Descripción	Habilidades requeridas
Elimine el motor de AWS Service Catalog para Terraform.	1. Inicie sesión en la consola de administración de AWS como usuario con permisos administrativos. 2. Abra la consola de Amazon S3. 3. En el panel de navegación, elija Buckets. 4. Seleccione el `sc-terraform-engine-logging-XXXX` depósito. 5. Selecciona Vacío. 6. Repita los pasos 4 y 5 para los siguientes cubos: • `sc-terraform-engine-state-XXXX` • `terraform-engine-bootstrap-XXXX` 7. Abra la CloudFormation consola de AWS y, a continuación, compruebe que se encuentra en la región de AWS correcta. 8. En la barra de navegación de la izquierda, selecciona Stacks. 9. Selecciona y`SAM-TRE`, a continuación, elige Eliminar. Espere a que se elimine la pila. 10. Seleccione y`Bootstrap-TRE`, a continuación, elija	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	Eliminar. Espere a que se elimine la pila.	

Recursos relacionados

Documentación de AWS

- Cómo empezar con un producto de Terraform

Documentación de Terraform

- Instalación de Terraform
- Configuración del backend de Terraform
- Documentación para proveedores de Terraform AWS

Información adicional

Política de acceso

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "s3:ExistingObjectTag/servicecatalog:provisioning": "true"
                }
            }
        },
        {
            "Action": [
                "s3:CreateBucket*",
                "s3:DeleteBucket*",
```

```
                "s3:Get*",
                "s3:List*",
                "s3:PutBucketTagging"
            ],
            "Resource": "arn:aws:s3:::*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "resource-groups:CreateGroup",
                "resource-groups:ListGroupResources",
                "resource-groups:DeleteGroup",
                "resource-groups:Tag"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "tag:GetResources",
                "tag:GetTagKeys",
                "tag:GetTagValues",
                "tag:TagResources",
                "tag:UntagResources"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

Política de confianza

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GivePermissionsToServiceCatalog",
            "Effect": "Allow",
            "Principal": {
                "Service": "servicecatalog.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
```

```
        },
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::account_id:root"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::accounti_id:role/TerraformEngine/
TerraformExecutionRole*",
                        "arn:aws:iam::accounti_id:role/TerraformEngine/
ServiceCatalogExternalParameterParserRole*",
                        "arn:aws:iam::accounti_id:role/TerraformEngine/
ServiceCatalogTerraformOSParameterParserRole*"
                    ]
                }
            }
        }
    ]
}
```

Registre varias cuentas de AWS con una sola dirección de correo electrónico mediante Amazon SES

Creado por Joe Wozniak (AWS) y Shubhangi Vishwakarma (AWS)

Repositorio de código: GitHub aws-account-factory-email	Entorno: PoC o piloto	Tecnologías: infraestructura; gestión y gobierno; mensajería y comunicacione
Servicios de AWS: Amazon DynamoDB; AWS Lambda; Amazon SES		

Resumen

Este patrón describe cómo puede desvincular las direcciones de correo electrónico reales de la dirección de correo electrónico asociada a una cuenta de AWS. Las cuentas de AWS requieren que se proporcione una dirección de correo electrónico única en el momento de la creación de la cuenta. En algunas organizaciones, el equipo que administra las cuentas de AWS debe asumir la carga de administrar muchas direcciones de correo electrónico únicas con su equipo de mensajería. Esto puede resultar difícil para las grandes organizaciones que administran muchas cuentas de AWS.

Este patrón proporciona una solución de venta de direcciones de correo electrónico única que permite a los propietarios de cuentas de AWS asociar una dirección de correo electrónico a varias cuentas de AWS. A continuación, las direcciones de correo electrónico reales de los propietarios de las cuentas de AWS se asocian a estas direcciones de correo electrónico generadas en una tabla. La solución gestiona todo el correo entrante de las cuentas de correo electrónico únicas, busca al propietario de cada cuenta y, a continuación, reenvía los mensajes recibidos al propietario.

Requisitos previos y limitaciones

Requisitos previos

- Acceso administrativo a una cuenta de AWS.
- Acceso a un entorno de desarrollo. Le recomendamos que utilice AWS Cloud9 para evitar tener que configurar usted mismo las herramientas y claves de acceso necesarias.

- (Opcional) Estar familiarizado con los flujos de trabajo del AWS Cloud Development Kit (AWS CDK) y el lenguaje de programación Python le ayudará a solucionar cualquier problema o a realizar modificaciones.

Limitaciones

- La longitud total de la dirección de correo electrónico vendida es de 64 caracteres. Para obtener más información, consulte CreateAccountla referencia de la API de AWS Organizations.

Versiones de producto

- Node.js versión 12.7.0 o posterior
- Python 3.9 o posterior
- Paquetes de Python pip y virtualenv
- CDK de AWS, versión 2.23.0 o posterior
- Docker, versión 20.10x o posterior

Arquitectura

Pila de tecnología de destino

- CloudFormation Pila de AWS
- Funciones de AWS Lambda
- Reglas y conjunto de reglas de Amazon Simple Email Address (Amazon SES)
- Roles y políticas de AWS Identity and Access Management (IAM)
- Un bucket de Amazon Simple Storage Service (Amazon S3) y política de bucket
- Política de claves y claves de AWS Key Management Service (AWS KMS)
- Tema de Amazon Simple Notification Service (Amazon SNS) y política de temas
- Tabla de Amazon DynamoDB

Arquitectura de destino

En este diagrama se muestran dos flujos:

- Flujo de venta de direcciones de correo electrónico: en el diagrama, el flujo de venta de direcciones de correo electrónico (sección inferior) comienza normalmente con una solución de venta de cuentas o con una automatización externa, o se invoca manualmente. En la solicitud, se llama a una función de Lambda con una carga útil que contiene los metadatos necesarios. La función utiliza esta información para generar un nombre de cuenta y una dirección de correo electrónico únicos, los almacena en una base de datos de DynamoDB y devuelve los valores a la persona que llama. Luego, estos valores se pueden usar para crear una nueva cuenta de AWS (normalmente, mediante AWS Organizations).
- Flujo de reenvío de correo electrónico: este flujo se ilustra en la sección superior del diagrama anterior. Cuando se crea una cuenta de AWS mediante el correo electrónico de la cuenta generado a partir del flujo de venta de direcciones de correo electrónico, AWS envía varios correos electrónicos, como la confirmación de registro de la cuenta y las notificaciones periódicas, a esa dirección de correo electrónico. Siguiendo los pasos de este patrón, se configura la cuenta de AWS con Amazon SES para recibir correos electrónicos de todo el dominio. Esta solución configura reglas de reenvío que permiten a Lambda procesar todos los correos electrónicos entrantes, comprobar si la dirección T0 está en la tabla de DynamoDB y, en su lugar, reenviar el mensaje a la dirección de correo electrónico del propietario de la cuenta. El uso de este proceso permite a los propietarios de las cuentas asociar varias cuentas a una sola dirección de correo electrónico.

Automatizar y escalar

Este patrón utiliza la CDK de AWS para automatizar completamente la implementación. La solución utiliza los servicios gestionados de AWS que se escalarán automáticamente (o se pueden configurar para) adaptarse a sus necesidades. Es posible que las funciones de Lambda requieran una configuración adicional para satisfacer sus necesidades de escalado. Para obtener más información, consulte escalado de funciones de Lambda en la documentación de Lambda.

Herramientas

Servicios de AWS

- AWS Cloud9 es un entorno de desarrollo integrado (IDE) que ayuda a codificar, crear, ejecutar, probar y depurar software. También ayuda a lanzar software a la nube de AWS.
- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.

- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.
- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Key Management Service (AWS KMS) facilita poder crear y controlar claves criptográficas para proteger los datos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Email Service (Amazon SES) facilita poder enviar y recibir correos electrónicos a través de los dominios y direcciones de correo electrónico propios.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Herramientas necesarias para la implementación

- Entorno de desarrollo con acceso a la CLI de AWS y a la IAM a su cuenta de AWS. Para obtener más información, consulte los enlaces de la sección recursos relacionados. Le recomendamos que utilice AWS Cloud9 para simplificar el proceso de configuración.
- Si usa AWS Cloud9, se configurará lo siguiente para usted. Si decide no utilizar AWS Cloud9, tendrá que instalar lo siguiente:
  - La CLI de AWS para configurar las credenciales de acceso a la CDK de AWS. Para obtener más información, consulte la documentación de la CLI de AWS.
  - Python, versión 3.9 o posterior
  - Paquetes de Python pip y virtualenv
  - Node.js versión 12.7.0 o posterior
  - CDK de AWS, versión 2.23.0 o posterior

- Docker, versión 20.10.x o posterior

Código

El código de este patrón está disponible en el repositorio de correo electrónico de la fábrica de cuentas de GitHub AWS.

Epics

Asigne un entorno de implementación objetivo

Tarea	Descripción	Habilidades requeridas
Identificar o crear una cuenta de AWS.	Identifique una cuenta de AWS existente o nueva a la que tenga acceso administrativo completo para implementar la solución de correo electrónico.	Administrador de la nube, administrador de AWS
Configure un entorno de implementación.	Configure un entorno de implementación fácil de usar y configure las dependencias siguiendo estos pasos: 1. Implemente una instancia de AWS Cloud9 como un entorno de implementación dedicado. Consulte Introducción a AWS Cloud9 para obtener instrucciones. 2. Clone la GitHub base de códigos del repositorio de correo electrónico de fábrica de cuentas de AWS en la instancia de AWS Cloud9 mediante el comando:	AWS DevOps, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`git clone https://github.com/aws-samples/aws-account-factory-email` 3. En el archivo `requirements.txt` (en la raíz del repositorio), actualice la línea que comienza con `aws-cdk-lib==` para que coincida con la versión de la CDK de AWS que se ejecuta en su entorno. Para identificar la versión, utilice el comando `cdk --version` .	

Configuración de un dominio verificado

Tarea	Descripción	Habilidades requeridas
Identifique y asigne un dominio.	La funcionalidad de reenvío de correo electrónico requiere un dominio dedicado. Identifique y asigne un dominio o subdominio que pueda verificar con Amazon SES. Este dominio debe estar disponible para recibir correo electrónico entrante en la cuenta de AWS en la que esté implementada la solución de reenvío de correo electrónico. Requisitos del dominio:	Administrador de la nube, administrador de redes, administrador de DNS

Tarea	Descripción	Habilidades requeridas
	• El dominio debe ser un dominio o subdominio estándar. • El dominio debe poder resolverse mediante DNS de forma externa, ya que se utilizará para recibir correos electrónicos de personas ajenas a la organización.	
Compruebe el dominio.	Compruebe que el dominio identificado se puede utilizar para aceptar el correo entrante. Complete las instrucciones de Verificación de su dominio para la recepción de correos electrónicos de Amazon SES en la documentación de Amazon SES. Esto requerirá la coordinación con la persona o el equipo responsable de los registros de DNS del dominio.	Desarrollador de aplicaciones, AWS DevOps

Tarea	Descripción	Habilidades requeridas
Configure los registros MX.	Configure su dominio con registros MX que apunten a los puntos de conexión de Amazon SES de su cuenta y región de AWS. Para obtener más información, consulte Publicar un registro MX para la recepción de correos electrónicos de Amazon SES en la documentación de Amazon SES.	Administrador de la nube, administrador de redes, administrador de DNS

Implemente la solución de venta y reenvío de correo electrónico

Tarea	Descripción	Habilidades requeridas
Modifique los valores predeterminados en cdk.json.	Edite algunos de los valores predeterminados del archivo `cdk.json` (en la raíz del repositorio) para que la solución funcione correctam ente una vez implementada. 1. Modifique el valor `SES_DOMAIN_NAME` para que coincida con el nombre de dominio que verificó anteriormente. 2. Modifique el valor `ADDRESS_FROM` para incluir el mismo dominio en el que se encuentra `SES_DOMAIN_NAME` . Su equipo de nube debe	Desarrollador de aplicaciones, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	determinar la parte local de la dirección. Esta dirección se convierte en la dirección `FROM` de todos los correos electrónicos que se reenvían a través de la solución. 3. Modifique el valor `ADDRESS_ADMIN` para que coincida con la dirección de correo electrónico a la que se reenviarán los mensajes entrantes que no coincidan . Este valor debe ser una dirección de correo electrónico válida y operativa.	

Tarea	Descripción	Habilidades requeridas
Implemente la solución de venta y reenvío de correo electrónico.	1. Cree un entorno virtual Python: `python -m venv .venv` 2. Active el entorno virtual Python: `source .venv/bin/activate` O bien, en la plataforma Windows, utilice: `% .venv\Scripts\activate.bat` 3. Instale todos los requisitos de Python sin errores: `pip install -r requirements.txt` 4. Sintetice la CloudFormation plantilla: `cdk synth` Confirme que no hay errores y que la CloudFormation plantilla completa contiene el resultado esperado. 5. (Opcional) Si va a implementar el código CDK de AWS en la cuenta	Desarrollador de aplicaciones, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	o región de AWS actual por primera vez, inicie el entorno. Para obtener más información, consulte Proceso de arranque en la documentación de CDK de AWS. `cdk bootstrap aws://AWS-ACCOUNT-NUMBER/REGION` Sustituya `AWS-ACCOUNT-NUMBER` y `REGION` por valores reales. 6. Implemente la solución: `cdk bootstrap` `cdk deploy` Los comandos deberían completarse sin errores.	

Tarea	Descripción	Habilidades requeridas
Compruebe que la solución se haya implementado.	Compruebe que la solución se ha implementado correctam ente antes de comenzar las pruebas: 1. Abra la CloudForm ation consola de AWS y busque una CloudForm ation pila que contenga el nombre`AwsMailFw dStack` . 2. Confirme que esta pila `AwsMailFwdStack` tenga los siguientes recursos: • Funciones de Lambda • Regla y conjunto de reglas de Amazon SES • Roles y políticas de IAM • Política de bucket y bucket de Amazon S3 • Clave y política de claves de AWS KMS • Tema y política de Amazon SNS • Tabla de DynamoDB	Desarrollador de aplicaciones, AWS DevOps

Compruebe que la venta y el reenvío de correo electrónico funcionan según lo previsto

Tarea	Descripción	Habilidades requeridas
Verifique que la API está en funcionamiento.	En este paso, debe enviar los datos de prueba a la API de la solución y confirmar	Desarrollador de aplicaciones, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	que la solución produce el resultado esperado y que las operaciones de backend se han realizado según lo previsto. Ejecute manualmente la función Vend Email de la función de Lambda mediante una entrada de prueba. (Para ver un ejemplo, consulte el archivo sample_vend_request.json). Para `OwnerAddress` , utilice una dirección de correo electrónico válida. La API debería devolver el nombre de la cuenta y el correo electrónico de la cuenta con los valores esperados.	

Tarea	Descripción	Habilidades requeridas
Compruebe que el correo electrónico se está reenviando.	En este paso, envía un correo electrónico de prueba a través del sistema y comprueba que el correo electrónico se ha reenviado al destinatario previsto. 1. Obtenga el correo electrónico de la cuenta del último paso. 2. Envíe un correo electrónico a esta dirección con el tema de la prueba y el cuerpo del texto. 3. Confirme que recibió el correo electrónico en la dirección de correo electrónico del propietario de la cuenta. 4. Confirme que el correo electrónico que ha recibido tiene una dirección `FROM` que coincide con la configuración `ADDRESS_FROM` indicada en `cdk.json`. 5. Confirme que el asunto y el cuerpo del correo electrónico recibido son los mismos que los del mensaje enviado originalmente.	Desarrollador de aplicaciones, AWS DevOps

Solución de problemas

Problema	Solución
El sistema no reenvía el correo electrónico como se esperaba.	Compruebe que la configuración es correcta: 1. Debería haber completado el proceso de verificación de Amazon SES para su dominio. 2. Su dominio debe estar configurado correctamente con registros MX que apunten a los puntos de conexión de Amazon SES de su cuenta y región de AWS. Para obtener más información, consulte Publicar un registro MX para la recepción de correos electrónicos de Amazon SES en la documentación de Amazon SES. Después de verificar la configuración de dominio, siga estos pasos: 1. Abra la CloudWatch consola de AWS de la cuenta y la región en las que implement ó la solución y navegue hasta los grupos de CloudWatch registros en el panel de navegación. 2. Busque en la lista de los grupos de registros para `SesMailForwardLogGroup` . 3. Investigue los registros de este grupo para ver si se ha generado algún error durante el proceso de venta y reenvío de correo electrónico.
Cuando intenta implementar la pila de CDK de AWS, recibe un error similar al siguiente:	En la mayoría de las instancias, este mensaje de error significa que la región a la que se dirige no tiene todos los servicios de AWS

Problema	Solución
“Error de formato de plantilla: tipos de recursos no reconocidos”	disponibles. Si utiliza AWS Cloud9 para implementar la solución, es posible que se dirija a una región diferente de la región en la que se ejecuta la instancia de AWS Cloud9. Nota: De forma predeterminada, la CDK de AWS se implementa en la región y la cuenta que configuró en la CLI de AWS. Posibles soluciones: 1. Consulte los servicios de AWS por región para comprobar si todos los servicios necesarios para esta solución (consulte la sección sobre la pila de tecnología destino que aparece más arriba en este patrón) se encuentran en la región de AWS a la que se dirige revisando servicios de AWS según región. 2. Si utiliza AWS Cloud9 y se dirige a una región diferente de la región en la que se ejecuta su instancia de AWS Cloud9, asegúrese de configurar la variable de entorno `AWS_DEFAULT_REGION` o establecer una región con la CLI de AWS antes de implementar la solución. Para obtener más información, consulte Variables de entorno para configurar la CLI de AWS en la documentación de la CLI de AWS. Como alternativa, puede modificar el archivo `app.py` en la raíz del repositorio para incluir un ID y región de cuenta de codificación rígida y una región siguiendo las instrucci ones de la documentación de CDK de AWS para entornos.

Problema	Solución
Al implementar la solución, recibirá el siguiente mensaje de error: «Falló la implementación: Error AwsMailFwdStack: no se encontró el parámetro SSM /cdk-bootstrap/hnb659fds/version. ¿Arrancó el entorno? Ejecute 'cdk bootstrap'"	Si nunca ha implementado ningún recurso de CDK de AWS en la cuenta y región de AWS a la que se dirige, primero tendrá que ejecutar el comando `cdk bootstrap` , tal y como indica el error. Si sigue recibiendo este error después de ejecutar el comando de arranque, es posible que esté intentando implementar la solución en una región distinta de la región en la que se ejecuta la instancia de AWS Cloud9. Para resolver este problema, defina la variable de entorno `AWS_DEFAULT_REGION` o defina una región con la CLI de AWS antes de implementar la solución. Como alternativa, puede modificar el archivo `app.py` en la raíz del repositorio para incluir un ID y región de cuenta de codificación rígida y una región siguiendo las instrucciones de la documentación de CDK de AWS para entornos.

Recursos relacionados

- Para obtener ayuda para instalar la CLI de AWS, consulte Instalación o actualización de la versión más reciente de la CLI AWS.
- Para obtener ayuda para configurar la CLI de AWS con las credenciales de acceso de IAM, consulte Configurar la CLI de AWS.
- Para obtener ayuda con la CDK de AWS, consulte Introducción a la CDK de AWS.

Información adicional

Costos

Al implementar esta solución, el titular de la cuenta de AWS puede incurrir en costos asociados al uso de los siguientes servicios. Es importante que comprenda cómo se facturan estos servicios para

estar al tanto de los posibles cargos. Para obtener información sobre precios, consulte las siguientes páginas:

- Precios de Amazon SES
- Precios de Amazon S3
- Precios de AWS Cloud9
- Precios de AWS KMS
- Precios de AWS Lambda
- Precios de Amazon DynamoDB

Configure la resolución de DNS para redes híbridas en un entorno de AWS de varias cuentas

Creado por Amir Durrani

Entorno: producción	Tecnologías: infraestructura; redes	Servicios de AWS: AWS RAM; Amazon Route 53; AWS Control Tower

Resumen

Este patrón describe cómo puede utilizar los servicios del Sistema de nombres de dominio (DNS) en las instalaciones con las reglas de Amazon Route 53 Resolver y los puntos de conexión salientes del Resolver para la resolución de nombres.

El DNS es fundamental para establecer y mantener las comunicaciones entre los entornos de red. Si tiene un entorno de conectividad de red híbrida, puede compartir servicios de red esenciales, como DNS y Active Directory, sin la carga operativa que supone administrar un entorno distribuido entre cuentas y nubes privadas virtuales (VPC). Este enfoque lo ayuda a crear y dar soporte a aplicaciones que abarcan un gran número de cuentas. Por ejemplo, si tiene cientos o miles de cuentas multirregionales con requisitos de conectividad híbrida, puede compartir los servicios de DNS de forma segura y eficiente en todos los entornos conectados de su organización de AWS.

El DNS es fundamental para las redes IP en todos los niveles (web, aplicaciones y bases de datos) de una aplicación. Se recomienda dar acceso total a este recurso únicamente al equipo de expertos en DNS para configurar, operar y dar soporte a este recurso. En un entorno de conectividad híbrida, puede seguir utilizando el DNS en las instalaciones para las solicitudes de resolución de nombres que se originen en recursos que residen en diferentes cuentas mediante el reenvío condicional.

Este patrón cubre la resolución de DNS híbrido en un entorno de varias cuentas de AWS. Para una única cuenta, consulte el patrón Configurar la resolución de DNS para redes híbridas en un entorno de AWS de una sola cuenta.

Requisitos previos y limitaciones

Requisitos previos

- Un entorno de varias cuentas de AWS que se basa en las prácticas recomendadas y que se ha creado con la AWS Control Tower. El diagrama de la siguiente sección muestra la arquitectura típica de un entorno de este tipo.
- Infraestructura de enrutamiento escalable entre las cuentas y las VPC mediante AWS Transit Gateway.
- Los puntos de conexión salientes de Resolver y las reglas de Resolver utilizan Amazon Route 53.
- Recursos compartidos para las reglas de resolución salientes mediante AWS Resource Access Manager (AWS RAM).

Arquitectura

Arquitectura de varias cuentas en AWS

Pila de tecnología de destino

- Una infraestructura de DNS en las instalaciones existente para la resolución de nombres salientes en una gran cantidad de entidades principales de AWS
- Reglas de Route 53 Resolver y puntos de conexión de salida de Resolver.
- RAM de AWS para compartir las reglas de Route 53 Resolver con otras entidades principales de AWS dentro y fuera de la organización de AWS

Arquitectura de destino

El siguiente diagrama describe los pasos para configurar la resolución de DNS end-to-end híbrida. La RAM de AWS se utiliza para compartir las reglas de Route 53 Resolver y los puntos de conexión del Resolver, que se configuran y administran desde la cuenta central de Shared Services. Los puntos de conexión de Route 53 Resolver están configurados para que cada zona de disponibilidad reciba las solicitudes de resolución de nombres salientes de los recursos que residen en el centro de datos en las instalaciones y, a continuación, reenvíen estas solicitudes a los solucionadores de DNS en las instalaciones. Los solucionadores de DNS en las instalaciones envían las respuestas de resolución de nombres a los puntos de conexión de salida, que luego las reenvían al solucionador de VPC. Estos pasos establecen end-to-end la comunicación mediante el uso de nombres de host en lugar de direcciones IP.

El siguiente diagrama muestra la arquitectura con más detalle.

Automatizar y escalar

Puede configurar y compartir las reglas de Route 53 Resolver a través de la RAM de AWS mediante CloudFormation plantillas de AWS.

Herramientas

Servicios de AWS

- AWS Control Tower le ayuda a configurar y regular un entorno de cuentas múltiples de AWS siguiendo las prácticas recomendadas prescriptivas.
- AWS Resource Access Manager (AWS RAM) lo ayuda a compartir sus recursos de forma segura entre las cuentas de AWS para reducir los gastos operativos y brindar visibilidad y auditabilidad.
- Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad.

Herramientas adicionales

- nslookup y dig son utilidades para consultar registros de DNS.

Epics

Configure los puntos de conexión y las reglas del Resolver

Tarea	Descripción	Habilidades requeridas
Configure los puntos de conexión y las reglas del Resolver saliente de Route 53.	1. Inicie sesión en la consola de administración de AWS correspondiente a la cuenta de AWS desde la que desea configurar y desde la que desea compartir la regla de resolución saliente de Route 53.	AWS general

Tarea	Descripción	Habilidades requeridas
	2. Abra la consola de Route 53 en https://console.aws.amazon.com/route53/. 3. En la barra de navegación, elija la región en la que desea configurar un punto de conexión del Resolver. 4. En el panel de navegación, seleccione Outbound endpoints (Puntos de conexión de salida) y, a continuación, elija Configure endpoints (Configurar puntos de conexión). 5. Proporcione la configuración general, las direcciones IP y la información de etiquetas opcional y, a continuación, seleccione Siguiente. 6. Cree una o más reglas para especificar los nombres de dominio de las consultas de DNS que quiere reenviar a su red y, a continuación, seleccione Save (Guardar). Para más información, consulte Reenvío de consultas de DNS de salida a la red en	

Tarea	Descripción	Habilidades requeridas
	la documentación de Route 53.	

Tarea	Descripción	Habilidades requeridas
Cree y comparta las reglas de resolución saliente de Route 53 con las entidades principales de AWS.	1. Abra la consola RAM de AWS en https://console.aws.amazon.com/ram/. 2. En el panel de navegación, seleccione Resource shares (Recursos compartidos) y, a continuación, elija Create resource share (Crear recurso compartido). 3. Proporcione un nombre para compartir. 4. Para el tipo de recurso, elija Reglas de Resolver. 5. Elija la regla de resolución que desee compartir, proporcione la información opcional sobre la clave y el valor de la etiqueta y, a continuación, seleccione Siguiente. 6. Elija las entidades principales con las que desea compartir el recurso de reglas de Resolver. Las entidades principales pueden ser internos o externos a su organización de AWS. Por ejemplo, puede elegir su organización de AWS, una unidad organizativa (OU) específica de la organización o una cuenta específica.	AWS general

Tarea	Descripción	Habilidades requeridas
	7. Revise y cree el recurso compartido. Una vez creado y compartido el recurso, aparece en la sección Shared with me (Compartido conmigo) del panel de navegación de las entidades principales con las que se comparte. 8. Asocie las VPC de la cuenta (de entidad principal) a la regla Resolver que ha compartido la cuenta de red o de servicios compartidos. Para obtener más información, consulte Cómo compartir los recursos AWS en la documentación de AWS RAM.	
Pruebe la resolución de nombres DNS salientes.	Pruebe la resolución de nombres mediante la utilidad nslookup o dig en las instancias de una VPC de una cuenta con la que haya compartido la regla de resolución. La consulta debe resolverse en la dirección IP de un recurso que reside en el centro de datos en las instalaciones.	AWS general

Recursos relacionados

- Resolución de DNS locales en entornos híbridos (vídeo)
- Reenvío de consultas de DNS de salida a la red (documentación de Route 53)
- Cómo compartir sus recursos de AWS (documentación de RAM de AWS)

Configure la resolución de DNS para redes híbridas en un entorno de AWS de una sola cuenta

Creado por Abdullahi Olaoye (AWS)

Entorno: producción	Tecnologías: bases de datos; infraestructura	Servicios de AWS: Amazon Route 53; Amazon VPC

Resumen

Este patrón describe cómo configurar una arquitectura de sistema de nombres de dominio (DNS) totalmente híbrida que permita la resolución end-to-end mediante DNS de recursos locales, recursos de AWS y consultas de DNS de Internet, sin sobrecargas administrativas. El patrón describe cómo configurar las reglas de reenvío de Amazon Route 53 Resolver que determinan dónde debe enviarse una consulta de DNS que se origina en AWS, en función del nombre de dominio. Las consultas de DNS para los recursos en las instalaciones se reenvían a los solucionadores de DNS en las instalaciones. Route 53 Resolver resuelve las consultas de DNS para los recursos de AWS y las consultas de DNS de Internet.

Este patrón cubre la resolución de DNS híbrido en un entorno de cuenta única de AWS. Para obtener información sobre la configuración de consultas de DNS salientes en un entorno de varias cuentas de AWS, consulte el patrón Configurar la resolución de DNS para redes híbridas en un entorno de AWS de varias cuentas.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS
- Crear una nube privada virtual (VPC) en la cuenta de AWS.
- Conectividad de red entre el entorno en las instalaciones y VPC a través de los servicios de AWS Virtual Private Network (AWS VPN) o AWS Direct Connect
- Direcciones IP de sus resolutores de DNS en las instalaciones (accesibles desde su VPC)
- Nombre de dominio o subdominio para reenviar a los solucionadores en las instalaciones (por ejemplo, onprem.mydc.com)

- Nombre de dominio/subdominio de la zona alojada privada de AWS (por ejemplo, myvpc.cloud.com)

Arquitectura

Pila de tecnología de destino

- Zona alojada privada de Amazon Route 53
- Amazon Route 53 Resolver
- Amazon VPC
- AWS VPN o Direct Connect

Arquitectura de destino

Herramientas

- Amazon Route 53 Resolver facilita la nube híbrida a los clientes empresariales al permitir una resolución de consultas de DNS perfecta en toda la nube híbrida. Puede crear puntos de conexión de DNS y reglas de reenvío condicional para resolver los espacios de nombres de DNS entre su centro de datos en las instalaciones y sus VPC.
- Una zona alojada privada de Amazon Route 53 es un contenedor que aloja información acerca de cómo desea que responda Amazon Route 53 a las consultas de DNS de un dominio y sus subdominios en una o varias VPC que haya creado en el servicio Amazon VPC.

Epics

Configure una zona alojada privada

Tarea	Descripción	Habilidades requeridas
Cree una zona alojada privada de Route 53 para un nombre	Esta zona contiene los registros de DNS de los recursos de AWS que	Administrador de red, administrador del sistema

Tarea	Descripción	Habilidades requeridas
de dominio reservado de AWS, como myvpc.cloud.com.	deben resolverse desde el entorno en las instalaciones. Para obtener instrucciones, consulte Crear una zona alojada privada en la documentación de Route 53.	
Asocie esta zona alojada privada con la VPC de la VPC.	Para permitir que los recursos de la VPC resuelvan los registros DNS en esta zona alojada privada, debe asociar la VPC a la zona alojada. Para obtener instrucciones, consulte Crear una zona alojada privada en la documentación de Route 53.	Administrador de red, administrador del sistema

Configure los puntos de conexión de Route 53 Resolver

Tarea	Descripción	Habilidades requeridas
Crear un punto de conexión de entrada	Route 53 Resolver utiliza un punto de conexión de entrada para recibir las consultas de DNS de los solucionadores en las instalaciones. Para obtener instrucciones, consulte Reenvío de consultas de DNS de entrada a su VPC en la documentación de Route 53. Anote la dirección IP del punto de conexión entrante.	Administrador de red, administrador del sistema
Crear un punto de conexión de salida	Route 53 Resolver utiliza un punto de conexión de salida	Administrador de red, administrador del sistema

Tarea	Descripción	Habilidades requeridas
	para enviar las consultas de DNS de los soluciona dores en las instalaciones. Para obtener instrucciones, consulte Reenvío de consultas de DNS de salida a su red en la documentación de Route 53. Anote el ID del punto de conexión de salida.	

Configure una regla de reenvío y asóciela a su VPC

Tarea	Descripción	Habilidades requeridas
Crear una regla de reenvío para un dominio en las instalaciones	Esta regla indicará a Route 53 Resolver que reenvíe cualquier consulta de DNS para los dominios en las instalaciones (como onprem.mydc.com) a los solucionadores de DNS en las instalaciones. Para crear esta regla, necesitará las direccion es IP de los resolutores de DNS en las instalaciones y el ID del punto de conexión de salida de Route 53 Resolver. Para obtener instrucciones, consulte Administración de reglas de reenvío en la documentación de Route 53.	Administrador de red, administrador del sistema
Asocie la regla de reenvío a su VPC.	Para que la regla de reenvío entre en vigor, debe asociarla a su VPC. Luego, Route 53	Administrador de red, administrador del sistema

Tarea	Descripción	Habilidades requeridas
	Resolver tiene en cuenta la regla al resolver un dominio. Para obtener instrucciones, consulte Administración de reglas de reenvío en la documentación de Route 53.	

Configuración de solucionadores DNS en las instalaciones

Tarea	Descripción	Habilidades requeridas
Configure el reenvío condicional en los solucionadores de DNS en las instalaciones.	Para que las consultas de DNS se envíen a la zona alojada privada de Route 53 desde el entorno en las instalaciones, debe configurar el reenvío condicional en los solucionadores de DNS en las instalaciones. Esto indica a los solucionadores de DNS que reenvíen todas las consultas de DNS del dominio de AWS (por ejemplo, para myvpc.cloud.com) a la dirección IP del punto de conexión entrante de Route 53 Resolver.	Administrador de red, administrador del sistema

Pruebe la resolución de end-to-end DNS

Tarea	Descripción	Habilidades requeridas
Probar la resolución DNS desde AWS en el entorno en las instalaciones.	Desde un servidor de la VPC, realice una consulta de DNS para un dominio en las	Administrador de red, administrador del sistema

Tarea	Descripción	Habilidades requeridas
	instalaciones (como server1.onprem.mydc.com).	
Probar la resolución DNS desde AWS en el entorno en las instalaciones.	Desde un servidor en las instalaciones, realice la resolución de DNS para un dominio de AWS (como server1.myvpc.cloud.com).	Administrador de red, administrador del sistema

Recursos relacionados

- Administración centralizada de DNS de la nube híbrida con Amazon Route 53 y AWS Transit Gateway (AWS Transit Gateway (AWS Transit Gateway (Blog de AWS Networking y Content Delivery)
- Simplifique la administración de DNS en un entorno multicuenta con Route 53 Resolver (publicación del blog de AWS Security)
- Trabajar con zonas alojadas privadas (documentación de Route 53)
- Introducción a Route 53 Resolver (documentación de Route 53)

Configure automáticamente los bots de UiPath RPA en Amazon EC2 mediante AWS CloudFormation

Creado por el Dr. Rahul Sharad Gaikwad (AWS) y Tamilselvan (AWS)

Entorno: PoC o piloto	Tecnologías: infraestructura; DevOps	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon CloudWatch; Amazon EC2 Image Builder; AWS Systems Manager; AWS CloudFormation		

Resumen

Este patrón explica cómo puede implementar bots de automatización robótica de procesos (RPA) en instancias de Amazon Elastic Compute Cloud (Amazon EC2). Utiliza una canalización de Generador de imágenes de EC2 para crear una Imagen de máquina de Amazon (AMI) personalizada. Una AMI es una imagen de máquina virtual (VM) preconfigurada que contiene el sistema operativo (SO) y el software preinstalado para implementar instancias de EC2. Este patrón utiliza CloudFormation plantillas de AWS para instalar la edición UiPath Studio Community en la AMI personalizada. UiPath es una herramienta de RPA que le ayuda a configurar robots para automatizar sus tareas.

Como parte de esta solución, las instancias EC2 de Windows se lanzan mediante la AMI base y la aplicación UiPath Studio se instala en las instancias. El patrón utiliza la herramienta Microsoft System Preparation (Sysprep) para duplicar la instalación personalizada de Windows. Después, elimina la información del host y crea una AMI final de la instancia. A continuación, puede lanzar las instancias bajo demanda mediante la AMI final con sus propias convenciones de nomenclatura y configuración de supervisión.

Nota: Este patrón no proporciona ninguna información sobre el uso de bots de RPA. Para obtener esa información, consulte la UiPath documentación. También puedes usar este patrón para configurar otras aplicaciones de bots de RPA personalizando los pasos de instalación en función de tus necesidades.

Este patrón proporciona las siguientes automatizaciones y ventajas:

- Implementación y uso compartido de aplicaciones: puede crear AMI de Amazon EC2 para el despliegue de aplicaciones y compartirlas en varias cuentas a través de una canalización de EC2 Image Builder, que utiliza CloudFormation plantillas de AWS como scripts de infraestructura como código (IaC).
- Aprovisionamiento y escalado de Amazon EC2: las plantillas de CloudFormation IaC proporcionan secuencias de nombres de ordenadores personalizadas y automatizan las uniones de Active Directory.
- Observabilidad y supervisión: el patrón configura los CloudWatch paneles de Amazon para ayudarlo a monitorear las métricas de Amazon EC2 (como el uso de CPU y disco).
- Ventajas de la RPA para su empresa: la RPA mejora la precisión porque los robots pueden realizar las tareas asignadas de forma automática y coherente. La RPA también aumenta la velocidad y la productividad porque elimina las operaciones que no añaden valor y gestiona las actividades repetitivas.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Permisos de AWS Identity and Access Management (IAM) para implementar plantillas CloudFormation
- Políticas de IAM para configurar la distribución de AMI entre cuentas con Generador de imágenes de EC2

Arquitectura

1. El administrador proporciona la AMI de Windows básica en el `ec2-image-builder.yaml` archivo e implementa la pila en la CloudFormation consola.
2. La CloudFormation pila implementa la canalización de EC2 Image Builder, que incluye los siguientes recursos:
   - `Ec2ImageInfraConfiguration`

- `Ec2ImageComponent`
- `Ec2ImageRecipe`
- `Ec2AMI`

3. La canalización de EC2 Image Builder lanza una instancia EC2 temporal de Windows mediante la AMI base e instala los componentes necesarios (en este caso UiPath , Studio).
4. El Generador de imágenes de EC2 elimina toda la información del host y crea una AMI desde Windows Server.
5. Actualice el archivo `ec2-provisioning yaml` con la AMI personalizada y lance varias instancias de EC2 en función de sus requisitos.
6. La macro Count se implementa mediante una plantilla. CloudFormation Esta macro proporciona una propiedad Count para CloudFormation los recursos, de modo que puede especificar fácilmente varios recursos del mismo tipo.
7. Actualiza el nombre de la macro en el CloudFormation `ec2-provisioning.yaml` archivo y despliega la pila.
8. El administrador actualiza el archivo `ec2-provisioning.yaml` en función de los requisitos y lanza la pila.
9. La plantilla despliega instancias de EC2 con la aplicación UiPath Studio.

Herramientas

Servicios de AWS

- AWS le CloudFormation ayuda a modelar y gestionar los recursos de infraestructura de forma automatizada y segura.
- Amazon le CloudWatch ayuda a observar y supervisar los recursos y las aplicaciones en AWS, en las instalaciones y en otras nubes.
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad informática segura de tamaño variable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- El Generador de imágenes de EC2 simplifica la creación, las pruebas y la implementación de máquinas virtuales e imágenes de contenedores para su uso en AWS o en las instalaciones.
- Amazon le EventBridge ayuda a crear aplicaciones basadas en eventos a escala en AWS, sistemas existentes o aplicaciones de software como servicio (SaaS).

- AWS Identity and Access Management (IAM) le ayuda a controlar de forma segura el acceso a los recursos de AWS. Con IAM, puede administrar de forma centralizada los permisos que controlan a qué recursos de AWS pueden acceder los usuarios. Utilice IAM para controlar quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos.
- AWS Lambda es un servicio de computación controlado por eventos sin servidor que permite ejecutar código para prácticamente cualquier tipo de aplicación o servicio backend, sin aprovisionar ni administrar servidores. Puede utilizar funciones de Lambda desde más de 200 servicios de AWS y aplicaciones SaaS y pagar solo por el consumo realizado.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Systems Manager Agent (SSM Agent) ayuda al administrador de sistemas a actualizar, administrar y configurar instancias de EC2, dispositivos periféricos, servidores en las instalaciones y máquinas virtuales (VM).

Repositorios de código

El código de este patrón está disponible en la configuración del bot de GitHub UiPath RPA mediante el repositorio. CloudFormation El patrón también usa una macro que está disponible en el repositorio de CloudFormation macros de AWS.

Prácticas recomendadas

- AWS publica nuevas AMI de Windows cada mes. Contienen los últimos parches del sistema operativo, controladores y agentes de lanzamiento. Le recomendamos que aproveche las AMI más recientes al lanzar nuevas instancias o al crear sus propias imágenes personalizadas.
- Aplique todos los parches de seguridad disponibles para Windows o Linux durante la creación de imágenes.

Epics

Implemente una canalización de imágenes para la imagen base

Tarea	Descripción	Habilidades requeridas
Configure una canalización de Generador de imágenes de EC2.	1. Clone la configuración del bot de UiPath RPA mediante un CloudFormation repositorio o descargue la `ec2-image-builder.yaml` plantilla del repositorio. 2. Inicie sesión en la consola de administración de AWS y abra la CloudFormation consola de AWS. 3. Seleccione Crear pila. 4. En la sección Specify template (Especificar plantilla) seleccione Upload a template file (Cargar un archivo de plantilla). 5. Busque y cargue la plantilla `ec2-image-builder.yaml` desde su ordenador y, a continuación, seleccione Siguiente. 6. Proporcione parámetros de entrada para su pila o acepte los valores predeterminados. Elija Siguiente. Nota: El número y los valores de los parámetros	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	pueden variar en función de los valores de entrada. 7. Si lo desea, configure las opciones de pila y luego elija Siguiente. 8. Revise los detalles de la pila. 9. Al final de la pantalla, seleccione la casilla de verificación para confirmar las capacidades y, a continuación, seleccione Enviar. 10. Supervise el progreso de la pila. Cuando el estado sea `CREATE_COMPLETE` , la implementación estará lista.	

Tarea	Descripción	Habilidades requeridas
Puede ver la configuración de Generador de imágenes de EC2.	La configuración de Generador de imágenes de EC2 incluye la configuración de la infraestructura, la configuración de distribución y la configuración de escaneo de seguridad. Para ver la configuración: 1. Abra la consola de Generador de imágenes de EC2. 2. En el panel de navegación, vaya a varios ajustes de Generador de imágenes. Nota: Como práctica recomendada, las actualizaciones de EC2 Image Builder se deben realizar únicamente a través de CloudFormation la plantilla.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Puede ver la canalización de imágenes.	Para ver la canalización de imágenes desplegada: 1. En la consola Generador de imágenes de EC2, elija Canalizaciones de imágenes en el panel de navegación. 2. Seleccione la canalizac ión de imágenes que ha creado. 3. Vea los detalles de configuración de las imágenes de salida, la receta de la imagen, la configuración de la infraestr uctura, los ajustes de distribución, EventBridge las reglas de Amazon y las etiquetas.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Ver los registros de Generador de imágenes.	Los registros de EC2 Image Builder se agrupan CloudWatch en grupos de registros. Para ver los registros en CloudWatch: 1. Abra la consola de CloudWatch . 2. En el panel de navegación, seleccione Registros, Grupos de registros. 3. Seleccione el nombre del grupo de registros. Los registros de Generador de imágenes de EC2 se agregan al grupo de registros de `/aws/imagebuilder/XXX` . 4. Compruebe los registros más recientes del flujo de registro correspondiente para ver si se ha producido algún error al ejecutar la canalización de imágenes. Los registros de Generador de imágenes de EC2 también se almacenan en un bucket S3. Para consultar los registros en el bucket: 1. Abra la consola de Amazon S3.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	2. En la lista de Buckets, seleccione el nombre del bucket. Los registros se agregan en el bucket S3 `<stack-name>-XXXXX X` .	
Cargue el UiPath archivo en un bucket de S3.	1. Descargue el `.msi` archivo de UiPath Studio desde la ubicación https://download.uipath.com/UiPathStudioCommunity .msi. 2. Cargue el archivo qen un bucket de S3. 3. Actualice el nombre del bucket y la clave de archivo en la plantilla `ec2-image -builder.yaml` , en la sección de datos de usuario, línea 310.	AWS DevOps

Implementación y pruebas de la macro Count

Tarea	Descripción	Habilidades requeridas
Implemente la macro Count.	1. Clona o descarga la CloudFormation macro Count. 2. Vaya a la carpeta `Count`. 3. Necesitará un depósito S3 para almacenar los CloudFormation artefactos. Si aún no tiene un bucket	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	de S3 en, cree uno con el nombre `aws s3 mb s3://<bucket name>` . 4. Package la plantilla de la macro Count. La plantilla utiliza el modelo de aplicaciones sin servidor (SAM) de AWS, por lo que debe transformarse antes de poder implementarla. `aws cloudformation package \ --template-file template.yaml \ --s3-bucket <your bucket name here> \ --output-template-file packaged.yaml` Por ejemplo: `aws cloudformation package \ --template-file template.yaml \ --s3-bucket count-macro-ec2 \ --output-template-file packaged.yaml` 5. Implemente la plantilla empaquetada para crear una CloudFormation pila.	

Tarea	Descripción	Habilidades requeridas
	`aws cloudformation deploy \ --stack-name Count-macro \ --template-file packaged.yaml \ --capabilities CAPABILITY_IAM` Si quieres usar la consola, sigue las instrucciones de la epopeya anterior o de la CloudFormation documentación.	
Pruebe la macro Count.	Para probar las capacidades de la macro, intente iniciar la plantilla de ejemplo que se proporciona con la macro. `aws cloudformation deploy \ --stack-name Count-test \ --template-file test.yaml \ --capabilities CAPABILITY_IAM`	DevOps ingeniero

Implemente la CloudFormation pila para aprovisionar instancias con la imagen personalizada

Tarea	Descripción	Habilidades requeridas
Implemente la plantilla de aprovisionamiento de Amazon EC2.	Para implementar EC2 Image Pipeline mediante CloudFormation: 1. Descargue la `ec2-provisioning.yaml` plantilla del GitHub repositorio o ubíquela en su ordenador si ha clonado el repositorio. 2. Abra la consola de CloudFormation . 3. Repite los pasos de la primera epopeya (o sigue las instrucciones de la CloudFormation documentación) para realizar la implementación`ec2-provisioning.yaml` .	AWS DevOps
Puede ver la configuración de Amazon EC2.	La configuración de Amazon EC2 incluye configuraciones de seguridad, redes, almacenamiento, comprobaciones de estado, supervisión y etiquetas. Para ver estas configuraciones: 1. Abra la consola de Amazon EC2. 2. En el panel de navegación, elija Instancias y, a continuación, seleccione la instancia EC2 que creó	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	la plantilla de aprovisio namiento de Amazon EC2. 3. En el resumen de la instancia, seleccione las pestañas para ver la configuración de Amazon EC2 correspondiente.	
Vea el CloudWatch panel de control.	1. Abra la consola de CloudWatch . 2. En el panel de navegación, seleccione Paneles. 3. Elija el panel de control que tiene el nombre de su pila. Nota: Después de aprovisio nar la pila, se tarda un tiempo en rellenar el panel con las métricas. El panel proporciona las siguientes métricas: `CPUUtilization` , `DiskUtilization` , `MemoryUtilization` , `NetworkIn` , `NetworkOut` , `StatusCheckFailed` .	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Vea las métricas personalizadas del uso de memoria y disco.	1. En la CloudWatch consola, elija Dashboards. 2. En el panel de navegación, seleccione Métricas y, a continuación, Todas las métricas. 3. Elija Espacios de nombres personalizados, CWAgent.	AWS DevOps
Vea las alarmas de uso de memoria y disco.	1. En la CloudWatch consola, en el panel de navegación, elija Dashboards. 2. Seleccione All alarms (Todas las alarmas).	AWS DevOps
Verifique la regla del ciclo de vida de las instantáneas.	1. Abra la consola de Amazon EC2. 2. En el panel de navegación, seleccione Lifecycle Manager (Administrador de ciclo de vida). 3. Verifique la configuración del ciclo de vida de la AMI.	AWS DevOps

Eliminar el entorno (opcional)

Tarea	Descripción	Habilidades requeridas
Eliminar las pilas.	Cuando haya completado su PoC o su proyecto piloto, le recomendamos que elimine las pilas que ha creado para asegurarse de que no se le cobre por estos recursos.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	1. Abra la CloudFormation consola de AWS. 2. En el panel de navegación, seleccione Pilas y, a continuación, seleccione una o las dos pilas que creó anteriormente y que desee eliminar. La pila se debe estar ejecutando en este momento. 3. En el panel de detalles de la pila, seleccione Delete (Eliminar). 4. Cuando se le solicite, seleccione Delete stack (Eliminar pila). Importante: La operación de eliminación de la pila no se puede detener una vez que comienza. La pila avanza al estado `DELETE_IN_PROGRESS` . Si la eliminación ha fallado, la pila tendrá el estado `DELETE_FAILED` . Para obtener soluciones, consulte Fallos al eliminar una pila en la documentación de CloudFormation solución de problemas de AWS.	

Tarea	Descripción	Habilidades requeridas
	Para obtener información sobre cómo proteger las pilas para que no se eliminen accidentalmente, consulte Cómo proteger una pila para que no se elimine en la CloudFormation documentación de AWS.	

Solución de problemas

Problema	Solución
Al implementar la plantilla de aprovisionamiento de Amazon EC2, aparece el error: Se ha recibido una respuesta con un formato incorrecto o de transform 123xxxx::Count.	Se trata de un problema conocido. (Consulte la solución personalizada y las relaciones públicas en el repositorio de CloudFormation macros de AWS). Para solucionar este problema, abra la consola de AWS Lambda y actualice `index.py` con el contenido del GitHub repositorio.

Recursos relacionados

GitHub repositorios

- UiPath Configuración del bot RPA mediante CloudFormation
- Count Macro CloudFormation

Referencias de AWS

- Creación de una pila en la CloudFormation consola de AWS (CloudFormation documentación)
- Solución de problemas CloudFormation (CloudFormation documentación)

- Monitorizar métricas de memoria y disco para instancias de Amazon EC2 (documentación de Amazon EC2)
- ¿Cómo puedo usar el CloudWatch agente para ver las métricas del Monitor de rendimiento en un servidor Windows? (artículo de AWS Re:post)

Referencia adicional

- UiPath documentación
- Configuración del nombre de host en una SysPreped AMI (entrada de blog de Brian Beach)
- ¿Cómo hago para que Cloudformation reprocese una plantilla mediante una macro cuando cambian los parámetros? (Desbordamiento de pila)

Configure la recuperación ante desastres para Oracle JD Edwards EnterpriseOne con AWS Elastic Disaster Recovery

Creado por Thanigaivel Thirumalai (AWS)

Entorno: Producción	Tecnologías: infraestructura, migración, redes	Carga de trabajo: Oracle
Servicios de AWS: AWS Elastic Disaster Recovery; Amazon EC2		

Resumen

Los desastres provocados por catástrofes naturales, fallos en las aplicaciones o interrupciones de servicios son perjudiciales para los ingresos y provocan tiempo de inactividad en las aplicaciones corporativas. Para reducir las repercusiones de este tipo de eventos, la planificación de la recuperación ante desastres (DR) es fundamental para las empresas que adoptan los sistemas de planificación de recursos EnterpriseOne empresariales (ERP) de JD Edwards y otros programas de software de misión crítica y empresarial.

Este patrón explica cómo las empresas pueden utilizar AWS Elastic Disaster Recovery como una opción de recuperación ante desastres para sus EnterpriseOne aplicaciones de JD Edwards. También describe los pasos para utilizar la conmutación por error y la recuperación ante fallos de Elastic Disaster Recovery a fin de crear una estrategia de recuperación ante desastres entre regiones para las bases de datos alojadas en una instancia de Amazon Elastic Compute Cloud (Amazon EC2) en la nube de AWS.

Nota: este patrón requiere que las regiones principal y secundaria para la implementación de DR entre regiones se alojen en AWS.

Oracle JD Edwards EnterpriseOne es una solución de software ERP integrada para empresas medianas y grandes de una amplia gama de sectores.

AWS Elastic Disaster Recovery minimiza el tiempo de inactividad y la pérdida de datos con una recuperación rápida y fiable de aplicaciones locales y basadas en la nube mediante el uso de un almacenamiento asequible, un cálculo y point-in-time una recuperación mínimos.

AWS proporciona cuatro patrones de arquitectura de DR principales. Este documento se centra en la instalación, configuración y optimización mediante una estrategia de prueba piloto. Esta estrategia le ayuda a crear un entorno de DR de coste reducido, en el que inicialmente se aprovisiona un servidor de replicación para replicar los datos de la base de datos de origen. El servidor de base de datos propiamente dicho se aprovisiona solo cuando se inicia un proceso de recuperación de desastres. Esta estrategia elimina los gastos de mantenimiento de un servidor de base de datos en la región de DR. En su lugar, usted paga por una instancia EC2 más pequeña que actúa como servidor de replicación.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una EnterpriseOne aplicación de JD Edwards que se ejecuta en Oracle Database o Microsoft SQL Server con una base de datos compatible en estado de ejecución en una instancia EC2 gestionada. Esta aplicación debe incluir todos los componentes EnterpriseOne básicos de JD Edwards (Enterprise Server, HTML Server y Database Server) instalados en una región de AWS.
- Un rol de AWS Identity and Access Management (IAM) para configurar el servicio Elastic Disaster Recovery.
- Una red para ejecutar Elastic Disaster Recovery, configurada de acuerdo con los ajustes de conectividad requeridos.

Limitaciones

- Puede usar este patrón para replicar todos los niveles, a menos que la base de datos esté alojada en Amazon Relational Database Service (Amazon RDS). En este caso, le recomendamos que use la funcionalidad de copia entre regiones de Amazon RDS.
- Elastic Disaster Recovery no es compatible con CloudEndure Disaster Recovery, pero puede actualizarse desde CloudEndure Disaster Recovery. Para obtener más información, consulte las preguntas frecuentes en la documentación de Elastic Disaster Recovery.
- Amazon Elastic Block Store (Amazon EBS) limita la velocidad a la que puede tomar instantáneas. Puede replicar un número máximo de 300 servidores en una única cuenta de AWS mediante Elastic Disaster Recovery. Para replicar más servidores, puede usar varias cuentas de AWS o varias regiones de AWS de destino. (Deberá configurar Elastic Disaster Recovery por separado

en cada cuenta y región). Para más información, consulte las Prácticas recomendadas en la documentación de Elastic Disaster Recovery.

- Las cargas de trabajo de origen (la EnterpriseOne aplicación y la base de datos de JD Edwards) deben alojarse en instancias EC2. Este patrón no admite cargas de trabajo en las instalaciones o en otros entornos de nube.
- Este patrón se centra en los componentes de JD Edwards EnterpriseOne . Un plan completo de DR y continuidad empresarial (BCP) debe incluir otros servicios básicos, como:
  - Redes (nube privada virtual, subredes y grupos de seguridad)
  - Active Directory
  - Amazon WorkSpaces
  - Elastic Load Balancing
  - Un servicio de base de datos administrado como Amazon Relational Database Service (Amazon RDS).

Para obtener información adicional sobre los requisitos previos, configuraciones y limitaciones, consulte la documentación de Elastic Disaster Recovery.

Versiones de producto

- Oracle JD Edwards EnterpriseOne (versiones compatibles con Oracle y SQL Server basadas en los requisitos técnicos mínimos de Oracle)

Arquitectura

Pila de tecnología de destino

- Una sola región y una sola nube privada virtual (VPC) para producción y no producción, y una segunda región para DR
- Zonas de disponibilidad únicas para asegurar una baja latencia entre los servidores
- Un equilibrador de carga de aplicación que distribuya el tráfico de red para mejorar la escalabilidad y la disponibilidad de las aplicaciones en varias zonas de disponibilidad
- Amazon Route 53, para proporcionar configuración de sistema de nombres de dominio (DNS)
- Amazon proporcionará WorkSpaces a los usuarios una experiencia de escritorio en la nube
- Amazon Simple Storage Service (Amazon S3) para almacenar copias de seguridad, archivos y objetos

- Amazon CloudWatch para el registro, la supervisión y las alarmas de aplicaciones
- Amazon Elastic Disaster Recovery, para la recuperación de desastres

Arquitectura de destino

El siguiente diagrama muestra la arquitectura de recuperación ante desastres interregional de JD Edwards EnterpriseOne mediante Elastic Disaster Recovery.

Procedimiento

A continuación puede ver un resumen de alto nivel del proceso. Para más información, consulte la sección Epics.

- La replicación de Elastic Disaster Recovery comienza con una sincronización inicial. Durante esta sincronización inicial, el agente de replicación de AWS replica todos los datos de los discos de origen en el recurso correspondiente de la subred del área transitoria.
- La replicación continua sigue realizándose indefinidamente una vez finalizada la sincronización inicial.
- Debe revisar los parámetros de lanzamiento, que incluyen las configuraciones específicas del servicio y una plantilla de lanzamiento de Amazon EC2, una vez que se haya instalado el agente y se haya iniciado la replicación. Cuando se indique que el servidor de origen está listo para la recuperación, podrá iniciar las instancias.
- Cuando Elastic Disaster Recovery emite una serie de llamadas a la API para iniciar la operación de lanzamiento, la instancia de recuperación se lanza inmediatamente en AWS según la configuración de lanzamiento. El servicio activa automáticamente un servidor de conversión durante el inicio.
- La nueva instancia se activa en AWS una vez finalizada la conversión y está lista para usarse. El estado del servidor de origen en el momento del lanzamiento se representa mediante los volúmenes asociados a la instancia lanzada. El proceso de conversión implica cambios en los controladores, la red y la licencia del sistema operativo para asegurar que la instancia se inicie de forma nativa en AWS.
- Tras el lanzamiento, los volúmenes recién creados ya no se mantienen sincronizados con los servidores de origen. El agente de replicación de AWS sigue replicando de forma rutinaria los cambios realizados en los servidores de origen de los volúmenes del área transitoria, pero las instancias lanzadas no reflejan dichos cambios.

- Al iniciar una nueva instancia de simulacro o recuperación, los datos siempre se reflejan en el estado más reciente que se ha replicado desde el servidor de origen a la subred del área transitoria.
- Cuando el servidor de origen esté marcado como preparado para la recuperación, podrá iniciar las instancias.

Nota: el proceso funciona en ambos sentidos: para la conmutación por error de una región de AWS principal a una región de DR, y también para la conmutación por recuperación al sitio principal una vez que se ha recuperado. Puede preparar la conmutación por recuperación invirtiendo la dirección de replicación de los datos desde el equipo de destino al equipo de origen de forma totalmente orquestada.

Entre las ventajas del proceso descrito en este patrón se incluyen las siguientes:

- Flexibilidad: los servidores de replicación escalan horizontal y verticalmente en función del conjunto de datos y del tiempo de replicación, por lo que puede realizar pruebas de DR sin interrumpir las cargas de trabajo de origen ni la replicación.
- Fiabilidad: la replicación es sólida, no disruptiva y continua.
- Automatización: esta solución proporciona un proceso unificado y automatizado para las pruebas, la recuperación y la conmutación por recuperación.
- Optimización de costos: puede replicar y pagar solo por los volúmenes necesarios, y pagar por los recursos de cómputo en el sitio de DR solo cuando esos recursos estén activados. Puede usar una instancia de replicación con costos optimizados (le recomendamos que emplee un tipo de instancia optimizada para la computación) para varias fuentes o una sola fuente con un gran volumen de EBS.

Automatizar y escalar

Al realizar una recuperación ante desastres a escala, los EnterpriseOne servidores de JD Edwards dependerán de otros servidores del entorno. Por ejemplo:

- Los servidores de EnterpriseOne aplicaciones de JD Edwards que se conectan a una base de datos EnterpriseOne compatible con JD Edwards durante el arranque dependen de esa base de datos.

- EnterpriseOne Los servidores de JD Edwards que requieren autenticación y necesitan conectarse a un controlador de dominio durante el arranque para iniciar los servicios dependen del controlador de dominio.

Por este motivo, le recomendamos que automatice las tareas de conmutación por error. Por ejemplo, puede usar AWS Lambda o AWS Step Functions para automatizar los scripts de EnterpriseOne inicio de JD Edwards y los cambios en el balanceador de carga para automatizar el end-to-end proceso de conmutación por error. Para obtener más información, consulte la publicación del blog Crear un plan de recuperación de desastres escalable con AWS Elastic Disaster Recovery.

Herramientas

Servicios de AWS

- Amazon Elastic Block Store (Amazon EBS) brinda volúmenes de almacenamiento por bloques para su uso con instancias de EC2.
- Amazon Elastic Compute Cloud (Amazon EC2) brinda capacidad de computación escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- AWS Elastic Disaster Recovery minimiza el tiempo de inactividad y la pérdida de datos con una recuperación rápida y fiable de aplicaciones locales y basadas en la nube mediante un almacenamiento asequible, un cálculo y point-in-time una recuperación mínimos.
- Amazon Virtual Private Cloud (Amazon VPC) le ofrece un control total sobre su entorno de redes virtuales, incluida la ubicación de los recursos, la conectividad y la seguridad.

Prácticas recomendadas

Prácticas recomendadas generales

- Elabore con antelación un plan de acción en caso de que se produzca un evento de recuperación real.
- Después de configurar Elastic Disaster Recovery correctamente, cree una CloudFormation plantilla de AWS que pueda crear la configuración bajo demanda, en caso de que sea necesario. Determine el orden en el que deben lanzarse los servidores y las aplicaciones, y regístrelo en el plan de recuperación.
- Realice un simulacro regular (se aplican las tarifas estándar de Amazon EC2).

- Supervise el estado de la replicación en curso mediante la consola de Elastic Disaster Recovery o mediante programación.
- Proteja las point-in-time instantáneas y confirme antes de finalizar las instancias.
- Cree un rol de IAM para la instalación del agente de replicación de AWS.
- Habilite la protección de finalización de las instancias de recuperación en un escenario real de DR.
- No use la acción Desconectar de AWS en la consola de Elastic Disaster Recovery en los servidores para los que lanzó instancias de recuperación, incluso en el caso de un evento de recuperación real. Al realizar una desconexión, se cancelan todos los recursos de replicación relacionados con estos servidores de origen, incluidos los puntos de recuperación point-in-time (PIT).
- Modifique la política de PIT para cambiar el número de días de retención de las instantáneas.
- Edite la plantilla de lanzamiento, en la configuración de lanzamiento de Elastic Disaster Recovery, para configurar la subred, el grupo de seguridad y el tipo de instancia correctos para su servidor de destino.
- Automatice el proceso de end-to-end conmutación por error mediante Lambda o Step Functions para automatizar los scripts de inicio de JD EnterpriseOne Edwards y los cambios en el balanceador de carga.

Optimización y consideraciones de JD Edwards EnterpriseOne

- Vaya PrintQueuea la base de datos.
- Vaya MediaObjectsa la base de datos.
- Excluya los registros y la carpeta temporal de los servidores lógicos y por lotes.
- Excluya la carpeta temporal de Oracle WebLogic.
- Cree scripts para el inicio después de la conmutación por error.
- Excluya la tempdb de SQL Server.
- Excluya el archivo temporal de Oracle.

Epics

Realice las tareas y configuración iniciales

Tarea	Descripción	Habilidades requeridas
Configure la red de replicación.	Implemente su EnterpriseOne sistema JD Edwards en la región principal de AWS e identifique la región de AWS para DR. Siga los pasos de la sección de requisitos de red de replicación de la documentación de Elastic Disaster Recovery para planificar y configurar su red de replicación y DR.	Administrador de AWS
Determine el RPO y el RTO.	Identifique el objetivo de tiempo de recuperación (RTO) y el objetivo de punto de recuperación (RPO) para los servidores de aplicaciones y la base de datos.	Arquitecto de la nube, arquitecto de DR
Habilite la replicación para Amazon EFS.	Si procede, habilite la replicación desde la región principal de AWS a la región DR para sistemas de archivos compartidos como Amazon Elastic File System (Amazon EFS) mediante AWS DataSync, rsync u otra herramienta adecuada.	Administrador de la nube
Administre el DNS de DR.	Identifique el proceso para actualizar el sistema de nombres de dominio (DNS)	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	durante el simulacro de DR o la recuperación real	
Crear un rol de IAM para la configuración.	Siga las instrucciones de la sección Inicialización y permisos de Elastic Disaster Recovery, de la documentación de Elastic Disaster Recovery, para crear un rol de IAM para inicializar y administrar el servicio de AWS.	Administrador de la nube
Configurar las interconexiones de VPC.	Asegúrese de que las VPC de origen y destino estén sincronizadas y sean accesibles entre sí. Para obtener instrucciones sobre la configuración, consulte la documentación de Amazon VPC.	Administrador de AWS

Configure los parámetros de replicación de Elastic Disaster Recovery

Tarea	Descripción	Habilidades requeridas
Inicialice Elastic Disaster Recovery.	Abra la consola de Elastic Disaster Recovery, seleccione la región de AWS de destino (donde replicará los datos y lanzará las instancias de recuperación) y, a continuación, elija Establecer la configuración de replicación predeterminada.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Configure los servidores de replicación	1. En el panel Configurar servidores de replicación, introduzca la subred del área transitoria y el tipo de instancia del servidor de replicación. La opción predeterminada es el tipo de instancia `t3.small`. Ajuste esta configuración en función de sus requisitos y recuerde tener en cuenta los precios de las instancias. Para obtener más información, consulte Precios de Amazon EC2. 2. En la sección Acceso al servicio, seleccione Ver detalles para revisar el rol vinculado al servicio y las políticas adicionales creadas durante la inicialización del servicio. 3. Elija Siguiente.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Configure los volúmenes y los grupos de seguridad.	1. En el panel Volúmenes y grupos de seguridad , seleccione el tipo de volumen de EBS para el servidor de replicación y establezca el cifrado de Amazon EBS como Predeterminado. 2. Seleccione Usar siempre grupo de seguridad de AWS Elastic Disaster Recovery para que Elastic Disaster Recovery pueda adjuntar y supervisar automáticamente el grupo de seguridad predeterm inado. 3. Elija Siguiente.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Configure los ajustes adicionales.	1. En el panel Configuración adicional, configure el enrutamiento y la limitación de datos, la política de PIT y las etiquetas. • El enrutamiento y la limitación de datos controlan la forma en que los datos fluyen desde el servidor externo a los servidores de replicación. Seleccione Usar IP privada para la replicación de datos. De lo contrario, a los servidores de replicación se les asignará automáticamente una IP pública y los datos fluirán a través de la internet pública. • En la sección Políticas de tiempo (PIT), configure una política de retención que determine el tiempo después del cual no es necesario conservar las instantáneas. El periodo de retención predeterminado es de siete días. • En la sección Etiquetas, añada etiquetas personalizadas a los recursos creados por Elastic	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	Disaster Recovery en su cuenta de AWS. 2. Seleccione Siguiente, revise la configuración en el panel y, a continuación, elija Crear predeterminado para crear la plantilla predeterminada.	

Instale el agente de replicación de AWS

Tarea	Descripción	Habilidades requeridas
Crear un rol de IAM.	Cree un rol de IAM que contenga la política `AWSElasticDisasterRecoveryAgentInstallationPolicy` . En la sección Seleccionar tipo de acceso de AWS, habilite el acceso programático. Apunte el ID de clave de acceso y la clave de acceso secreta. Necesitará esta información durante la instalación del agente de replicación de AWS.	Administrador de AWS
Compruebe los requisitos.	Compruebe y complete los requisitos previos de la documentación de Elastic Disaster Recovery para instalar el agente de replicación de AWS.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Instale el agente de replicación de AWS.	Siga las instrucciones de instalación de su sistema operativo e instale el agente de replicación de AWS. • Para Microsoft Windows: descargue los archivos de configuración y ejecute el archivo .exe como administrador. Siga las indicaciones para completar la instalación. • Para Linux: copie los siguientes comandos (en el orden en que aparecen) y péguelos en su sesión de Secure Shell (SSH). El primer comando descarga el instalador y el segundo lo ejecuta. `wget -O ./aws-replication-installer-init.py https://aws-elastic-disaster-recovery-us-west-2.s3.amazonaws.com/latest/linux/aws-replication-installer-init.py` Nota: cambie la URL para que refleje su región.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	`sudo python3 aws-replication-installer-init.py` Siga las indicaciones para completar la instalación. Repita estos pasos en el servidor restante.	
Supervisar la replicación	Regrese al panel Servidores de origen de Elastic Disaster Recovery para supervisar el estado de la replicación. La sincronización inicial tardará algún tiempo en función del tamaño de la transferencia de datos. Cuando el servidor de origen esté completamente sincronizado, el estado del servidor se actualizará a Listo. Esto significa que se ha creado un servidor de replicación en el área transitoria, y que los volúmenes de EBS se han replicado desde el servidor de origen al área de almacenamiento transitorio.	Administrador de AWS

Configure los ajustes de lanzamiento

Tarea	Descripción	Habilidades requeridas
Edite la configuración de lanzamiento.	Para actualizar la configuración de lanzamiento de las instancias de simulacro y recuperación, en la consola de Elastic Disaster Recovery, seleccione el servidor de origen y, a continuación, seleccione Acciones y Editar configuración de lanzamiento. También puede elegir las máquinas de origen que se van a replicar en la página Servidores de origen y, a continuación, elegir la pestaña Configuración de lanzamiento. Esta pestaña tiene dos secciones: Configuración general de lanzamiento y plantilla de lanzamiento de EC2.	Administrador de AWS
Configure los ajustes generales de lanzamiento.	Revise la configuración general de lanzamiento según sus necesidades. • Tamaño correcto del tipo de instancia: si elige Básico, Elastic Disaster Recovery omite el tipo de instancia que seleccionó en la plantilla de lanzamiento de Amazon EC2 y elige automáticamente el tipo	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	de instancia en función del sistema operativo, la CPU y la RAM del servidor de origen. • Copiar IP privada: seleccione si desea que Elastic Disaster Recovery se asegure de que la IP privada usada por la instancia de simulacro o recuperación coincide con la IP privada usada por el servidor de origen. Si elige Sí, asegúrese de que el rango de IP de la subred que configuró en la plantilla de lanzamiento de Amazon EC2 incluya la dirección IP privada. Para obtener más información, consulte la Configuración general de lanzamiento en la documentación de Elastic Disaster Recovery.	

Tarea	Descripción	Habilidades requeridas
Configure la plantilla de lanzamiento de Amazon EC2.	Elastic Disaster Recovery emplea plantillas de lanzamiento de Amazon EC2 para lanzar instancias de simulacro y recuperación para cada servidor de origen. La plantilla de lanzamiento se crea automáticamente para cada servidor de origen que añada a Elastic Disaster Recovery tras instalar AWS Replication Agent. Debe configurar la plantilla de lanzamiento de Amazon EC2 como plantilla de lanzamiento predeterminada si desea usarla con Elastic Disaster Recovery. Para obtener más información, consulte la Plantilla de lanzamiento de EC2 en la documentación de Elastic Disaster Recovery.	Administrador de AWS

Inicie el simulacro y la conmutación por error de DR

Tarea	Descripción	Habilidades requeridas
Inicie el simulacro	1. En la consola de Elastic Disaster Recovery, abra la página Servidores de origen y compruebe que el estado	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	del servidor de origen es Listo. 2. Seleccione todos los servidores de origen en los que desee realizar el simulacro de recuperación de desastres. 3. En el menú Iniciar trabajo de recuperación, elija Iniciar el simulacro y seleccione la point-in-time instantán ea adecuada. Se iniciará un trabajo de recuperac ión en los servidores de origen seleccionados. Puede supervisar el estado del trabajo en la pestaña Historial de trabajos de recuperación. Nota: los cambios que se realicen en el servidor de origen se sincronizarán con el servidor de replicaci ón, no con la instancia de simulacro. La instancia de simulacro lanzada aparecerá también en la página Instancias de recuperación. 4. Pruebe y verifique la instancia de simulacro de DR.	

Tarea	Descripción	Habilidades requeridas
	5. En la página Instancias de recuperación, seleccione la instancia de simulacro y, a continuación, elija Acciones, Desconectar de AWS. Se eliminará AWS Replication Agent de la instancia de recuperación y se eliminarán todos los recursos asociados a la instancia de recuperación de Elastic Disaster Recovery. 6. Seleccione Eliminar instancias de recuperación. Se eliminará la representación de la instancia de la consola de Elastic Disaster Recovery y se desvinculará completamente la instancia del servicio de Elastic Disaster Recovery. No se eliminará la instancia de EC2 subyacente. 7. Finalice la instancia de simulacro de DR desde la consola de Amazon EC2. Para obtener más información, consulte las Preparación para la conmutación por error en la documentación de Elastic Disaster Recovery.	

Tarea	Descripción	Habilidades requeridas
Valide el simulacro.	En el paso anterior, lanzó nuevas instancias de destino en la región de DR. Las instancias de destino son réplicas de los servidore s de origen basadas en la instantánea realizada al iniciar el lanzamiento. En este procedimiento, se conectará a las máquinas de destino de Amazon EC2 para confirmar que funcionan según lo previsto. 1. Abra la consola de Amazon EC2. 2. Seleccione Instancias (en ejecución). 3. Seleccione la instancia de destino y anote su dirección IPv4 privada. 4. Asegúrese de que puede conectarse a la instancia EC2 y de que el JD Edwards EnterpriseOne y los componentes relaciona dos se replican según lo previsto.	

Tarea	Descripción	Habilidades requeridas
Iniciar la conmutación por error.	La conmutación por error es la redirección del tráfico de un sistema principal a un sistema secundario. Elastic Disaster Recovery le ayuda a realizar una conmutación por error al lanzar instancias de recuperación en AWS. Cuando se lanzan las instancias de recuperación, el tráfico de sus sistemas principales se redirige a estas instancias. 1. En la consola de Elastic Disaster Recovery, abra la página Servidores de origen y compruebe que en la columna Listo para recuperación del servidor de origen aparezca Listo, y que en la columna Estado de replicación de datos aparezca Correcto. 2. Seleccione el servidor de origen. En el menú Iniciar trabajo de recuperación, seleccione Iniciar recuperación. 3. Seleccione la point-in-time instantánea desde la que desea lanzar la instancia de recuperación y, a continuación, elija Iniciar la recuperación.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	Se iniciará un trabajo de recuperación. Puede supervisar el estado del trabajo en la página Instancias de recuperación. 4. Pruebe y verifique la instancia de recuperación. Si es necesario, ajuste la configuración del DNS y conecte la EnterpriseOne aplicación JD Edwards a la base de datos. 5. Ahora puede desconectar y retirar el EnterpriseOne servidor JD Edwards de origen, ya que todos los cambios se han escrito en la nueva instancia de recuperación. 6. Registre la instancia de recuperación como servidor de origen en la región de DR siguiendo el proceso descrito en la épica Instale el agente de replicación de AWS. Para más información, consulte las Efectuar una conmutación por error en la documentación de Elastic Disaster Recovery.	

Tarea	Descripción	Habilidades requeridas
Inicie la conmutación por recuperación.	El proceso para iniciar una conmutación por recuperación es similar al proceso para iniciar una conmutación por error. 1. Abre la consola de Elastic Disaster Recovery en la región principal. Vaya a la página Instancias de recuperación, seleccione la instancia de perforación y, a continuación, elija Acciones, Desconectar de AWS, Eliminar instancias de recuperación. 2. Abre la consola de Elastic Disaster Recovery en la región de DR. Registre su nuevo EnterpriseOne servidor de JD Edwards como servidor de origen en la región de RD mediante la instalación del AWS Replication Agent. Los datos se sincronizarán con un nuevo servidor de replicación aprovisionado en la nueva subred transitoria. Nota: Cuando el nuevo EnterpriseOne servidor de JD Edwards se registre como servidor de origen,	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	es posible que vea dos servidores de origen en la consola de Elastic Disaster Recovery: un servidor que se creó a partir de la instancia de EC2 principal y el nuevo servidor que se creó a partir de la instancia de recuperación. Se recomienda etiquetar los servidores correctamente para evitar confusiones y, preferiblemente, añadir el nuevo servidor a la plantilla de lanzamiento. 3. Para reiniciar la replicación de DR desde la región principal, desasocie la instancia de recuperación lanzada de la consola de Elastic Disaster Recovery en la región de DR y registre el host como servidor de origen en la región principal. Para más información, consulte las Efectuar una conmutación por recuperación en la documentación de Elastic Disaster Recovery.	

Tarea	Descripción	Habilidades requeridas
Inicie los EnterpriseOne componentes de JD Edwards.	1. Inicie la EnterpriseOne base de datos de JD Edwards iniciando sesión en el servidor de la base de datos. 2. Cuando la base de datos esté en ejecución, inicie los servidores EnterpriseOne lógicos y de lotes de JD Edwards. 3. Comience WebLogic en los servidores web e inicie una instancia JAS en los servidores JAS. 4. Comience WebLogic en el servidor de aprovisio namiento y en el servidor de la consola SM. 5. Inicie SM Agent en los servidores. 6. Confirme que el inicio de sesión en JD Edwards EnterpriseOne funciona correctamente. Deberá incorporar los cambios en Route 53 y Application Load Balancer para que funcione el EnterpriseOne enlace de JD Edwards. Puede automatizar estos pasos mediante Lambda, Step	JD Edwards CNC Enterpris eOne

Tarea	Descripción	Habilidades requeridas
	Functions y Systems Manager (Run Command). Nota: Elastic Disaster Recovery realiza la replicación a nivel de bloque de los volúmenes EBS de la instancia de EC2 de origen que alojan el sistema operativo y los sistemas de archivos. Los sistemas de archivos compartidos creados con Amazon EFS no forman parte de esta replicación. Puede replicar los sistemas de archivos compartidos en la región de DR mediante AWS DataSync, como se indica en la primera epopeya, y luego montar estos sistemas de archivos replicados en el sistema de DR.	

Solución de problemas

Problema	Solución
El estado de la replicación de los datos del servidor de origen es Estancado y la replicación se retrasa. Si comprueba los detalles, el estado de la replicación de datos muestra Agente no encontrado.	Compruebe que el servidor de origen estancado está en funcionamiento. Nota: si el servidor de origen deja de funcionar, el servidor de replicación finaliza automáticamente.

Problema	Solución
	Para obtener más información sobre problemas de retardo, consulte Problemas de retardo en la replicación en la documentación de Elastic Disaster Recovery.
La instalación de AWS Replication Agent en la instancia de EC2 de origen falla en RHEL 8.2 después de escanear los discos. `aws_replication_agent_installer.log` indica que faltan los encabezados del kernel.	Antes de instalar AWS Replication Agent en RHEL 8, CentOS 8 u Oracle Linux 8, ejecute: `sudo yum install elfutils-libelf-devel` Para más información, consulte las Requisitos de instalación de Linux en la documentación de Elastic Disaster Recovery.
En la consola de Elastic Disaster Recovery, verá el servidor de origen como Listo con retardo, y el estado de replicación de datos como Estancado. En función del tiempo que AWS Replication Agent no esté disponible, el estado puede indicar un retardo elevado, pero el problema seguirá siendo el mismo.	Use un comando del sistema operativo para confirmar que AWS Replication Agent se está ejecutando en la instancia de EC2 de origen o confirme que la instancia se está ejecutando. Tras corregir los problemas, Elastic Disaster Recovery reiniciará el escaneo. Espere a que se hayan sincronizado todos los datos y el estado de la replicación sea Correcto antes de iniciar un simulacro de DR.

Problema	Solución
Replicación inicial con retardo elevado. En la consola de Elastic Disaster Recovery, puede ver que el estado de sincronización inicial es extremadamente lento para un servidor de origen.	Compruebe los problemas de retardo en la replicación documentados en la sección Problemas de retardo en la replicación de la documentación de Elastic Disaster Recovery. Es posible que el servidor de replicación no pueda gestionar la carga debido a las operaciones informáticas intrínsecas. En ese caso, intente actualizar el tipo de instancia tras consultar con el equipo de soporte técnico de AWS.

Recursos relacionados

- Guía del usuario de AWS Elastic Disaster Recovery
- Crear un plan de recuperación de desastres escalable con AWS Elastic Disaster Recovery (publicación del blog de AWS)
- AWS Elastic Disaster Recovery: introducción técnica (curso de AWS Skill Builder; requiere iniciar sesión)
- Guía de inicio rápido de AWS Elastic Disaster Recovery

Sincronice los datos entre los sistemas de archivos de Amazon EFS en distintas regiones de AWS mediante AWS DataSync

Creado por Sarat Chandra Pothula (AWS) y Aditya Ambati (AWS)

Repositorio de código: aws-efs-crossregion-datasync	Entorno: PoC o piloto	Tecnologías: infraestructura; almacenamiento y respaldo
Servicios de AWS: AWS CDK; AWS DataSync; Amazon EFS		

Resumen

Esta solución proporciona un marco sólido para una sincronización de datos eficiente y segura entre instancias de Amazon Elastic File System (Amazon EFS) en diferentes regiones de AWS. Este enfoque es escalable y proporciona una replicación de datos controlada entre regiones. Esta solución puede mejorar sus estrategias de recuperación ante desastres y redundancia de datos.

Al utilizar el AWS Cloud Development Kit (AWS CDK), este patrón utiliza un enfoque de infraestructura como código (IaC) para implementar los recursos de la solución. La aplicación AWS CDK implementa los recursos esenciales de AWS, DataSync Amazon EFS, Amazon Virtual Private Cloud (Amazon VPC) y Amazon Elastic Compute Cloud (Amazon EC2). Este IaC proporciona un proceso de implementación repetible y controlado por versiones que está totalmente alineado con las prácticas recomendadas de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- AWS Command Line Interface (AWS CLI) versión 2.9.11 o posterior, instalada y configurada
- AWS CDK versión 2.114.1 o posterior, instalada y arrancada
- Nodejs versión 20.8.0 o posterior, instalada

Limitaciones

- La solución hereda las limitaciones de DataSync Amazon EFS, como las tasas de transferencia de datos, las limitaciones de tamaño y la disponibilidad regional. Para obtener más información, consulte Cuotas de AWS y DataSync Cuotas de Amazon EFS.
- Esta solución solo es compatible con Amazon EFS. DataSync es compatible con otros servicios de AWS, como Amazon Simple Storage Service (Amazon S3) y Amazon FSx for Lustre. Sin embargo, esta solución requiere modificaciones para sincronizar los datos con estos otros servicios.

Arquitectura

Esta solución implementa las siguientes pilas de CDK de AWS:

- Pila de Amazon VPC: esta pila configura los recursos de la nube privada virtual (VPC), incluidas subredes, una puerta de enlace a Internet y una puerta de enlace NAT en las regiones de AWS principal y secundaria.
- Pila de Amazon EFS: esta pila implementa los sistemas de archivos de Amazon EFS en las regiones principal y secundaria y los conecta a sus VPC respectivas.
- Pila Amazon EC2: esta pila lanza instancias EC2 en las regiones principal y secundaria. Estas instancias están configuradas para montar el sistema de archivos Amazon EFS, lo que les permite acceder al almacenamiento compartido.
- DataSync pila de ubicaciones: esta pila utiliza una construcción personalizada denominada `DataSyncLocationConstruct` para crear recursos de DataSync ubicación en las regiones principal y secundaria. Estos recursos definen los puntos finales para la sincronización de datos.
- DataSync pila de tareas: esta pila utiliza una construcción personalizada llamada `DataSyncTaskConstruct` para crear una DataSync tarea en la región principal. Esta tarea está configurada para sincronizar los datos entre las regiones principal y secundaria mediante las ubicaciones de DataSync origen y destino.

Herramientas

Servicios de AWS

- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura de la nube de AWS en código.

- AWS DataSync es un servicio de transferencia y descubrimiento de datos en línea que le ayuda a mover archivos o datos de objetos hacia, desde y entre los servicios de almacenamiento de AWS.
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon Elastic File System (Amazon EFS) le ayuda a crear y configurar sistemas de archivos compartidos en la nube de AWS.
- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esta red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Repositorio de código

El código de este patrón está disponible en el repositorio de DataSync proyectos multiregionales de GitHub Amazon EFS.

Prácticas recomendadas

Siga las prácticas recomendadas descritas en Prácticas recomendadas para usar la CDK de AWS TypeScript para crear proyectos de IaC.

Epics

Implemente la aplicación AWS CDK

Tarea	Descripción	Habilidades requeridas
Clone el repositorio del proyecto.	Introduzca el siguiente comando para clonar el repositorio del DataSync proyecto multiregional de Amazon EFS. `git clone https://github.com/aws-samples/aws-efs-crossregion-datasync.git`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Instale las dependencias de npm.	Escriba el siguiente comando. `npm ci`	AWS DevOps
Elija las regiones principal y secundaria.	En el repositorio clonado, navegue hasta el `src/infra` directorio. En el `Launcher.ts` archivo, actualice los `SECONDARY_AWS_REGION` valores `PRIMARY_AWS_REGION` y. Utilice los códigos de región correspondientes. `const primaryRegion = { account: account, region: '<PRIMARY_AWS_REGION>' }; const secondaryRegion = { account: account, region: '<SECONDARY_AWS_REGION>' };`	AWS DevOps
Inicie el entorno.	Introduzca el siguiente comando para iniciar la cuenta de AWS y la región de AWS que desee utilizar. `cdk bootstrap <aws_account>/<aws_region>` Para obtener más información, consulte Proceso de arranque en la documentación de AWS CDK.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Enumere las pilas de CDK de AWS.	Introduzca el siguiente comando para ver una lista de las pilas de CDK de AWS de la aplicación. `cdk ls`	AWS DevOps
Sintetice las pilas de CDK de AWS.	Introduzca el siguiente comando para generar una CloudFormation plantilla de AWS para cada pila definida en la aplicación AWS CDK. `cdk synth`	AWS DevOps
Implemente la aplicación AWS CDK.	Introduzca el siguiente comando para implementar todas las pilas en su cuenta de AWS, sin necesidad de aprobación manual para realizar ningún cambio. `cdk deploy --all --require-approval never`	AWS DevOps

Valide la implementación

Tarea	Descripción	Habilidades requeridas
Inicie sesión en la instancia EC2 de la región principal.	1. Con Session Manager, una función de AWS Systems Manager, inicie sesión en la instancia EC2 de la región principal. Para obtener	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	instrucciones, consulte Conectarse a su instancia de Linux con el administrador de sesiones de AWS Systems Manager. 2. Cambie los directorios a la ruta de montaje de Amazon EFS. `cd /mnt/efs`	
Cree un archivo temporal.	Introduzca el siguiente comando para crear un archivo temporal en la ruta de montaje de Amazon EFS. `sudo dd if=/dev/zero \` `of=tmptst.dat \` `bs=1G \` `seek=5 \` `count=0` `ls -lrt tmptst.dat`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Inicie la DataSync tarea.	Introduzca el siguiente comando para replicar el archivo temporal de la región principal a la región secundaria, donde `<ARN-task>` se encuentra el nombre del recurso de Amazon (ARN) de la tarea. DataSync `aws datasync start-task-execution \` `--task-arn <ARN-task>` El comando devuelve el ARN de la ejecución de la tarea en el siguiente formato. `arn:aws:datasync:<region>:<account-ID>:task/task-execution/<exec-ID>`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Compruebe el estado de la transferencia de datos.	Introduzca el siguiente comando para describir la tarea de DataSync ejecución , donde `<ARN-task-execution>` está el ARN de la ejecución de la tarea. `aws datasync describe-task-execution \ --task-execution-arn <ARN-task-execution>` La DataSync tarea está completa cuando `PrepareStatus` `TransferStatus` , y `VerifyStatus` todas tienen el valor`SUCCESS`.	AWS DevOps
Inicie sesión en la instancia EC2 de la región secundaria.	1. Con Session Manager, una función de AWS Systems Manager, inicie sesión en la instancia EC2 de la región secundaria. Para obtener instrucciones, consulte Conectarse a su instancia de Linux con el administrador de sesiones de AWS Systems Manager. 2. Cambie los directorios a la ruta de montaje de Amazon EFS. `cd /mnt/efs`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Valide la replicación.	Introduzca el siguiente comando para comprobar que el archivo temporal existe en el sistema de archivos Amazon EFS. `ls -lrt tmptst.dat`	AWS DevOps

Recursos relacionados

Documentación de AWS

- Referencia de la API CDK de AWS
- Configuración de las DataSync transferencias de AWS con Amazon EFS
- Solución de problemas con las DataSync transferencias de AWS

Otros recursos de AWS

- DataSync Preguntas frecuentes sobre AWS

Actualizar los clústeres de SAP Pacemaker de ENSA1 a ENSA2

Creado por Gergely Cerdi (AWS) y Balazs Sandor Skublics (AWS)

Entorno: producción	Origen: clúster Pacemaker basado en ENSA1	Destino: clúster de marcapasos basado en la ENSA2
Tipo R: renovar arquitectura	Carga de trabajo: SAP	Tecnologías: infraestructura; modernización
Servicios de AWS: Amazon EC2		

Resumen

Este patrón explica los pasos y las consideraciones para actualizar un clúster de SAP Pacemaker basado en el servidor Enqueue independiente (ENSA1) a ENSA2. La información de este patrón se aplica a los sistemas operativos SUSE Linux Enterprise Server (SLES) y Red Hat Enterprise Linux (RHEL).

Los clústeres Pacemaker de SAP NetWeaver 7.52 o S/4HANA 1709 y versiones anteriores se ejecutan en una arquitectura ENSA1 y están configurados específicamente para ENSA1. Si ejecuta sus cargas de trabajo de SAP en Amazon Web Services (AWS) y está interesado en pasarse a ENSA2, es posible que la documentación de SAP, SUSE y RHEL no proporcione información completa. Este patrón describe los pasos técnicos necesarios para reconfigurar los parámetros de SAP y los clústeres Pacemaker para actualizar de ENSA1 a ENSA2. Proporciona ejemplos de sistemas SUSE, pero el concepto es el mismo para los clústeres RHEL.

> Notas: ENSA1 y ENSA2 son conceptos que se refieren únicamente a las aplicaciones de SAP, por lo que la información de este patrón no se aplica a SAP HANA ni a otros tipos de clústeres.
>
> Técnicamente, ENSA2 se puede utilizar con o sin Enqueue Replicator 2. Sin embargo, la alta disponibilidad (HA) y la automatización de la conmutación por error (mediante una solución de clúster) requieren Enqueue Replicator 2. Este patrón utiliza el término clústeres ENSA2 para referirse a los clústeres con Enqueue Server 2 y Enqueue Replicator 2 independientes.

Requisitos previos y limitaciones

Requisitos previos

- Clúster funcional basado en ENSA1 que utiliza Pacemaker y Corosync en SLES o RHEL.
- Al menos dos instancias de Amazon Elastic Compute Cloud (Amazon EC2) en las que se estén ejecutando las instancias (ABAP) de SAP Central Services (ASCS/SCS) y Enqueue Replication Server (ERS).
- Conocimientos sobre la gestión de clústeres y aplicaciones de SAP.
- Acceso al entorno Linux como usuario raíz.

Limitaciones

- Los clústeres basados en ENSA1 solo admiten una arquitectura de dos nodos.
- Los clústeres basados en ENSA2 no se pueden implementar en versiones de SAP anteriores a la 7.52. NetWeaver
- Las instancias EC2 de los clústeres deben estar en distintas zonas de disponibilidad de AWS.

Versiones de producto

- SAP versión 7.52 NetWeaver o posterior
- A partir de S/4HANA 2020, solo se admiten los clústeres ENSA2
- Kernel 7.53 o posterior, compatible con ENSA2 y Enqueue Replicator 2
- SLES para aplicaciones SAP, versión 12 o posterior
- RHEL para SAP con alta disponibilidad (HA) versión 7.9 o posterior

Arquitectura

Pila de tecnología de origen

- SAP NetWeaver 7.52 con SAP Kernel 7.53 o posterior
- Sistema operativo SLES o RHEL

Pila de tecnología de destino

- SAP NetWeaver 7.52 con SAP Kernel 7.53 o posterior, incluido S/4HANA 2020 con plataforma ABAP
- Sistema operativo SLES o RHEL

Arquitectura de destino

El siguiente diagrama muestra una configuración de alta disponibilidad de instancias ASCS/SCS y ERS basada en un clúster ENSA2.

Comparación de los clústeres ENSA1 y ENSA2

SAP presentó el ENSA2 como el sucesor del ENSA1. Un clúster basado en ENSA1 admite una arquitectura de dos nodos en la que la instancia de ASCS/SCS se conmuta por error al ERS cuando se produce un error. Esta limitación se debe a la forma en que la instancia de ASCS/SCS recupera la información de la tabla de bloqueo de la memoria compartida del nodo ERS tras la conmutación por error. Los clústeres basados en ENSA2 con Enqueue Replicator 2 eliminan esta limitación, ya que la instancia ASCS/SCS puede recopilar la información de bloqueo de la instancia ERS a través de la red. Los clústeres basados en ENSA2 pueden tener más de dos nodos, ya que la instancia ASCS/SCS ya no es necesaria para realizar la conmutación por error al nodo ERS. (Sin embargo, en un entorno de clúster ENSA2 de dos nodos, la instancia de ASCS/SCS seguirá realizando la conmutación por error al nodo ERS porque no hay otros nodos del clúster a los que realizar la conmutación por error). Se admite ENSA2 a partir del kernel 7.50 de SAP, con algunas limitaciones. Para una configuración de alta disponibilidad compatible con Enqueue Replicator 2, el requisito mínimo es de NetWeaver 7.52 (consulte la nota 2630416 de SAP OSS). El S/4HANA 1809 viene con la arquitectura ENSA2 recomendada de forma predeterminada, mientras que S/4HANA solo es compatible con ENSA2 a partir de la versión 2020.

Automatizar y escalar

El clúster de alta disponibilidad de la arquitectura de destino hace que el ASCS realice automáticamente la conmutación por error a otros nodos.

Escenarios para pasar a clústeres basados en ENSA2

Existen dos escenarios principales para la actualización a clústeres basados en ENSA2:

- Escenario 1: seleccione actualizar a ENSA2 sin una actualización de SAP o una conversión a S/4HANA, suponiendo que su versión de SAP y su versión de kernel sean compatibles con ENSA2.
- Escenario 2: pase a ENSA2 como parte de una actualización o conversión (por ejemplo, a S/4HANA 1809 o posterior) mediante SUM.

La sección Epics describe los pasos para estos dos escenarios. El primer escenario requiere que configure manualmente los parámetros relacionados con SAP antes de cambiar la configuración del clúster para ENSA2. En el segundo escenario, SUM implementa los binarios y los parámetros relacionados con SAP, y la única tarea restante es actualizar la configuración del clúster para HA. Aun así, le recomendamos que valide los parámetros de SAP después de usar SUM. En la mayoría de los casos, la conversión a S/4HANA es el motivo principal de la actualización de un clúster.

Herramientas

- Para los administradores de paquetes de sistemas operativos, recomendamos las herramientas Zypper (para SLES) o YUM (para RHEL).
- Para la administración de clústeres, recomendamos los servidores crm (para SLES) o pcs (para RHEL).
- Herramientas de administración de instancias de SAP, como SAPControl.
- (Opcional) Herramienta SUM para la actualización de conversión a S/4HANA.

Prácticas recomendadas

- Para conocer las prácticas recomendadas sobre el uso de cargas de trabajo de SAP en AWS, consulte SAP Lens para el Marco de AWS Well-Architected
- Tenga en cuenta la cantidad de nodos del clúster (pares o impares) en su arquitectura de varios nodos ENSA2.
- Configure el clúster ENSA2 para el SLES 15 de acuerdo con el estándar de certificación SAP S/4-HA-CLU 1.0.
- Guarde o haga copias de seguridad del estado del clúster y de la aplicación existentes antes de actualizar a ENSA2.

Epics

Configure los parámetros de SAP manualmente para ENSA2 (solo en el escenario 1)

Tarea	Descripción	Habilidades requeridas
Configure los parámetros en el perfil predeterminado.	Si desea actualizar a ENSA2 mientras utiliza la misma versión de SAP o si su versión de destino está predeterminada en ENSA1, defina los parámetros del perfil predeterminado (archivo DEFAULT.PFL) en los siguientes valores. `enq/enable=TRUE` `enq/serverhost=sapascsvirt` `enq/serverinst=10` `(instance number of ASCS/SCS instance)` `enque/process_location=REMOTESA` `enq/replicatorhost=sapersvirt` `enq/replicatorinst=11` `(instance number of ERS instance)` donde `sapascsvirt` es el nombre de host virtual de las instancias de ASCS y es `sapersvirt` el nombre de host virtual de las instancias de ERS. Puede cambiarlos para adaptarlos a su entorno de destino.	SAP

Tarea	Descripción	Habilidades requeridas
	Nota: para utilizar esta opción de actualización, la versión de SAP y la versión del núcleo deben ser compatibles con ENSA2 y Enqueue Replicator 2.	

Tarea	Descripción	Habilidades requeridas
Configure el perfil de instancia de ASCS/SCS.	Si desea actualizar a ENSA2 mientras utiliza la misma versión de SAP o si su versión de destino está predeterm inada en ENSA1, defina los siguientes parámetros en el perfil de instancia de ASCS/ SCS. La sección del perfil en la que se define ENSA1 tiene un aspecto parecido al siguiente. `#----------------- ----------------- ----------------- --------- Start SAP enqueue server #----------------- ----------------- ----------------- ------- _EN = en.sap$(S APSYSTEMNAME)$(INS TANCE_NAME) Execute_04 = local rm - f $(_EN) Execute_05 = local ln - s -f $(DIR_EXECUTABLE)/ enserver$(FT_EXE) $(_EN) Start_Program_01 = local $(_EN) pf=$(_PF)` Para reconfigurar esta sección para ENSA2:	SAP

Tarea	Descripción	Habilidades requeridas
	1. Cambie el prefijo del programa _EN para que _ENQ se base en la información más reciente de SAP (OSS Note 2501860; requiere una cuenta de usuario de SAP ONE Support Launchpad). 2. Cambie el binario para el servidor de puesta en cola de `enserver` a `enq_server` . 3. Defina el parámetro `enq/server/replication/enable` como `TRUE`. 4. Asegúrese de que `Autostart = 0`. Esta sección de perfil tendrá un aspecto similar al siguiente después de los cambios. `#------------------ ------------------ ------------------ --------- Start SAP enqueue server #------------------ ------------------ ------------------ ------- _ENQ = enq.sap$( SAPSYSTEMNAME)$(IN STANCE_NAME)`	

Tarea	Descripción	Habilidades requeridas
	`Execute_04 = local rm -f $(_ENQ)` `Execute_05 = local ln -s -f $(DIR_EXECUTABLE)/enq_server$(FT_EXE) $(_ENQ)` `Start_Program_01 = local $(_ENQ) pf=$(_PF)` `...` `enq/server/replication/enable = TRUE` `Autostart = 0` Importante: _ENQ no debe tener habilitada la opción de reinicio. Si `RestartProgram_01` está configurada para _ENQ, cámbiela a `StartProgram_01` . Esto evita que SAP reinicie el servicio o interfiera con los recursos gestionados por el clúster.	

Tarea	Descripción	Habilidades requeridas
Configurar el perfil ERS.	Si desea actualizar a ENSA2 mientras utiliza la misma versión de SAP o si su versión de destino está predeterm inada en ENSA1, defina los siguientes parámetros en el perfil de la instancia ERS. Busque la sección en la que está definido el replicador de puesta en cola. Será similar al siguiente. `#------------------ ------------------ ------------------- Start enqueue replicati on server #------------------- ------------------ ------------------ _ER = er.sap$(S APSYSTEMNAME)$(INS TANCE_NAME) Execute_03 = local rm - f $(_ER) Execute_04 = local ln - s -f $(DIR_EXECUTABLE)/ enrepserver$(FT_EXE) $(_ER) Start_Program_00 = local $(_ER) pf=$(_PF) NR=$(SCSID)` Para volver a configurar esta sección para el replicador de puesta en cola 2:	SAP

Tarea	Descripción	Habilidades requeridas
	1. Cambie el prefijo del `_ER` programa para que `_ENQR` se base en las últimas notas de SAP (OSS Note 2501860; requiere una SAP ONE Support Launchpad user account). 2. Cambie el binario del replicador de colas a en lugar de `enq_replicator` a `enrepserver`. 3. Asegúrese de que `Autostart = 0`. Esta sección de perfil tendrá un aspecto similar al siguiente después de los cambios. `#------------------ ------------------ ------------------- Start enqueue replication server #------------------- ------------------ ------------------ _ENQR = enqr.sap$(SAPSYSTEMNAME)$(INSTANCE_NAME) Execute_01 = local rm -f $(_ENQR) Execute_02 = local ln -s -f $(DIR_EXECUTABLE)/enq_replicator$(FT_EXE) $(_ENQR)`	

Tarea	Descripción	Habilidades requeridas
	`` Start_Program_00 = local $(_ENQR) pf= $(_PF) NR=$(SCSID) … Autostart = 0 ``` Importante: `_ENQR` no debe tener habilitada la opción de reinicio. Si `RestartProgram_01` está configurada para `_ENQR`, cámbiela a `StartProgram_01`. Esto evita que SAP reinicie el servicio o interfiera con los servicios gestionados por clústeres.	

Tarea	Descripción	Habilidades requeridas
Reinicie SAP Start Services.	Tras cambiar los perfiles descritos anteriormente en esta epopeya, reinicie SAP Start Services tanto para ASCS/SCS como para ERS. `sapcontrol -nr 10 -function RestartService SCT` `sapcontrol -nr 11 -function RestartService SCT` donde `SCT` se refiere al ID del sistema SAP y suponiendo que 10 y 11 son los números de instancia de las instancias de ASCS/SCS y ERS, respectivamente.	SAP

Vuelva a configurar el clúster para ENSA2 (obligatorio para ambos escenarios)

Tarea	Descripción	Habilidades requeridas
Verifique los números de versión en los agentes de recursos de SAP.	Cuando utiliza SUM para actualizar SAP a S/4HANA 1809 o posterior, SUM gestiona los cambios de parámetros en los perfiles de SAP. Solo el clúster requiere un ajuste manual. Sin embargo, le recomendamos que compruebe la configuración de los parámetros antes	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	de realizar cualquier cambio en el clúster. Nota: en los ejemplos de esta epic, se supone que está utilizando el sistema operativo SUSE. Si está utilizando RHEL, necesitará utilizar herramientas como YUM y pcs shell en lugar de Zypper y crm. Compruebe ambos nodos de la arquitectura para confirmar que el paquete de `resource-agents` coincide con la versión mínima recomenda da por SAP. Para el SLES, consulte la nota 2641019 de SAP OSS. Para RHEL, consulte la nota 2641322 de SAP OSS. (SAP Notes requiere una cuenta de usuario de SAP ONE Support Launchpad). `sapers:sctadm 23> zypper search -s -i resource-agents Loading repository data... Reading installed packages... S | Name | Type | Version | Arch | Repository`	

Tarea	Descripción	Habilidades requeridas
	`--+------------ ----+---------+--- ----------+-- ------+---------- ----------------- i | resource-agents | package | 4.8.0+git 30.d0077df0-150300 .8.28.1 | x86_64 | SLE-Product-HA15-SP3- Updates` Actualice la versión `resource-agents` si es necesario.	
Realice una copia de seguridad de la configuración del clúster.	Realice una copia de seguridad de la configuración del clúster de CRM de la siguiente manera. `crm configure show > /tmp/cluster_config_backup.txt`	Administrador de sistemas de AWS
Establecer el modo de mantenimiento.	Configure el clúster en modo de mantenimiento. `crm configure property maintenance-mode="true"`	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
Compruebe la configuración del clúster.	Compruebe la configuración actual del clúster. `crm configure show` He aquí un extracto del resultado completo: `node 1: sapascs` `node 2: sapers` `...` `primitive rsc_sap_S` `CT_ASCS10 SAPInstance` `\` `operations $id=rsc_s` `ap_SCT_ASCS10-oper` `ations \` `op monitor interval=120` `timeout=60 on-fail=r` `estart \` `params InstanceN` `ame=SCT_ASCS10_sap` `ascsvirt START_PRO` `FILE="/sapmnt/SCT/` `profile/SCT_ASCS10` `_sapascsvirt" \` `AUTOMATIC_RECOVER=` `false \` `meta resource-stickines` `s=5000 failure-t` `imeout=60 migration-` `threshold=1 priority=` `10` `primitive rsc_sap_S` `CT_ERS11 SAPInstance \` `operations $id=rsc_s` `ap_SCT_ERS11-opera` `tions \` `op monitor interval=120` `timeout=60 on-fail=r` `estart \`	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	<pre>params InstanceN ame=SCT_ERS11_sape rsvirt START_PRO FILE="/sapmnt/SCT/ profile/SCT_ERS11_ sapersvirt" \ AUTOMATIC_RECOVER= false IS_ERS=true \ meta priority=1000 ... colocation col_sap_S CT_no_both -5000: grp_SCT_ERS11 grp_SCT_ASCS10 location loc_sap_S CT_failover_to_ers rsc_sap_SCT_ASCS10 \ rule 2000: runs_ers_SCT eq 1 order ord_sap_S CT_first_start_asc s Optional: rsc_sap_S CT_ASCS10:start rsc_sap_SCT_ERS11: stop symmetrical=false ...</pre> donde `sapascsvirt` se refiere al nombre de host virtual de las instancias de ASCS, `sapersvirt` se refiere al nombre de host virtual de las instancias de ERS y SCT se refiere al ID del sistema SAP.	

Tarea	Descripción	Habilidades requeridas
Elimine la restricción de colocación de la conmutación por error.	En el ejemplo anterior, la restricción de ubicación `loc_sap_SCT_failover_to_ers` especifica que la función ENSA1 del ASCS debe seguir siempre la instancia del ERS en caso de conmutación por error. Con ENSA2, el ASCS debería poder realizar la conmutación por error libremente a todos los nodos participantes, de modo que se pueda eliminar esta restricción. `crm configure delete loc_sap_SCT_failover_to_ers`	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
Ajuste las primitivas.	También necesitará realizar cambios menores en las primitivas SAPInstance de ASCS y ERS. Este es un ejemplo de una primitiva ASCS SAPInstan ce que está configurada para ENSA1. `primitive rsc_sap_S CT_ASCS10 SAPInstance \ operations $id=rsc_s ap_SCT_ASCS10-oper ations \ op monitor interval=120 timeout=60 on-fail=r estart \ params InstanceN ame=SCT_ASCS10_sap ascsvirt START_PRO FILE="/sapmnt/SCT/ profile/SCT_ASCS10 _sapascsvirt" \ AUTOMATIC_RECOVER= false \ meta resource-stickines s=5000 failure-t imeout=60 migration- threshold=1 priority= 10` Para actualizar a ENSA2, cambie esta configuración por la siguiente.	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	`primitive rsc_sap_S CT_ASCS10 SAPInstance \ operations $id=rsc_s ap_SCT_ASCS10-oper ations \ op monitor interval=120 timeout=60 on-fail=r estart \ params InstanceN ame=SCT_ASCS10_sap ascsvirt START_PRO FILE="/sapmnt/SCT/ profile/SCT_ASCS10 _sapascsvirt" \ AUTOMATIC_RECOVER= false \ meta resource-stickines s=3000`  Este es un ejemplo de una primitiva SAPInstance de ERS configurada para ENSA1.  `primitive rsc_sap_S CT_ERS11 SAPInstance \ operations $id=rsc_s ap_SCT_ERS11-opera tions \ op monitor interval=120 timeout=60 on-fail=r estart \ params InstanceN ame=SCT_ERS11_sape rsvirt START_PRO FILE="/sapmnt/SCT/ profile/SCT_ERS11_ sapersvirt" \ AUTOMATIC_RECOVER= false IS_ERS=true \`	

Tarea	Descripción	Habilidades requeridas
	`meta priority=1000` Para actualizar a ENSA2, cambie esta configuración por la siguiente. `primitive rsc_sap_SCT_ERS11 SAPInstance \ operations $id=rsc_sap_SCT_ERS11-operations \ op monitor interval=120 timeout=60 on-fail=restart \ params InstanceName=SCT_ERS11_sapersvirt START_PROFILE="/sapmnt/SCT/profile/SCT_ERS11_sapersvirt" \ AUTOMATIC_RECOVER=false IS_ERS=true` Puede cambiar las primitivas de varias formas. Por ejemplo, puede revisarlas en un editor como vi, como se muestra en el siguiente ejemplo. `crm configure edit rsc_sap_SCT_ERS11`	

Tarea	Descripción	Habilidades requeridas
Deshabilitar el modo de mantenimiento.	Deshabilitar el modo de mantenimiento en el clúster. `crm configure property maintenance-mode=" false"` Cuando el clúster está fuera del modo de mantenimiento, intente poner en línea las instancias de ASCS y ERS con la nueva configuración de ENSA2.	Administrador de sistemas de AWS

(Opcional) Añada nodos de clúster

Tarea	Descripción	Habilidades requeridas
Consulte las mejores prácticas .	Antes de añadir más nodos, asegúrese de comprender las prácticas recomendadas, como por ejemplo si debe utilizar un número par o impar de nodos.	Administrador de sistemas de AWS
Añadir nodos.	Añadir más nodos implica una serie de tareas, como actualizar el sistema operativo , instalar paquetes de software que coincidan con los nodos existentes y hacer que los montajes estén disponibl es. Puede utilizar la opción Preparar un host adicional en el Administrador de aprovisio	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	namiento de software de SAP (SWPM) para crear una línea base del host específic a para SAP. Para obtener más información, consulte las guías de SAP que se muestran en la siguiente sección.	

Recursos relacionados

Referencias de SAP y SUSE

Para acceder a SAP Notes, debe tener una cuenta de usuario de SAP ONE Support Launchpad. Para obtener más información, consulte el sitio web de soporte de SAP.

- SAP Note 2501860 – Documentación del servidor de aplicaciones SAP para ABAP 7.52 NetWeaver
- SAP Note 2641019: Instalación de ENSA2 y actualización de ENSA1 a ENSA2 en un entorno SUSE HA
- SAP Note 2641322: Instalación de ENSA2 y actualización de ENSA1 a ENSA2 al utilizar las soluciones de Red Hat HA para SAP
- Nota de SAP 2711036: Uso del servidor Enqueue 2 independiente en un entorno de alta disponibilidad
- Servidor Enqueue 2 independiente (documentación de SAP)
- SAP S/4 HANA: Clúster de alta disponibilidad de Enqueue Replication 2: guía de configuración (documentación de SUSE)

Referencias de AWS

- SAP HANA en AWS: guía de configuración de alta disponibilidad para SLES y RHEL
- SAP Lens: Marco de AWS Well-Architected

Utilice zonas de disponibilidad coherentes en las VPC en diferentes cuentas de AWS

Creado por Adam Spicer (AWS)

Repositorio de código: mapeo de zonas de disponibilidad de varias cuentas	Entorno: producción	Tecnologías: bases de datos; infraestructura
Servicios de AWS: AWS CloudFormation; Amazon VPC; AWS Lambda		

Resumen

En la nube de Amazon Web Services (AWS), una zona de disponibilidad tiene un nombre que puede variar entre sus cuentas de AWS y un Identificador de zona de disponibilidad (AZ ID) que identifica su ubicación. Si utiliza AWS CloudFormation para crear nubes privadas virtuales (VPC), debe especificar el nombre o el ID de la zona de disponibilidad al crear las subredes. Si crea VPC en varias cuentas, el nombre de la zona de disponibilidad es aleatorio, lo que significa que las subredes utilizan distintas zonas de disponibilidad en cada cuenta.

Para usar la misma zona de disponibilidad en todas sus cuentas, debe asignar el nombre de la zona de disponibilidad de cada cuenta al mismo Identificador de zona de disponibilidad. Por ejemplo, en el siguiente diagrama se muestra que el Identificador AZ de `use1-az6` se llama `us-east-1a` en la cuenta A de AWS y `us-east-1c` en la cuenta Z de AWS.

Este patrón ayuda a garantizar la coherencia zonal al proporcionar una solución escalable y multicuenta para utilizar las mismas zonas de disponibilidad en sus subredes. La coherencia zonal garantiza que el tráfico de red entre cuentas evite las rutas de red entre zonas de disponibilidad, lo que ayuda a reducir los costos de transferencia de datos y a reducir la latencia de red entre las cargas de trabajo.

Este patrón es un enfoque alternativo a la CloudFormation AvailabilityZoneId propiedad de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Al menos dos cuentas de AWS activas en la misma región de AWS.
- Evalúe cuántas zonas de disponibilidad se necesitan para cumplir con los requisitos de VPC en la región.
- Identifique y registre el Identificador de zona de disponibilidad para cada zona de disponibilidad que necesite admitir. Para obtener más información al respecto, consulte los Identificadores de zona de disponibilidad de sus recursos de AWS en la documentación de AWS Resource Access Manager.
- Una lista ordenada y separada por comas de sus Identificadores de AZ. Por ejemplo, la primera zona de disponibilidad de la lista se mapea como `az1`, la segunda zona de disponibilidad se mapea como `az2` y esta estructura de mapeo continúa hasta que la lista separada por comas esté completamente mapeada. No hay un número máximo de Identificadores de AZ que se pueden mapear.
- El `az-mapping.yaml` archivo del repositorio de mapeo de zonas de disponibilidad de GitHub múltiples cuentas, copiado en su máquina local

Arquitectura

El siguiente diagrama muestra la arquitectura que se implementa en una cuenta y que crea los valores de Almacén de parámetros de AWS Systems Manager. Estos valores del almacén de parámetros se consumen al crear una VPC en la cuenta.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. La solución de este patrón se implementa en todas las cuentas que requieren coherencia zonal para una VPC.
2. La solución crea valores de almacén de parámetros para cada Identificador de zona de disponibilidad y almacena el nombre de la nueva zona de disponibilidad.
3. La CloudFormation plantilla de AWS utiliza el nombre de la zona de disponibilidad almacenado en cada valor del almacén de parámetros, lo que garantiza la coherencia zonal.

En el siguiente diagrama, se muestra el flujo de trabajo para crear una VPC con la solución de este patrón.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Envíe una plantilla para crear una VPC a AWS. CloudFormation
2. AWS CloudFormation resuelve los valores del almacén de parámetros de cada zona de disponibilidad y devuelve el nombre de la zona de disponibilidad de cada ID de zona de disponibilidad.
3. Se crea una VPC con los Identificador de AZ correctos necesarios para garantizar la coherencia zonal.

Tras implementar la solución de este patrón, puede crear subredes que hagan referencia a los valores del almacén de parámetros. Si usa AWS CloudFormation, puede hacer referencia a los valores de los parámetros de mapeo de zonas de disponibilidad del siguiente código de ejemplo con formato YAML:

```
Resources:
    PrivateSubnet1AZ1:
        Type: AWS::EC2::Subnet
        Properties:
            VpcId: !Ref VPC
            CidrBlock: !Ref PrivateSubnetAZ1CIDR
            AvailabilityZone:
                !Join
                    - ''
                    - - '{{resolve:ssm:/az-mapping/az1:1}}'
```

Este código de muestra se incluye en el `vpc-example.yaml` archivo del repositorio de mapeo de zonas de disponibilidad de GitHub varias cuentas. Le muestra cómo crear una VPC y subredes que se alineen con los valores del almacén de parámetros para garantizar la coherencia zonal.

Pila de tecnología

- AWS CloudFormation
- AWS Lambda
- Almacén de parámetros de AWS Systems Manager

Automatizar y escalar

Puede implementar este patrón en todas sus cuentas de AWS mediante AWS CloudFormation StackSets o la solución Customizations for AWS Control Tower. Para obtener más información, consulte Trabajar con AWS CloudFormation StackSets en la documentación de AWS Cloudformation y Personalizaciones para la Torre de Control de AWS en la biblioteca de soluciones de AWS.

Después de implementar la CloudFormation plantilla de AWS, puede actualizarla para usar los valores del almacén de parámetros e implementar sus VPC en canalizaciones o según sus requisitos.

Herramientas

Servicios de AWS

- AWS le CloudFormation ayuda a modelar y configurar sus recursos de AWS, a aprovisionarlos de forma rápida y coherente y a gestionarlos durante todo su ciclo de vida. Facilita poder usar una plantilla para describir los recursos y sus dependencias, y lanzarlos y configurarlos juntos como una pila, en lugar de administrarlos de forma individual. Puede administrar y aprovisionar pilas en varias cuentas y regiones de AWS.
- AWS Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo. Solo pagará por el tiempo de computación que consuma, no se aplican cargos cuando el código no se está ejecutando.
- Almacén de parámetros de AWS Systems Manager es una funcionalidad de AWS Systems Manager. Proporciona un almacenamiento seguro y jerárquico para administrar los datos de configuración y los secretos.

Código

El código de este patrón se proporciona en el repositorio de mapeo de zonas de disponibilidad de GitHub múltiples cuentas.

Epics

Implemente el archivo az-mapping.yaml

Tarea	Descripción	Habilidades requeridas
Determine las zonas de disponibilidad requeridas para la región.	1. Determine los Identificador de zona de disponibilidad que se deben utilizar de forma sistemática en su región. 2. Registre estos Identificador de AZ en una lista separada por comas y en el orden en el que desea que se apliquen. Por ejemplo, la primera zona de disponibilidad de la lista se mapea como `az1` y la segunda se mapea como `az2`. No hay un número máximo de Identificadores de AZ que se pueden mapear.	Arquitecto de la nube
Implemente el archivo az-mapping.yaml.	Utilice el `az-mapping.yaml` archivo para crear una CloudFormation pila de AWS en todas las cuentas de AWS necesarias. En el parámetro `AZIds`, utilice la lista separada por comas que creó anteriormente. Le recomendamos que utilice AWS CloudFormation StackSets o la solución	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	Customizations for AWS Control Tower.	

Implemente las VPC en sus cuentas

Tarea	Descripción	Habilidades requeridas
Personalice las CloudFormation plantillas de AWS.	Cuando cree las subredes con AWS CloudFormation, personalice las plantillas para que usen los valores del almacén de parámetros que creó anteriormente. Para ver una plantilla de ejemplo, consulte el `vpc-example.yaml` archivo en el repositorio de mapeo de zonas de disponibilidad de GitHub múltiples cuentas.	Arquitecto de la nube
Implemente las VPC.	Implemente las CloudFormation plantillas de AWS personalizadas en sus cuentas. Por lo tanto, cada VPC de la región tiene coherencia zonal en las zonas de disponibilidad utilizadas para las subredes	Arquitecto de la nube

Recursos relacionados

- Identificadores de zona de disponibilidad para sus recursos de AWS (documentación de AWS Resource Access Manager)

- AWS::EC2::Subnet(CloudFormation documentación de AWS)

Validar Account Factory para el código Terraform (AFT) localmente

Creado por Alexandru Pop (AWS) y Michal Gorniak (AWS)

Entorno: producción	Tecnologías: infraestructura; modernización DevOps; desarrollo y pruebas de software	Carga de trabajo: código abierto
Servicios de AWS: AWS Control Tower		

Resumen

Este patrón muestra cómo probar localmente el código de HashiCorp Terraform administrado por AWS Control Tower Account Factory for Terraform (AFT). HashiCorp Terraform es una herramienta de infraestructura como código (IaC) y de código abierto que facilita usar el código para aprovisionar y administrar la infraestructura y los recursos de la nube. AFT configura una canalización de Terraform que le ayuda a aprovisionar y personalizar varias cuentas de AWS Control Tower.

Durante el desarrollo del código, puede resultar útil probar su infraestructura de Terraform como código (IaC) a nivel local, fuera de la canalización de AFT. Este ejemplo muestra cómo hacer lo siguiente:

- Obtenga una copia local del código de Terraform que está almacenado en los CodeCommit repositorios de AWS de su cuenta de administración de AFT.
- Simule la canalización de AFT de forma local con el código recuperado.

Este procedimiento también se puede utilizar para ejecutar comandos de Terraform que no forman parte de la canalización AFT normal. Por ejemplo, puede usar este método para ejecutar comandos como `terraform validate`, `terraform plan`, `terraform destroy`, `yterraform import`.

Requisitos previos y limitaciones

Requisitos previos

- Un entorno multicuenta de AWS activo que utiliza AWS Control Tower

- Un entorno AFT completamente implementado
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada
- Ayudante de credenciales de AWS CLI para Code Commit, instalado y configurado
- Python 3.x
- Git, instalada y configurada en la máquina
- git-remote-commit utilidad, instalada y configurada
- Terraform, instalado y configurado (la versión local del paquete Terraform debe coincidir con la versión que se utiliza en la implementación de AFT)

Limitaciones

- Este patrón no cubre los pasos de implementación necesarios para AWS Control Tower, AFT ni ningún módulo específico de Terraform.
- El resultado que se genera localmente durante este procedimiento no se guarda en los registros de tiempo de ejecución de AFT Pipeline.

Arquitectura

Pila de tecnología de destino

- Infraestructura AFT implementada dentro de una implementación de AWS Control Tower
- Terraform
- Git
- CLI de AWS versión 2

Automatizar y escalar

Este patrón muestra cómo invocar localmente el código de Terraform para las personalizaciones de cuentas globales de AFT en una única cuenta de AWS administrada por AFT. Una vez validado el código de Terraform, puede aplicarlo al resto de las cuentas de su entorno de múltiples cuentas. Para obtener más información, consulte Volver a invocar las personalizaciones en la documentación de AWS Control Tower.

También puede usar un proceso similar para ejecutar las personalizaciones de la cuenta AFT en una terminal local. Para invocar localmente el código de Terraform desde las personalizaciones

de la cuenta AFT, clone el aft-account-customizations repositorio en lugar del aft-global-account-customizationsrepositorio desde CodeCommit su cuenta de administración de AFT.

Herramientas

Servicios de AWS

- AWS Control Tower le ayuda a configurar y regular un entorno de cuentas múltiples de AWS siguiendo las prácticas recomendadas prescriptivas.
- La Interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que permite interactuar con los servicios de AWS mediante comandos en el intérprete de comandos de línea de comandos.

Otros servicios

- HashiCorp Terraform es una herramienta de código abierto de infraestructura como código (IaC) que le ayuda a usar el código para aprovisionar y administrar la infraestructura y los recursos de la nube.
- Git es un sistema de control de versiones distribuido y de código abierto.

Código

El siguiente es un ejemplo de un script bash que se puede usar para ejecutar localmente el código de Terraform administrado por AFT. Para usar el script, sigue las instrucciones de la sección Epics de este patrón.

```
#! /bin/bash
# Version: 1.1 2022-06-24 Unsetting AWS_PROFILE since, when set, it interferes with
 script operation
#          1.0 2022-02-02 Initial Version
#
# Purpose: For use with AFT: This script runs the local copy of TF code as if it were
 running within AFT pipeline.
#        * Facilitates testing of what the AFT pipline will do
#           * Provides the ability to run terraform with custom arguments (like 'plan'
 or 'move') which are currently not supported within the pipeline.
#
# © 2021 Amazon Web Services, Inc. or its affiliates. All Rights Reserved.
# This AWS Content is provided subject to the terms of the AWS Customer Agreement
# available at http://aws.amazon.com/agreement or other written agreement between
```

```
# Customer and either Amazon Web Services, Inc. or Amazon Web Services EMEA SARL or
 both.
#
# Note: Arguments to this script are passed directly to 'terraform' without parsing nor
 validation by this script.
#
# Prerequisites:
#    1. local copy of ct GIT repositories
#    2. local backend.tf and aft-providers.tf filled with data for the target account
 on which terraform is to be run
#       Hint: The contents of above files can be obtain from the logs of a previous
 execution of the AFT pipeline for the target account.
#    3. 'terraform' binary is available in local PATH
#    4. Recommended: .gitignore file containing 'backend.tf', 'aft_providers.tf' so the
 local copy of these files are not pushed back to git

readonly credentials=$(aws sts assume-role \
    --role-arn arn:aws:iam::$(aws sts get-caller-identity --query "Account" --output
 text ):role/AWSAFTAdmin \
    --role-session-name AWSAFT-Session \
    --query Credentials )

unset AWS_PROFILE
export AWS_ACCESS_KEY_ID=$(echo $credentials | jq -r '.AccessKeyId')
export AWS_SECRET_ACCESS_KEY=$(echo $credentials | jq -r '.SecretAccessKey')
export AWS_SESSION_TOKEN=$(echo $credentials | jq -r '.SessionToken')
terraform "$@"
```

Epics

Guardar el código de ejemplo como un archivo local

Tarea	Descripción	Habilidades requeridas
Guardar el código de ejemplo como un archivo local.	1. Copia el script bash de ejemplo que se encuentra en la sección Código de este patrón y pégalo en un editor de código. 2. Nombre el archivo `ct_terraform.sh` .	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	Luego, guarde el archivo localmente dentro de una carpeta dedicada, como `~/scripts ov~/bin`.	

Tarea	Descripción	Habilidades requeridas
Haga que el código de ejemplo sea ejecutable.	Abra una ventana de terminal y autentíquese en su cuenta de administración de AWS AFT al realizar una de las siguientes acciones: • Utilice un perfil de AWS CLI existente que esté configurado con los permisos necesarios para acceder a la cuenta de administración de AFT. Para utilizar el perfil, puede ejecutar el siguiente comando: `export AWS_PROFILE=<aft account profile name>` • Si su organización usa el SSO para acceder a AWS, introduzca las credenciales de su cuenta de administración de AFT en la página de SSO de su organización. Nota: Es posible que su organización también tenga una herramienta personalizada para proporcionar credenciales de autenticación a su entorno de AWS.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Verifique el acceso a la cuenta de administración de AFT en la región de AWS correcta.	Importante: asegúrese de utilizar la misma sesión de terminal con la que se autenticó en su cuenta de administración de AFT. 1. Navegue hasta la región de AWS de su implement ación de AFT ejecutando el siguiente comando: `export AWS_REGIO N=<aft_region>` 2. Asegúrese de estar en la cuenta correcta al realizar lo siguiente: • Ejecute el siguiente comando: `aws code-commit list-repositories` • A continuación, compruebe que los repositorios que aparecen en el resultado coincidan con los nombres de los repositor ios que se encuentran en su cuenta de administr ación de AFT.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Crear un nuevo directorio local para almacenar el código del repositorio de AFT.	En la misma sesión de terminal, ejecute los siguientes comandos: `mkdir my_aft` `cd my_aft`	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Clone el código del repositorio AFT remoto.	1. Ejecute el siguiente comando desde el terminal: `git clone codecommit::$AWS_REGION://aft-global-customizations` Nota: para simplificar, este procedimiento y AFT utilizan únicamente una rama de código principal. Para utilizar la ramificación de código, también puede introducir comandos de ramificación de código aquí. Sin embargo, cualquier cambio aplicado desde la rama no principal se revertirá cuando la automatización de AFT aplique el código desde la rama principal. 2. A continuación, navegue hasta el directorio clonado ejecutando el siguiente comando: `cd aft-global-customizations/terraform`	Administrador de AWS

Cree los archivos de configuración de Terraform necesarios para que la canalización AFT se ejecute localmente

Tarea	Descripción	Habilidades requeridas
Abra una canalización AFT previamente ejecutada y copie los archivos de configuración de Terraform en una carpeta local.	Nota: los archivos de configuración backend.tf y aft-providers.tf que se crean en esta epic son necesarios para que la canalización de AFT se ejecute localmente. Estos archivos se crean automáticamente dentro de la canalización de AFT basada en la nube, pero deben crearse manualmente para que la canalización se ejecute localmente. La ejecución local de la canalización de AFT requiere un conjunto de archivos que represente la ejecución de la canalización en una sola cuenta de AWS. 1. Con las credenciales de su cuenta de administración de AWS Control Tower, inicie sesión en la Consola de administración de AWS. A continuación, abra la CodePipeline consola de AWS. Asegúrese de que está en la misma Región de AWS donde ha implementado AFT.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	2. En el panel de navegación izquierdo, seleccione Canalizaciones. 3. Seleccione ##########-customizations-pipeline. (El ########## es la ID de cuenta de AWS que utiliza para ejecutar el código de Terraform de forma local). 4. Asegúrese de que la ejecución más reciente marcada muestre un valor correcto. Si el valor es diferente, debe volver a invocar las personalizaciones en el proceso de AFT. Para obtener más información, consulte Volver a invocar las personalizaciones en la documentación de AWS Control Tower. 5. Seleccione el tiempo de ejecución más reciente para ver sus detalles. 6. En la sección Apply-AFT-Global-Customizations, busque la etapa Apply-Terraform. 7. Seleccione la sección Detalles de la etapa Apply-Terraform.	

Tarea	Descripción	Habilidades requeridas
	8. Busque el registro de tiempo de ejecución de la etapa Apply-Terraform. 9. En el registro de tiempo de ejecución, busca la sección que comienza y termina con las siguientes líneas: “\n \n aft-providers.tf … “\n \n backend.tf” 10. Copia el resultado entre estas dos etiquetas y guárdalo como un archivo local con un nombre `aft-providers.tf` dentro de la carpeta Terraform local (el directorio de trabajo actual de tu sesión de terminal). Ejemplo de sentencia providers.tf generada automáticamente `## Autogenerated providers.tf ## ## Updated on: 2022-05-31 16:27:45 ## provider "aws" { region = "us-east-2" assume_role { role_arn = "arn:aws:iam::######## :role/AWSAFTExecution" }`	

Tarea	Descripción	Habilidades requeridas
	<pre>default_tags { tags = { managed_by = "AFT" } } }</pre> 11. En el registro de tiempo de ejecución, busque la sección que comienza y termina con las siguiente s líneas: “\n\n tf … “\n \n backup.tf 12. Copia el resultado entre estas dos etiquetas y guárdalo como un archivo local con un nombre `tf` dentro de la carpeta Terraform local (el directori o de trabajo actual de tu sesión de terminal). Ejemplo de sentencia backend.tf generada automáticamente <pre>## Autogenerated backend.tf ## ## Updated on: 2022-05-3 1 16:27:45 ## terraform { required_version = ">= 0.15.0" backend "s3" { region = "us-east-2"</pre>	

Tarea	Descripción	Habilidades requeridas
	<pre> bucket = "aft-backend-##### #######-primary-re gion" key = "############-aft- global-customizati ons/terraform.tfst ate" dynamodb_table = "aft-backend-##### #######" encrypt = "true" kms_key_id = "cbdc21d6-e04d-4c3 7-854f-51e199cfcb7c" kms_key_id = "########-####-####- ####-############" role_arn = "arn:aws:iam::#### #########:role/AWS AFTExecution" } }</pre> Nota: los archivos `backend.tf` y `aft-providers.tf` están vinculados a una cuenta de AWS, una implement ación de AFT y una carpeta específicas. Estos archivos también son diferentes, dependiendo de si están en el aft-global-customi zationsrepositorio y en el aft-account-custom izationsrepositorio dentro de	

Tarea	Descripción	Habilidades requeridas
	la misma implementación de AFT. Asegúrese de generar ambos archivos a partir de la misma lista de tiempo de ejecución.	

Ejecute la canalización AFT localmente mediante el script bash de ejemplo

Tarea	Descripción	Habilidades requeridas
Implemente los cambios de configuración de Terraform que desee validar.	1. Navegue hasta el aft-global-customizationsrepository clonado ejecutando el siguiente comando: `cd aft-global-customizations/terraform` Nota: los archivos `backend.tf` y `aft-providers.tf` están en este directorio. El directorio también contiene los archivos de Terraform del aft-global-customizations repositorio. 2. Incorpore los cambios de código de Terraform que desee probar localmente en los archivos de configuración.	Administrador de AWS
Ejecute el script ct_terraform.sh y revise el resultado.	1. Navegue hasta la carpeta local que contiene el script sh.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	2. Para validar el código de Terraform modificado, ejecute el script `ct_terraform.sh` ejecutando el siguiente comando: `~/scripts/ct_terraform.sh apply` Nota: puedes ejecutar cualquier comando de Terraform durante este paso. Para ver una lista completa de comandos de Terraform, ejecute el siguiente comando: `terraform --help` 3. Revise el resultado de este comando. A continuación, depure los cambios de código localmente antes de confirmarlos y devolverlos al repositorio AFT. Importante: • Cualquier cambio realizado localmente y que no se devuelva al repositorio remoto es temporal y se puede deshacer en cualquier momento	

Tarea	Descripción	Habilidades requeridas
	mediante una automatiz ación de canalización de AFT en ejecución. • La automatización de AFT se puede ejecutar en cualquier momento, ya que otros usuarios pueden invocarla y activar la automatización de AFT. • AFT siempre aplicará el código de la rama principal del repositorio, deshacien do cualquier cambio no confirmado.	

Confirmar y devolver los cambios de su código local al repositorio AFT

Tarea	Descripción	Habilidades requeridas
Añada referencias a los archivos.tf de backend.tf y aft-providers.tf a un archivo.g itignore.	Añada los archivos `backend.tf` y `aft-providers.tf` que creó a un archivo `.gitignore` ejecutando los siguientes comandos: `echo backend.tf >> .gitignore` `echo aft-providers.tf >>.gitignore` Nota: al mover los archivos al archivo `.gitignore` , se garantiza que no se confirmen	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	ni se devuelvan al repositorio AFT remoto.	
Confirme y envíe los cambios de código al repositorio AFT remoto.	1. Para añadir nuevos archivos de configuración de Terraform al repositor io, ejecute el siguiente comando: `git add <filename>` 2. Para confirmar los cambios y enviarlos al repositor io AFT remoto de AWS CodeCommit, ejecute los siguientes comandos: `git commit -a` `git push` Importante: los cambios de código que introduzca siguiendo este procedimi ento hasta este momento se aplican únicamente a una cuenta de AWS.	Administrador de AWS

Implemente los cambios en varias cuentas administradas por AFT

Tarea	Descripción	Habilidades requeridas
Implementar los cambios en todas sus cuentas administr adas por AFT.	Para implementar los cambios en varias cuentas de AWS administradas por AFT, siga las instrucciones en Volver	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	a invocar personalizaciones en la documentación de AWS Control Tower.	

Más patrones

- Agregue HA a Oracle PeopleSoft en Amazon RDS Custom mediante una réplica de lectura
- Automatice la adición o actualización de entradas de registro de Windows con AWS Systems Manager
- Automatice la evaluación de recursos de AWS
- Automatice la implementación de productos y la cartera de AWS Service Catalog mediante AWS CDK
- Automatice la conmutación por error y la conmutación por recuperación entre regiones mediante DR Orchestrator Framework
- ???
- Automatice la replicación de las instancias de Amazon RDS en todas las cuentas de AWS
- Adjunte automáticamente una política administrada de AWS para Systems Manager a los perfiles de instancia de EC2 mediante Cloud Custodian y AWS CDK
- Crear automáticamente canalizaciones de CI/CD y clústeres de Amazon ECS para microservicios mediante AWS CDK
- Detecta automáticamente los cambios e inicia diferentes CodePipeline canalizaciones para un monorepo en CodeCommit
- ???
- Cree una canalización de datos para incorporar, transformar y analizar los datos de Google Analytics con el kit de DataOps desarrollo de AWS
- Creación de un PAC de Micro Focus Enterprise Server con Amazon EC2 Auto Scaling y Systems Manager
- Cree e inserte imágenes de Docker en Amazon ECR mediante GitHub Actions y Terraform
- Centralice la administración de claves de acceso de IAM en AWS Organizations mediante Terraform
- Centralice la distribución de paquetes de software en AWS Organizations mediante Terraform
- Encadene los servicios de AWS mediante un enfoque sin servidor
- Configure una extensión de centro de datos para VMware Cloud en AWS mediante el modo Hybrid Linked Mode
- Configure el enrutamiento de solo lectura en un grupo de disponibilidad Always On en SQL Server en AWS
- ???

- Crear automáticamente canalizaciones de CI dinámicas para proyectos de Java y Python
- Implemente un SDDC de VMware en AWS mediante VMware Cloud en AWS
- Implemente una API de Amazon API Gateway en un sitio web interno mediante puntos de conexión privados y un Equilibrador de carga de aplicación
- Implementar y depurar clústeres de Amazon EKS
- Implemente y gestione los controles de la Torre de Control de AWS mediante AWS CDK y AWS CloudFormation
- Implementación y administración de los controles de AWS Control Tower mediante Terraform
- Despliega canarios de CloudWatch Synthetics con Terraform
- Implementar la solución Security Automations para AWS WAF mediante Terraform
- Documente el diseño de su zona de aterrizaje de AWS
- Asegúrese de que el perfil de IAM esté asociado a una instancia de EC2
- Exportar los informes de AWS Backup de toda la organización en AWS Organizations como un archivo CSV
- Genere recomendaciones personalizadas y reclasificadas con Amazon Personalize
- Identifique y avise cuando los recursos de Amazon Data Firehose no estén cifrados con una clave de AWS KMS
- Implemente Account Factory for Terraform (AFT) mediante una canalización de arranque
- Instalación del agente SSM en los nodos de trabajo de Amazon EKS mediante Kubernetes DaemonSet
- Instale el agente SSM y el CloudWatch agente en los nodos de trabajo de Amazon EKS mediante preBootstrapCommands
- Integre VMware vRealize Network Insight con VMware Cloud on AWS
- Administre los productos de AWS Service Catalog en varias cuentas y regiones de AWS
- Gestión de las aplicaciones de contenedores en las instalaciones mediante la configuración de Amazon ECS Anywhere con AWS CDK
- Migrar registros DNS de forma masiva a una zona alojada privada de Amazon Route 53
- Migre Oracle E-Business Suite a Amazon RDS Custom
- Migre Oracle PeopleSoft a Amazon RDS Custom
- Migración de los sistemas BYOL de RHEL a instancias con licencia incluida de AWS mediante AWS MGN
- Migración de VMware SDDC a VMware Cloud en AWS mediante VMware HCX

- Supervise ElastiCache los clústeres de Amazon para comprobar el cifrado en reposo
- Supervise ElastiCache los clústeres para grupos de seguridad
- Supervise los clústeres de SAP RHEL Pacemaker mediante los servicios de AWS
- Acceda de forma privada a un punto de conexión de servicio central de AWS desde varias VPC
- Rotar las credenciales de la base de datos sin reiniciar los contenedores
- Enviar una notificación cuando se cree un usuario de IAM
- Envíe registros desde VMware Cloud on AWS a Splunk mediante VMware Aria Operations for Logs
- Configure una canalización de CI/CD para cargas de trabajo híbridas en Amazon ECS Anywhere mediante AWS CDK y GitLab
- Configure una PeopleSoft arquitectura de alta disponibilidad en AWS
- ???
- Configure una infraestructura de escritorio virtual (VDI) con escalado automático mediante NICE EnginFrame y el administrador de sesiones NICE DCV
- Configure una arquitectura HA/DR para Oracle E-Business Suite en Amazon RDS Custom con una base de datos en espera activa
- Configure la detección de CloudFormation desviaciones de AWS en una organización multirregional y multicuenta
- Configure una infraestructura Multi-AZ para una FCI Always On de SQL Server mediante Amazon FSx
- Configure la funcionalidad UTL_FILE de Oracle en Aurora compatible con PostgreSQL
- Simplifique la administración de certificados privados mediante AWS Private CA y AWS RAM
- Etiquete automáticamente las conexiones de puerta de enlace de tránsito con AWS Organizations
- Funciones de transición para una PeopleSoft aplicación de Oracle en Amazon RDS Custom for Oracle
- Use Serverspec para desarrollar código de infraestructura basado en pruebas

IoT

Temas

Configure el registro y la supervisión de eventos de seguridad en su entorno de AWS IoT

Creado por Prateek Prakash (AWS)

Entorno: producción	Tecnologías: IoT; seguridad, identidad, conformidad; DevOps; operaciones	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon CloudWatch; Amazon OpenSearch Service; Amazon GuardDuty; AWS IoT Core; AWS IoT Device Defender; AWS IoT Device Management; Amazon CloudWatch Logs		

Resumen

Garantizar la seguridad de sus entornos de Internet de las cosas (IoT) es una prioridad importante, ya que las organizaciones conectan miles de millones de dispositivos a sus entornos de TI. Este patrón proporciona una arquitectura de referencia que puede usar para implementar el registro y supervisión de eventos de seguridad en todo su entorno de IoT en la nube de Amazon Web Services (AWS). Por lo general, un entorno de IoT en la nube de AWS tiene estas tres capas:

- Dispositivos de IoT que generan datos de telemetría relevantes.
- Servicios de AWS IoT (por ejemplo, AWS IoT Core, AWS IoT Device Management o AWS IoT Device Defender) que conectan sus dispositivos de IoT a otros dispositivos y servicios de AWS.
- Servicios de AWS de backend que ayudan a procesar los datos de telemetría y proporcionan información útil para sus diferentes casos de uso empresarial.

Las prácticas recomendadas incluidas en el documento técnico AWS IoT Lens: Marco de AWS Well-Architected pueden ayudarle a revisar y mejorar su arquitectura basada en la nube, así como a comprender mejor el impacto empresarial de sus decisiones de diseño. Una recomendación

importante es que analice los registros y las métricas de las aplicaciones en sus dispositivos y en la nube de AWS. Para ello, puede emplear diferentes enfoques y técnicas (por ejemplo, el modelado de amenazas) con el fin de identificar las métricas y los eventos que deben supervisarse para detectar posibles problemas de seguridad.

Este patrón describe cómo usar los servicios de seguridad de AWS y AWS IoT para diseñar e implementar una arquitectura de referencia de supervisión y registro de seguridad para un entorno de IoT en la nube de AWS. Esta arquitectura aplica las prácticas recomendadas de seguridad de AWS existentes a su entorno de IoT.

Requisitos previos y limitaciones

Requisitos previos

- Un entorno de zona de aterrizaje existente. Para obtener más información al respecto, consulte la guía Configurar un entorno de AWS multicuenta seguro y escalable en el sitio web de Recomendaciones de AWS.
- Su zona de aterrizaje debe tener disponibles las siguientes cuentas:
  - Cuenta de archivo de registros: esta cuenta es para los usuarios que necesitan acceder a la información de registro de las cuentas en las unidades organizativas (OU) de su zona de aterrizaje. Para obtener más información al respecto, consulte la sección OU de seguridad: cuenta de archivo de registros de la guía Arquitectura de referencia de seguridad de AWS en el sitio web de Recomendaciones de AWS.
  - Cuenta de seguridad: sus equipos de seguridad y conformidad usan esta cuenta para realizar auditorías u operaciones de seguridad de emergencia. Esta cuenta también se designa como cuenta de administrador de Amazon GuardDuty. Los usuarios de la cuenta de administrador pueden configurar GuardDuty, además de ver y gestionar GuardDuty los resultados, para su propia cuenta y para todas las cuentas de los miembros. Para obtener más información al respecto, consulta la sección Gestión de varias cuentas GuardDuty en la GuardDuty documentación de Amazon.
  - Cuenta de IoT: esta cuenta es para su entorno de IoT.

Arquitectura

Este patrón amplía la solución de registro centralizado de la biblioteca de soluciones de AWS para recopilar y procesar eventos de IoT relacionados con la seguridad. La solución de registro centralizado se implementa en la cuenta de seguridad y ayuda a recopilar, analizar y mostrar

CloudWatch los registros de Amazon en un único panel de control. Esta solución consolida, administra y analiza los archivos de registro de múltiples fuentes. Por último, la solución de registro centralizado también utiliza Amazon OpenSearch Service y OpenSearch Dashboards para mostrar una vista unificada de todos los eventos de registro.

El siguiente diagrama de arquitectura muestra los componentes clave de una arquitectura de registro y referencia de seguridad de IoT en la nube de AWS.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Los objetos del IoT son los dispositivos que deben supervisarse para detectar eventos de seguridad anómalos. Estos dispositivos ejecutan un agente para publicar eventos o métricas de seguridad en AWS IoT Core y AWS IoT Device Defender.
2. Cuando el registro de AWS IoT está habilitado, AWS IoT envía eventos de progreso sobre cada mensaje a medida que pasa de sus dispositivos a través del agente de mensajes y el motor de reglas a Amazon CloudWatch Logs. Puede usar las suscripciones de CloudWatch Logs para enviar eventos a una solución de registro centralizado. Para obtener más información al respecto, consulte métricas y dimensiones de AWS IoT en la documentación de AWS IoT Core.
3. AWS IoT Device Defender ayuda a supervisar las configuraciones inseguras y las métricas de seguridad de sus dispositivos de IoT. Cuando se detecta una anomalía, las alarmas notifican a Amazon Simple Notification Service (Amazon SNS), que cuenta con una función de Lambda de AWS como suscriptor. La función Lambda envía la alarma como un mensaje a CloudWatch Logs. Puede usar las suscripciones de CloudWatch Logs para enviar eventos a su solución de registro centralizado. Para obtener más información al respecto, consulte Comprobaciones de auditoría, Métricas en el lado del dispositivo y Métricas en el lado de la nube en la documentación de AWS IoT Core.
4. AWS CloudTrail registra las acciones del plano de control de AWS IoT Core que realizan cambios (por ejemplo, crear, actualizar o adjuntar API). Cuando CloudTrail se configura como parte de una implementación de landing zone, envía los eventos a los CloudWatch registros y puedes usar las suscripciones para enviar los eventos a tu solución de registro centralizado.
5. Las reglas administradas o personalizadas de AWS Config evalúan los recursos que forman parte de su entorno de IoT. Supervise sus notificaciones de cambios de conformidad utilizando CloudWatch Events with CloudWatch Logs como objetivo. Después de enviar las notificaciones de cambios de conformidad a CloudWatch Logs, puede utilizar las suscripciones para transferir los eventos a su solución de registro centralizado.

6. Amazon analiza GuardDuty continuamente los eventos CloudTrail de administración y ayuda a identificar las llamadas a las API realizadas a los puntos de conexión de AWS IoT Core desde direcciones IP maliciosas conocidas, geolocalizaciones inusuales o proxies anónimos. Supervisa GuardDuty las notificaciones mediante Amazon CloudWatch Events con grupos de CloudWatch registros en Logs como destino. Cuando GuardDuty las notificaciones se envían a CloudWatch Logs, puede usar las suscripciones para enviar los eventos a su solución de monitoreo centralizado o usar la GuardDuty consola de su cuenta de seguridad para ver las notificaciones.
7. AWS Security Hub supervisa su cuenta de IoT mediante las prácticas recomendadas de seguridad. Supervise las notificaciones de Security Hub utilizando CloudWatch Eventos con grupos de CloudWatch registros en Logs como destino. Cuando las notificaciones de Security Hub se envíen a CloudWatch Logs, utilice las suscripciones para enviar eventos a su solución de supervisión centralizada o utilice la consola del Security Hub de su cuenta de seguridad para ver las notificaciones.
8. Amazon Detective evalúa y analiza la información para aislar la causa raíz y tomar medidas en función de los resultados de seguridad de las llamadas inusuales a puntos de conexión de AWS IoT u otros servicios de su arquitectura de IoT.
9. Amazon Athena consulta los registros almacenados en su cuenta de Log Archive para comprender mejor los resultados de seguridad e identificar tendencias y actividades maliciosas.

Herramientas

- Amazon Athena es un servicio de consultas interactivo que facilita el análisis de datos directamente en Amazon Simple Storage Service (Amazon S3) con SQL estándar.
- AWS le CloudTrail ayuda a habilitar la gobernanza, el cumplimiento y la auditoría operativa y de riesgos de su cuenta de AWS.
- Amazon CloudWatch supervisa los recursos de AWS y las aplicaciones que ejecuta en AWS en tiempo real. Puede utilizarlas CloudWatch para recopilar y realizar un seguimiento de las métricas, que son variables que puede medir para sus recursos y aplicaciones.
- Amazon CloudWatch Logs centraliza los registros de todos los sistemas, aplicaciones y servicios de AWS que utilice. Esto le permite consultarlos, buscar códigos de error o patrones específicos, filtrarlos en función de campos específicos o archivarlos de forma segura para análisis futuros.
- AWS Config brinda una visión detallada de la configuración de los recursos de AWS de su cuenta de AWS.

- Amazon Detective ayuda a analizar, investigar e identificar rápidamente la causa raíz de resultados de seguridad o actividades sospechosas.
- AWS Glue es un servicio completamente administrado de ETL (extracción, transformación y carga) con el que resulta más rentable y sencillo categorizar los datos, limpiarlos, enriquecerlos y moverlos de manera fiable entre distintos almacenes y flujos de datos.
- Amazon GuardDuty es un servicio de supervisión continua de la seguridad.
- AWS IoT Core proporciona una comunicación bidireccional segura para que los dispositivos conectados a Internet (como sensores, actuadores, dispositivos integrados, dispositivos inalámbricos y dispositivos inteligentes) se conecten a la nube de AWS a través de MQTT, HTTPS y WAN. LoRa
- AWS IoT Device Defender es un servicio de seguridad que le permite auditar las configuraciones de los dispositivos, monitorizar los dispositivos conectados para detectar un comportamiento anómalo y mitigar los riesgos de seguridad.
- Amazon OpenSearch Service es un servicio gestionado que facilita la implementación, el funcionamiento y el escalado de OpenSearch clústeres en la nube de AWS.
- AWS Organizations es un servicio de administración de cuentas que le permite agrupar varias cuentas de AWS en una organización que usted crea y administra de manera centralizada.
- AWS Security Hub le proporciona una vista completa de su postura de seguridad en AWS y le ayuda a verificar su entorno con respecto a los estándares y las prácticas recomendadas del sector de la seguridad.
- Amazon Virtual Private Cloud (Amazon VPC) le permite aprovisionar una sección aislada de forma lógica de la nube de AWS donde puede lanzar recursos de AWS en una red virtual que haya definido. Dicha red virtual es prácticamente idéntica a las redes tradicionales que se utilizan en sus propios centros de datos, con los beneficios que supone utilizar la infraestructura escalable de AWS.

Epics

Configure una cuenta de IoT en su entorno de zona de aterrizaje

Tarea	Descripción	Habilidades requeridas
Valide las barreras de protección de la cuenta de IoT.	Compruebe que las barandill as de CloudTrail AWS Config y Security Hub estén habilitad	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	as en su cuenta de IoT. GuardDuty	
Verifique que su cuenta de IoT esté configurada como cuenta de miembro de su cuenta de seguridad.	Valide que su cuenta de IoT esté configurada y asociada como cuenta de miembro GuardDuty y Security Hub en su cuenta de seguridad. Para obtener más información al respecto, consulte Administrar GuardDuty cuentas con AWS Organizations en la GuardDuty documentación de Amazon y Administrar cuentas de administradores y miembros en la documentación de AWS Security Hub.	Administrador de AWS
Valide el archivado de registros.	Compruebe que CloudTrail los registros de AWS Config y VPC Flow estén almacenados en la cuenta de Log Archive.	Administrador de AWS

Configure la solución de registro centralizado

Tarea	Descripción	Habilidades requeridas
Configure la solución de registro centralizado en su cuenta de seguridad.	Inicie sesión en la consola de administración de AWS de su cuenta de seguridad y configure la solución de registro centralizado de la biblioteca de soluciones de AWS para recopilar,	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	analizar y mostrar CloudWatch los registros en Amazon OpenSearch Service y en los OpenSearch paneles de control. Para obtener más información al respecto, consulte Recopilar, analizar y mostrar Amazon CloudWatch Logs en un único panel con la solución de registro centralizado en la guía de implementación del registro centralizado de la biblioteca de soluciones de AWS.	

Configure y ajuste los recursos de AWS en su cuenta de IoT

Tarea	Descripción	Habilidades requeridas
Configure el registro de AWS IoT.	Inicie sesión en la consola de administración de AWS usando su cuenta de IoT. Configure y configure AWS IoT Core para enviar CloudWatch registros a Logs. Para obtener más información al respecto, consulte Configurar los registros de AWS IoT y monitorizar AWS IoT mediante CloudWatch registros en la documentación de AWS IoT Core.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Configure AWS IoT Device Defender.	Configure AWS IoT Device Defender para auditar sus recursos de IoT y detectar anomalías. Para obtener más información al respecto, consulte Introducción a AWS IoT Device Defender en la documentación de AWS IoT Core.	Administrador de AWS
Configurar CloudTrail.	Configurado CloudTrail para enviar eventos a CloudWatch Logs. Para obtener más información al respecto, consulte Envío de eventos a CloudWatch registros en la CloudTrail documentación de AWS.	Administrador de AWS
Configure AWS Config y las reglas de AWS Config.	Configure AWS Config y las reglas necesarias de AWS Config. Para obtener más información sobre este tema, consulte Configuración de AWS Config con la consola y Configuración de reglas de AWS Config con la consola en la documentación de AWS Config.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Configurar GuardDuty.	Configure y configure GuardDuty para enviar los resultados a Amazon CloudWatch Events con grupos de CloudWatch registros en Logs como destino. Para obtener más informaci ón al respecto, consulta Crear respuestas personalizadas a GuardDuty los hallazgos con Amazon CloudWatch Events en la GuardDuty documenta ción de Amazon.	Administrador de AWS
Configure Security Hub.	Configure Security Hub y active los estándares CIS AWS Foundations Benchmark y AWS Foundational Security Best Practices. Para obtener más informaci ón al respecto, consulte Respuesta y correcció n automatizadas en la documentación de AWS Security Hub.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Configure Amazon Detective.	Configure Detective para facilitar el análisis de los resultados de seguridad Para obtener más información, consulte Setting up Amazon Detective en la documentación de Amazon Detective.	Administrador de AWS
Configure Amazon Athena y AWS Glue.	Configure Athena y AWS Glue para consultar los registros de los servicios de AWS que llevan a cabo investigaciones de incidentes de seguridad. Para obtener más informaci ón al respecto, consulte los Consultas de registros de servicios de AWS en la documentación de Amazon Athena.	Administrador de AWS

Recursos relacionados

- ¿Qué es una zona de aterrizaje?

Extraiga y consulte SiteWise los atributos de metadatos de AWS IoT en un lago de datos

Creado por Ambarish Dongaonkar (AWS)

Entorno: producción	Tecnologías: IoT; Análisis; Macrodatos	Servicios de AWS: AWS IoT SiteWise; AWS Lambda; AWS Glue

Resumen

AWS IoT SiteWise utiliza jerarquías y modelos de activos para representar sus equipos, procesos e instalaciones industriales. Cada modelo o activo puede tener varios atributos específicos de su entorno. Los ejemplos de atributos de los metadatos incluyen el sitio o la ubicación física del activo, los detalles de la planta y los identificadores del equipo. Estos valores de atributos complementan los datos de medición de los activos para maximizar el valor empresarial. El machine learning (ML) puede proporcionar información adicional sobre estos metadatos y agilizar las tareas de ingeniería.

Sin embargo, los atributos de metadatos no se pueden consultar directamente desde el SiteWise servicio AWS IoT. Para que los atributos se puedan consultar, debe extraerlos e incorporarlos a un lago de datos. Este patrón utiliza un script de Python para extraer los atributos de todos los SiteWise activos de AWS IoT e incorporarlos a un lago de datos de un bucket de Amazon Simple Storage Service (Amazon S3). Cuando haya completado este proceso, podrá utilizar consultas SQL en Amazon Athena para acceder a los atributos de SiteWise metadatos de AWS IoT y a otros conjuntos de datos, como los conjuntos de datos de medidas. La información de los atributos de metadatos también es útil cuando se trabaja con SiteWise monitores o paneles de AWS IoT. También puede crear un QuickSight panel de AWS mediante los atributos extraídos en el bucket de S3.

El patrón tiene un código de referencia y puede implementarlo utilizando los mejores servicios de computación para su caso de uso, como AWS Lambda o AWS Glue.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.

- Permisos para configurar funciones de AWS Lambda o trabajos de AWS Glue.
- Un bucket de Amazon S3.
- Los modelos y jerarquías de activos se configuran en AWS IoT SiteWise. Para obtener más información, consulte Creación de modelos de activos (SiteWise documentación de AWS IoT).

Arquitectura

Puede utilizar una función de Lambda o un trabajo de AWS Glue para completar este proceso. Recomendamos usar Lambda si tiene menos de 100 modelos y cada modelo tiene un promedio de 15 atributos o menos. En todos los demás casos de uso, recomendamos utilizar AWS Glue.

En el siguiente diagrama se muestra la arquitectura de la solución y el flujo de trabajo.

1. Se ejecuta el trabajo programado de AWS Glue o la función de Lambda. Extrae los atributos de metadatos de los activos de AWS IoT SiteWise y los ingiere en un bucket de S3.
2. Un rastreador de AWS Glue rastrea los datos extraídos del bucket de S3 y crea tablas en un catálogo de datos de AWS Glue.
3. Con SQL estándar, Amazon Athena consulta las tablas del catálogo de datos de AWS Glue.

Automatizar y escalar

Puede programar la función Lambda o el trabajo de AWS Glue para que se ejecute de forma diaria o semanal, según la frecuencia de actualización de las configuraciones de sus SiteWise activos de AWS IoT.

No hay límite en cuanto a la cantidad de SiteWise activos de AWS IoT que el código de muestra puede procesar, pero una gran cantidad de activos puede aumentar el tiempo necesario para completar el proceso.

Herramientas

- Amazon Athena es un servicio interactivo de consultas que le permite analizar datos directamente en Amazon Simple Storage Service (Amazon S3) usando SQL estándar.
- AWS Glue es un servicio de extracción, transformación y carga (ETL) completamente administrado. Ayuda a categorizar, limpiar, enriquecer y mover datos de forma fiable entre almacenes de datos y flujos de datos.

- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS IoT le SiteWise ayuda a recopilar, modelar, analizar y visualizar datos de equipos industriales a escala.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS SDK para Python (Boto3) es un kit de desarrollo de software que permite integrar su aplicación, biblioteca o script de Python con los servicios de AWS.

Epics

Configurar el trabajo o la función

Tarea	Descripción	Habilidades requeridas
Configurar los permisos en IAM.	En la consola de IAM, conceda permisos a la función de IAM que asume la función de Lambda o el trabajo de AWS Glue para realizar lo siguiente: • Lea información del SiteWise servicio AWS IoT • Escribir en el bucket de S3 Para más información, consulte Crear un rol para un servicio de AWS (document ación de IAM)	AWS general

Tarea	Descripción	Habilidades requeridas
Cree la función de Lambda o el trabajo de AWS Glue.	Si utiliza Lambda, cree una función de Lambda nueva. En Tiempo de ejecución, elija Python. Para más informaci ón, consulte Creación de funciones de Lambda con Python (documentación de Lambda). Si utiliza AWS Glue, cree un nuevo trabajo del intérprete de comandos de Python en la consola de AWS Glue. Para más información, consulte Adición de trabajos de shell de Python (documentación de AWS Glue).	AWS general
Actualice la función de Lambda o el trabajo de AWS Glue.	Modifique la nueva función de Lambda o el trabajo de AWS Glue e introduzca el ejemplo de código en la sección Información adicional . Modifique el código según sea necesario para su caso de uso. Para obtener más información, consulte Editar código mediante el editor de consola (documentación de Lambda) y Trabajar con scripts (documentación de AWS Glue).	AWS general

Ejecutar el trabajo o la función

Tarea	Descripción	Habilidades requeridas
Ejecute la función de Lambda o el trabajo de AWS Glue.	Ejecute la función de Lambda o el trabajo de AWS Glue. Para obtener más informaci ón, consulte Invocar la función de Lambda (document ación de Lambda) o Iniciar trabajos mediante desencade nadores (documentación de AWS Glue). Esto extrae los atributos de metadatos de los activos y modelos de la SiteWise jerarquía de AWS IoT y los almacena en el bucket de S3 especificado.	AWS general
Configure un rastreador de AWS Glue.	Configure un rastreador AWS Glue con el clasificador de formato necesario para un archivo con formato CSV. Utilice los detalles del bucket y el prefijo de S3 utilizados en la función de Lambda o en el trabajo de AWS Glue. Para más información, consulte Definición de rastreadores (documentación de AWS Glue).	AWS general
Ejecute el rastreador de AWS Glue.	Ejecute el rastreador para procesar el archivo de datos creado por la función de Lambda o el trabajo de AWS Glue. El rastreador crea una	AWS general

Tarea	Descripción	Habilidades requeridas
	tabla en el catálogo de datos de AWS Glue especificado. Para obtener más información, consulte Inicio de rastreadores mediante desencadenadores (documentación de AWS Glue).	
Consulte los atributos de los metadatos.	Con Amazon Athena, utilice SQL estándar para consultar el catálogo de datos de AWS Glue según sea necesario para su caso de uso. Puede unir la tabla de atributos de metadatos con otras bases de datos y tablas. Para más información, consulte Introducción (documentación de Amazon Athena).	AWS general

Recursos relacionados

- Documentación de Amazon Athena
- Documentación de AWS Glue
- Referencia de la SiteWise API de AWS IoT
- Guía del SiteWise usuario de AWS IoT
  - Introducción
  - Crear modelos de activos industriales
  - Definición de relaciones entre los modelos de activos (jerarquías)
  - Asociación y disociación de activos
  - Creación de la SiteWise demostración de AWS IoT
- IOT SiteWise (documentación del SDK para Python)

- Documentación de Lambda

Información adicional

Código

El código de ejemplo que se proporciona es de referencia y puede personalizarlo según sea necesario para su caso de uso.

```
# Following code can be used in an AWS Lambda function or in an AWS Glue Python shell
 job.
# IAM roles used for this job need read access to the AWS IoT SiteWise service and
 write access to the S3 bucket.
sw_client = boto3.client('iotsitewise')
s3_client = boto3.client('s3')
output = io.StringIO()

attribute_list=[]
bucket = '{3_bucket name}'
prefix = '{s3_bucket prefix}'
output.write("model_id,model_name,asset_id,asset_name,attribuet_id,attribute_name,attribute_val
\n")

m_resp = sw_client.list_asset_models()
for m_rec in m_resp['assetModelSummaries']:
     model_id = m_rec['id']
     model_name = m_rec['name']

     attribute_list.clear()
     dam_response = sw_client.describe_asset_model(assetModelId=model_id)
     for rec in dam_response['assetModelProperties']:
         if 'attribute' in rec['type']:
            attribute_list.append(rec['name'])

     response = sw_client.list_assets(assetModelId=model_id, filter='ALL')
     for asset in response['assetSummaries']:
         asset_id = asset['id']
         asset_name = asset['name']
         resp = sw_client.describe_asset(assetId=asset_id)
         for rec in resp['assetProperties']:
            if rec['name'] in attribute_list:
```

```
                p_resp = sw_client.get_asset_property_value(assetId=asset_id,
 propertyId=rec['id'])
                if 'propertyValue' in p_resp:
                    if p_resp['propertyValue']['value']:
                        if 'stringValue' in p_resp['propertyValue']['value']:
                             output.write(model_id + "," + model_name + ","
 + asset_id + "," + asset_name + "," + rec['id'] + "," + rec['name'] + "," +
 str(p_resp['propertyValue']['value']['stringValue']) + "\n")

                        if 'doubleValue' in p_resp['propertyValue']['value']:
                             output.write(model_id + "," + model_name + ","
 + asset_id + "," + asset_name + "," + rec['id'] + "," + rec['name'] + "," +
 str(p_resp['propertyValue']['value']['doubleValue']) + "\n")
                        if 'integerValue' in p_resp['propertyValue']['value']:
                             output.write(model_id + "," + model_name + ","
 + asset_id + "," + asset_name + "," + rec['id'] + "," + rec['name'] + "," +
 str(p_resp['propertyValue']['value']['integerValue']) + "\n")
                         if 'booleanValue' in p_resp['propertyValue']['value']:
                             output.write(model_id + "," + model_name + ","
 + asset_id + "," + asset_name + "," + rec['id'] + "," + rec['name'] + "," +
 str(p_resp['propertyValue']['value']['booleanValue']) + "\n")

output.seek(0)
s3_client.put_object(Bucket=bucket, Key= prefix + '/data.csv', Body=output.getvalue())
output.close()
```

Configuración y solución de problemas de AWS IoT Greengrass con dispositivos cliente

Creado por Marouane Sefiani y Akalanka De Silva (AWS)

Entorno: PoC o piloto	Tecnologías: IoT	Servicios de AWS: AWS IoT Greengrass; AWS IoT Core

Resumen

AWS IoT Greengrass es un servicio en la nube y de tiempo de ejecución de periferia de código abierto que lo ayuda a crear, implementar y administrar software de Internet de las Cosas (IoT) en los dispositivos periféricos. Los casos de uso de AWS IoT Greengrass incluyen:

- Hogares inteligentes en los que se utiliza una puerta de enlace de AWS IoT Greengrass como centro de automatización del hogar
- Fábricas inteligentes donde AWS IoT Greengrass puede facilitar la incorporación y el procesamiento local de datos desde el taller

AWS IoT Greengrass puede actuar como un punto de conexión MQTT seguro y autenticado para otros dispositivos periféricos (también conocidos como dispositivos cliente) que, de otro modo, normalmente se conectarían directamente a AWS IoT Core. Esta capacidad resulta útil cuando los dispositivos cliente no tienen acceso directo a la red del punto de conexión de AWS IoT Core.

Puede configurar AWS IoT Greengrass para su uso con dispositivos cliente en los siguientes casos de uso:

- Para que los dispositivos cliente envíen datos a AWS IoT Greengrass
- Para que AWS IoT Greengrass reenvíe datos a AWS IoT Core
- Para aprovechar las características avanzadas del motor de reglas de AWS IoT Core

Estas capacidades requieren la instalación y configuración de los siguientes componentes en el dispositivo AWS IoT Greengrass:

- Intermediario MQTT

- Puente MQTT
- Autenticación del dispositivo cliente
- Detector de IP

Además, los mensajes publicados desde los dispositivos cliente deben estar en formato JSON o en formato Protocol Buffers (protobuf).

Este patrón describe cómo instalar y configurar estos componentes necesarios y proporciona consejos para la solución de problemas y las prácticas recomendadas.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Interfaz de la línea de comandos de AWS (AWS CLI) versión 2
- Dos dispositivos cliente con Python 3.7 o posterior
- Un dispositivo central que ejecute Java Runtime Environment (JRE) versión 8 o posterior y Amazon Corretto 11 u OpenJDK 11

Limitaciones

- Debe elegir una región de AWS en la que esté disponible AWS IoT Core. Para ver la lista actual de regiones de AWS IoT Core, consulte Servicios de AWS por región.
- El dispositivo principal debe tener al menos 172 MB de RAM y 512 MB de espacio en disco.

Arquitectura

El siguiente diagrama muestra la arquitectura de soluciones para este patrón.

La arquitectura incluye:

- Dos dispositivos cliente. Cada dispositivo contiene una clave privada, un certificado de dispositivo y un certificado de la entidad de certificación (CA) raíz. El SDK para dispositivos de AWS IoT, que contiene un cliente MQTT, también está instalado en cada dispositivo cliente.

- Un dispositivo principal que haya implementado AWS IoT Greengrass con los siguientes componentes:
  - Intermediario MQTT
  - Puente MQTT
  - Autenticación del dispositivo cliente
  - Detector de IP

Esta arquitectura admite los siguientes escenarios:

- Los dispositivos cliente pueden usar su cliente MQTT para comunicarse entre sí a través del intermediario MQTT del dispositivo principal.
- Los dispositivos cliente también pueden comunicarse con AWS IoT Core en la nube a través del intermediario MQTT del dispositivo principal y el puente MQTT.
- AWS IoT Core en la nube puede enviar mensajes a los dispositivos cliente a través del cliente de prueba MQTT y el puento MQTT y el intermediario MQTT del dispositivo principal.

Para obtener más información sobre las comunicaciones entre los dispositivos cliente y el dispositivo principal, consulte la sección información adicional.

Herramientas

Servicios de AWS

- AWS IoT Greengrass es un servicio en la nube y de tiempo de ejecución de borde de Internet de las Cosas (IoT) de código abierto que lo ayuda a crear, implementar y administrar aplicaciones de IoT en los dispositivos.
- AWS IoT Core proporciona una comunicación bidireccional segura para que los dispositivos conectados a Internet se conecten a la nube de AWS.
- Los SDK de dispositivos de AWS IoT son un kit de desarrollo de software que contienen bibliotecas de código abierto, guías de desarrolladores con ejemplos y guías de migración para que pueda crear productos o soluciones de IoT innovadores en las plataformas de hardware deseadas.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.

Prácticas recomendadas

- La carga útil de los mensajes de los dispositivos cliente debe estar en formato JSON o Protobuf para aprovechar las características avanzadas del motor de reglas de AWS IoT Core, como la transformación y las acciones condicionales.
- Configure el puente MQTT para permitir la comunicación bidireccional.
- Configure e implemente el componente detector de IP en AWS IoT Greengrass para garantizar que las direcciones IP del dispositivo principal se incluyan en el campo del nombre alternativo del asunto (SAN) del certificado de intermediario de MQTT.

Epics

Configure el dispositivo principal

Tarea	Descripción	Habilidades requeridas
Configurar AWS IoT Greengrass en el dispositivo principal.	Instale el software AWS IoT Greengrass Core siguiendo las instrucciones de la guía para desarrolladores.	AWS IoT Greengrass
Compruebe el estado de la instalación.	Utilice el siguiente comando para comprobar el estado del servicio AWS IoT Greengrass en su dispositivo principal: `sudo systemctl status greengrass.service` El resultado esperado del comando es: `Launched Nucleus successfully`	AWS general

Tarea	Descripción	Habilidades requeridas
Configure una política de IAM y asóciela al rol de servicio de Greengrass.	1. Cree una política de IAM para permitir las comunicaciones hacia y desde el puente MQTT. A continuación se muestra un ejemplo de política: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "iot:*" ], "Resource": "*" }, { "Sid": "GreengrassActions", "Effect": "Allow", "Action": [ "greengrass:*" ], "Resource": "*" } ] }`	AWS general

Tarea	Descripción	Habilidades requeridas
	2. Asocie la política al rol de servicio de Greengrass. Para obtener el rol de servicio, use el comando: `aws greengrassv2 get-service-role-for-account --region <region>` donde `<region>` se refiere a su región de AWS.	
Configure e implemente los componentes necesarios en el dispositivo principal de AWS IoT Greengrass.	Configure e implemente los siguientes componentes: • `greengrass.clientdevices.mqtt.Moquette` (obtener los detalles de configuracion) • `greengrass.clientdevices.mqtt.Bridge` (obtener los detalles de configuración y la siguiente tarea) • `greengrass.clientdevices.Auth` (obtener los detalles de configuración y la tarea luego de la siguiente) • `aws.greengrass.clientdevices.IPDetector` (obtener los detalles de configuracion)	AWS IoT Greengrass

Tarea	Descripción	Habilidades requeridas
Confirme que el puente MQTT permite la comunicación bidireccional.	Para retransmitir mensajes MQTT entre los dispositivos cliente y AWS IoT Core, configure e implemente el componente puente MQTT y especifique los temas que se van a retransmitir. A continuación se muestra un ejemplo: `{ "mqttTopicMapping": { "ClientDevicesToCloud": { "topic": "dt/#", "source": "LocalMqtt", "target": "IotCore" }, "CloudToClientDevices": { "topic": "cmd/#", "source": "IotCore", "target": "LocalMqtt" } } }`	AWS IoT Greengrass

Tarea	Descripción	Habilidades requeridas
Confirme que el componente de autenticación permite a los dispositivos cliente conectarse y publicar temas o suscribirse a ellos.	La siguiente configuración `aws.greengrass.clientdevices.Auth` permite que todos los dispositivos cliente se conecten, publiquen mensajes y se suscriban a todos los temas. `{ "deviceGroups": { "formatVersion": "2021-03-05", "definitions": { "MyPermissiveDeviceGroup": { "selectionRule": "thingName: *", "policyName": "MyPermissivePolicy" } }, "policies": { "MyPermissivePolicy": { "AllowAll": { "statementDescription": "Allow client devices to perform all actions.", "operations": ["*"], "resources": ["*"] } }`	AWS IoT Greengrass

Tarea	Descripción	Habilidades requeridas
	<pre> } } }</pre>	

Configurar los dispositivos cliente

Tarea	Descripción	Habilidades requeridas
Instalar el SDK para dispositivos con AWS IoT.	Instale el SDK para dispositivos con AWS IoT en los dispositivos cliente. Para obtener una lista completa de los idiomas compatibles y los SDK asociados, consulte la documentación de AWS IoT Core. Por ejemplo, el SDK de dispositivos de AWS IoT para Python se encuentra en GitHub. Para instalar este SDK: 1. Confirme que Python 3.7 o posterior esté instalado , tal y como se indica en la página de requisitos previos del GitHub repositorio. 2. Utilice el comando pip para instalar el SDK. Para macOS y Linux: <pre>python3 -m pip install awsiotsdk</pre>	AWS IoT general

Tarea	Descripción	Habilidades requeridas
	Para Windows: `python -m pip install awsiotsdk` Como opción, puede instalar el SDK desde el repositorio de origen: `# Create a workspace directory to hold all the SDK files` `mkdir sdk-workspace` `cd sdk-workspace` `# Clone the repository` `git clone https://github.com/aws/aws-iot-device-sdk-python-v2.git` `# Install using Pip (use 'python' instead of 'python3' on Windows)` `python3 -m pip install ./aws-iot-device-sdk-python-v2`	

Tarea	Descripción	Habilidades requeridas
Crear un objeto.	1. En la consola de AWS IoT, si aparece un botón Get started (Empezar), elíjalo. De lo contrario, en el panel de navegación, seleccione Security Policies (Políticas de seguridad). 2. Si aparece el cuadro de diálogo You don't have any policies yet (Aún no tiene ninguna política), elija Create a policy (Crear una política). De lo contrario, seleccione Create (Crear). 3. Escriba un nombre para la política de AWS IoT (por ejemplo, `ClientDevicePolicy`). 4. En la sección Add statements (Añadir instrucciones), sustituya la política existente por el siguiente código JSON. Sustituya `<region>` y `<account>` por su región de AWS y su número de cuenta AWS. `{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": "iot:Connect",`	AWS IoT Core

Tarea	Descripción	Habilidades requeridas
	"Resource": "arn:aws:iot:region:account:client/*" }, { "Effect": "Allow", "Action": "iot:Publish", "Resource": "*" }, { "Effect": "Allow", "Action": "iot:Receive", "Resource": "*" }, { "Effect": "Allow", "Action": "iot:Subscribe", "Resource": "*" }, { "Effect": "Allow", "Action": ["iot:GetThingShadow", "iot:UpdateThingShadow", "iot:DeleteThingShadow"], "Resource": "arn:aws:iot:region:account:thing/*"	

Tarea	Descripción	Habilidades requeridas
	<pre>}] }</pre> 5. Seleccione Crear. 6. En la consola AWS IoT, en el panel de navegación, seleccione Manage (Administrar), Things (Objetos). 7. Si aparece el cuadro de diálogo You don't have any things yet (Aún no tiene ningún objeto), elija Register a thing (Registrar un objeto). De lo contrario, seleccione Crear. 8. En la página Creating AWS IoT things (Creación de objetos de AWS IoT), elija Create a single thing (Crear un solo objeto). 9. En la página Añadir su dispositivo al registro de dispositivos, escriba un nombre para el objeto de IoT (por ejemplo, `ClientDevice1`) y, a continuación, elija Siguiente . Nota: no puede modificar el nombre de un objeto una vez creado. Para cambiar	

Tarea	Descripción	Habilidades requeridas
	el nombre,, debe crear otro objeto nuevo, asignarle el nuevo nombre y eliminar después el objeto anterior. 10. En la página Add a certificate for your thing (Añadir un certificado para el objeto), elija Create certificate (Crear certificado). 11. Elija los enlaces Descargar para descargar el certificado, la clave privada y el certificado de CA raíz. Importante: esta es su única oportunidad para descargar su certificado y su clave privada. 12. Elija Activate (Activar) para activar su certificado. El certificado debe estar activo para que un dispositivo se conecte a AWS IoT. 13. Elija Attach a policy (Asociar una política). 14. En Añadir una política para lo tuyo ClientDevicePolicy, selecciona Registrar cosa.	

Tarea	Descripción	Habilidades requeridas
Descargue el certificado de CA del dispositivo principal de Greengrass.	Si espera que el dispositivo principal de Greengrass funcione en entornos fuera de línea, debe poner el certificado de CA principal de Greengrass a disposición del dispositivo cliente para que pueda verificar el certificado del intermediario MQTT (emitido por la CA principal de Greengrass). Por lo tanto, es importante obtener una copia de este certificado. Utilice alguna de los siguientes opciones para descargar el certificado de CA: • Si tiene acceso de red al dispositivo AWS IoT Greengrass desde su PC, acceda a `https://<device IP>:8883` en su navegador web y consulte el certificado de intermediario MQTT y el certificado de CA. También puede guardar el certificado de CA en el dispositivo cliente. • Como opción, puede utilizar la línea de comando OpenSSL:	AWS general

Tarea	Descripción	Habilidades requeridas
	`openssl s_client -showcerts -connect <device IP>:8883`	
Copiar las credenciales en los dispositivos cliente.	Copiar el certificado de CA principal de Greengrass, el certificado del dispositivo y la clave privada en los dispositivos cliente.	AWS general

Tarea	Descripción	Habilidades requeridas
Asociar los dispositivos cliente al dispositivo principal.	Asociar los dispositivos cliente a un dispositivo principal para que puedan detectar el dispositivo principal. A continuación, los dispositivos cliente pueden usar la API de descubrimiento de Greengrass para recuperar la información de conectividad y los certificados de sus dispositivos principales asociados. Para obtener más información, consulte Asociación de dispositivos cliente en la documentación de AWS IoT Greengrass. 1. En la consola de AWS IoT Greengrass, elija Core devices (Dispositivos principales). 2. Elija el dispositivo principal que desee administrar. 3. En la página de detalles del dispositivo principal, elija la pestaña Client devices (Dispositivos cliente). 4. En la sección Associated client devices (Dispositivos cliente asociados), seleccione Associate client devices (Asociar dispositivos cliente).	AWS IoT Greengrass

Tarea	Descripción	Habilidades requeridas
	5. En el modal Associate client devices with core device (Asociar dispositivos cliente a dispositivos principal es), haga lo siguiente para cada dispositivo cliente que desee asociar: a. Introduzca el nombre del objeto de AWS IoT que desee asociar como dispositivo cliente. b. Elija Add (Añadir). 6. Elija Associate (Asociar). Los dispositivos cliente que asoció ahora pueden usar la API de detección de Greengrass para detectar este dispositivo principal.	

Envíe y reciba datos

Tarea	Descripción	Habilidades requeridas
Enviar datos de un dispositivo cliente a otro dispositivo cliente.	Utilice el cliente MQTT de su dispositivo para publicar un mensaje sobre el tema `dt/client1/sensor` .	AWS general
Envíe datos desde el dispositivo cliente a AWS IoT Core.	Utilice el cliente MQTT de su dispositivo para publicar un mensaje sobre el tema `dt/client1/sensor` .	AWS general

Tarea	Descripción	Habilidades requeridas
	En el cliente de prueba de MQTT, suscríbase al tema sobre el que el dispositivo está enviando mensajes o suscríbase a # para todos los temas (consulte los detalles).	
Enviar mensajes desde AWS IoT Core a dispositivos cliente.	En la página del cliente de prueba de MQTT, en la pestaña Publish to a topic (Publicar en un tema), en el campo Topic name (Nombre del tema), introduzca el nombre del tema de su mensaje. En este ejemplo, utilice `cmd/client1` para el tema.	AWS general

Solución de problemas

Problema	Solución
No se pudo verificar el error del certificado del servidor	Este error se produce cuando el cliente MQTT no puede verificar el certificado presentado por el intermediario MQTT durante el protocolo de enlace TLS. La razón más común es que el cliente MQTT no tiene el certificado de CA. Siga estos pasos para asegurarse de que el certificado de CA se proporciona al cliente MQTT. 1. Si tiene acceso de red al dispositivo AWS IoT Greengrass desde su PC, acceda a `https://<device IP>:8883` en una ventana de navegador para consulte el

Problema	Solución
	certificado de intermediario MQTT y el certificado de CA. También puede guardar el certificado de CA en el dispositivo cliente. Como opción, puede utilizar la línea de comando OpenSSL: `openssl s_client -showcerts -connect <device IP>:8883` 2. Guardar el contenido de los certificados Moquette CA y Greengrass Core CA en archivos y, a continuación, visualizar el contenido decodificado mediante el comando: `openssl x509 -in <Name of CA>.pem -text` El certificado CA de Moquette debe mostrar el campo SAN, como en este ejemplo: `X509v3 Subject Alternative Name: IP Address:XXX.XXX.XXX.XXX, IP Address:127.0.0.1, DNS:localhost`

Problema	Solución
No se pudo verificar el error del nombre del servidor	Este error se produce cuando el cliente MQTT no puede comprobar que se está conectando al servidor correcto. La razón más común es que la dirección IP del dispositivo Greengrass no aparece en el campo SAN del certificado. Siga las instrucciones de la solución anterior para obtener el certificado de intermediario MQTT y compruebe que el campo SAN contiene la dirección IP del dispositivo AWS IoT Greengrass, tal y como se explica en la sección Información adicional. Si no es así, confirme que el componente del detector de IP está instalado correctamente y reinicie el dispositivo principal.
No se puede verificar el nombre del servidor solo cuando se conecta desde un dispositivo cliente integrado	Mbed TLS, que es una biblioteca TLS popular que se utiliza en los dispositivos integrado s, actualmente solo admite la verificación de nombres DNS en el campo SAN del certificado, como se muestra en el código de la bibliotec a Mbed TLS. Como el dispositivo principal no tiene su propio nombre de dominio y depende de la dirección IP, los clientes de TLS que utilizan Mbed TLS no pasarán la verificación del nombre del servidor durante el protocolo de enlace TLS, lo que provocará un fallo de conexión. Recomendamos que añada la verificación de la dirección IP de SAN a la biblioteca Mbed TLS en la función x509_crt_ check_san.

Recursos relacionados

- Documentación de AWS IoT Greengrass
- Documentación de AWS IoT Core de AWS IoT Core
- Componente intermediario MQTT
- Componente puente MQTT
- Componente de autenticación del dispositivo cliente
- Componente detector de IP
- SDK de dispositivos AWS IoT
- Implementación de dispositivos de clientes locales con AWS IoT Greengrass (entrada del blog de AWS)
- RFC 5280: perfil del certificado de infraestructura de clave pública X.509 de Internet y de la lista de revocación de certificados (CRL)

Información adicional

Esta sección ofrece información adicional sobre las comunicaciones entre los dispositivos cliente y el dispositivo principal.

El intermediario MQTT escucha en el puerto 8883 del dispositivo principal los intentos de conexión con un cliente TLS. En la siguiente ilustración se muestra un ejemplo de un certificado de servidor de intermediario MQTT.

El certificado de ejemplo muestra los siguientes detalles:

- El certificado lo emite la CA principal de AWS IoT Greengrass, que es local y específica del dispositivo principal; es decir, actúa como una CA local.
- El componente de autenticación del cliente rota automáticamente este certificado cada semana, como se muestra en la siguiente ilustración. Puede establecer este intervalo en la configuración del componente de autenticación del cliente.

- El nombre alternativo del asunto (SAN) desempeña un papel fundamental en la verificación del nombre del servidor por parte del cliente TLS. Ayuda al cliente TLS a garantizar que se conecta al servidor correcto y ayuda a evitar man-in-the-middle ataques durante la configuración de la sesión TLS. En el certificado de ejemplo, el campo SAN indica que este servidor escucha en localhost (el conector de dominio Unix local) y que la interfaz de red tiene la dirección IP 192.168.1.12.

El cliente TLS utiliza el campo SAN del certificado para comprobar que se está conectando a un servidor legítimo durante la verificación del servidor. Por el contrario, durante un protocolo de enlace TLS típico entre un servidor HTTP y un navegador, el nombre de dominio del campo del nombre común (CN) o del campo SAN se utiliza para comprobar el dominio al que se está conectando realmente el navegador durante el proceso de verificación del servidor. Si el dispositivo principal no tiene un nombre de dominio, la dirección IP incluida en el campo SAN sirve para el mismo propósito. Para obtener más información, consulte la sección Nombre alternativo del asunto de RFC 5280: perfil del certificado de infraestructura de clave pública X.509 de Internet y de la lista de revocación de certificados (CRL).

El componente detector de IP de AWS IoT Greengrass garantiza que se incluyan las direcciones IP correctas en el campo SAN del certificado.

El certificado del ejemplo lo firma el dispositivo AWS IoT Greengrass que actúa como CA local. El cliente TLS (cliente MQTT) no conoce esta CA, por lo que debemos proporcionar un certificado de CA similar al siguiente.

Más patrones

- Capturar datos de IoT directamente en Amazon S3 de forma rentable con AWS IoT Greengrass

Machine learning e IA

Temas

Agregue datos en Amazon DynamoDB para pronósticos de ML en Athena

Creado por Sachin Doshi (AWS) y Peter Molnar (AWS)

Repositorio de código: utilice predicciones de aprendizaje automático sobre datos de Amazon DynamoDB con Amazon Athena ML	Entorno: producción	Tecnologías: Machine learning e IA; Bases de datos; Sin servidor
Carga de trabajo: código abierto	Servicios de AWS: Amazon Athena; Amazon DynamoDB; AWS Lambda; Amazon; Amazon SageMaker QuickSight	

Resumen

Este patrón muestra cómo compilar agregaciones complejas de datos de Internet de las cosas (IoT) en una tabla de Amazon DynamoDB mediante Amazon Athena. También aprenderá a enriquecer los datos con inferencias de aprendizaje automático (ML) mediante Amazon SageMaker y a consultar datos geoespaciales mediante Athena. Puede usar este patrón como base para crear una solución de pronóstico de ML que satisfaga las necesidades de su organización.

Con fines de demostración, este patrón emplea como ejemplo una empresa que opera un servicio de transporte compartido de patinetes, y quiere predecir la cantidad óptima de patinetes a instalar para los clientes de diferentes barrios urbanos. La empresa usa un modelo de ML previamente entrenado que predice la demanda de los clientes para la próxima hora en función de las últimas cuatro horas. Este escenario emplea un conjunto de datos públicos de la Oficina de Innovación y Tecnología Cívicas del gobierno metropolitano de Louisville. Los recursos para este escenario están disponibles en un repositorio. GitHub

Requisitos previos y limitaciones

- Una cuenta de AWS activa

- Permisos para crear una CloudFormation pila de AWS con las funciones de AWS Identity and Access Management (IAM) para lo siguiente:
  - Bucket de Amazon Simple Storage Service (Amazon S3)
  - Athena
  - DynamoDB
  - SageMaker
  - AWS Lambda

Arquitectura

Pila de tecnología

- Amazon QuickSight
- Amazon S3
- Athena
- DynamoDB
- Lambda
- SageMaker

Arquitectura de destino

El siguiente diagrama muestra una arquitectura para crear agregaciones de datos complejas en DynamoDB mediante las capacidades de consulta de Athena, una función de Lambda, el almacenamiento de Amazon S3, un punto final y un panel de control. SageMaker QuickSight

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Una tabla de DynamoDB incorpora los datos de IoT que se transmiten desde una flota de patinetes.
2. Una función de Lambda carga la tabla de DynamoDB con los datos incorporados.
3. Una consulta de Athena crea una nueva tabla de DynamoDB para datos geoespaciales que representan los barrios urbanos.
4. La ubicación de la consulta se guarda en un bucket de S3.

5. Una función Athena consulta la inferencia de ML desde el SageMaker punto final que aloja el modelo de ML previamente entrenado.
6. Athena consulta los datos directamente de las tablas de DynamoDB y los agrega para su análisis.
7. Un usuario ve el resultado de los datos analizados en un panel de control. QuickSight

Herramientas

Herramientas de AWS

- Amazon Athena es un servicio de consultas interactivo que facilita el análisis de datos en Amazon S3 con SQL estándar.
- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- Amazon SageMaker es un servicio de aprendizaje automático gestionado que le ayuda a crear y entrenar modelos de aprendizaje automático y, a continuación, a implementarlos en un entorno hospedado listo para la producción.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Amazon QuickSight es un servicio de inteligencia empresarial (BI) a escala de nube que le ayuda a visualizar, analizar y elaborar informes sobre sus datos en un único panel de control.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.

Código

El código de este patrón está disponible en el repositorio GitHub Use ML predictions over Amazon DynamoDB data with Amazon Athena ML. Puede utilizar la CloudFormation plantilla del repositorio para crear los siguientes recursos que se utilizan en el escenario de ejemplo:

- Una tabla de DynamoDB
- Una función de Lambda para cargar la tabla con los datos relevantes
- Un SageMaker punto final para las solicitudes de inferencia, con el modelo XGBoost previamente entrenado que se almacena en Amazon S3

- Un grupo de trabajo de Athena llamado `V2EngineWorkGroup`
- Consultas con nombre de Athena para buscar los archivos geoespaciales y predecir la demanda de patinetes
- Un conector de Amazon Athena y DynamoDB prediseñado que permite a Athena comunicarse con DynamoDB y emplea AWS Serverless Application Model (AWS SAM) para compilar la aplicación en referencia al conector de DynamoDB

Epics

Descargue el conjunto de datos de ejemplo

Tarea	Descripción	Habilidades requeridas
Descargue el conjunto de datos y los recursos.	1. Descargue un conjunto de datos públicos sobre el alquiler de vehículos en vía pública. Con fines de demostración, estos datos se rellenan previamente en DynamoDB como parte del caso de uso. En un entorno de producción, los datos se envían a DynamoDB a través de varios mecanismos, como dispositivos de IoT o consumidores de Amazon Kinesis. Estos mecanismos emplean Lambda para insertar datos en DynamoDB. 2. Descargue los archivos shapefile de GIS que representan los límites de los barrios históricos y culturales de la ciudad de Louisville, Kentucky.	Desarrollador de aplicaciones, científico de datos

Tarea	Descripción	Habilidades requeridas
	El conjunto de datos público lo proporciona el Consorcio de Información del condado de Jefferson y Louisville, Kentucky. Los shapefiles originales ya están convertidos en un archivo de texto que puede consultar con Athena, pero puede encontrar el código Python para transformar los shapefiles en el cuaderno de Jupyter en Geo-Spatial Processing of GIS shapefiles con Amazon Athena en. GitHub 3. Descargue el código Python previamente entrenado que entrena el modelo de aprendizaje automático para las previsiones SageMaker horarias mediante Athena. 4. Obtenga la consulta SQL de Athena que contiene todo lo necesario para realizar predicciones en tiempo real a partir de los datos almacenados en DynamoDB. 5. (Opcional) Úselo QuickSight para visualizar datos geoespaciales en un mapa de Louisville, Kentucky.	

Utilice una CloudFormation plantilla para implementar los recursos necesarios

Tarea	Descripción	Habilidades requeridas
Crea una CloudFormation pila.	1. Descarga la CloudFormation plantilla del GitHub repositorio. 2. Inicie sesión en la consola de administración de AWS y seleccione `us-east-1` . Nota: El modelo de ML se almacena en el Amazon Elastic Container Registry (Amazon ECR) de la región de AWS `us-east-1` , pero el patrón es independiente de la región. Puede replicar el patrón en cualquier región compatible con los servicios de AWS usados en este patrón. 3. Abre la CloudFormation consola y, a continuación, selecciona Stacks en el panel de navegación. 4. Elija Create stack (Crear pila) y, a continuación, seleccione With existing resources (import resources) (Con recursos existentes (importar recursos)). 5. En la página Identificar recursos, seleccione Siguiente. 6. En la sección Especificar plantilla, en Origen de la	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	plantilla, seleccione Cargar un archivo de plantilla. 7. Selecciona Archivo y, a continuación, elige la CloudFormation plantilla que descargaste anteriormente. 8. Seleccione Siguiente, acepte los valores de los parámetros predeterminados y seleccione Siguiente para continuar con el asistente de configuración. 9. Seleccione la casilla de verificación Acepto que AWS CloudFormation podría crear recursos de IAM con nombres personalizados. 10. Seleccione Crear pila. Nota: La CloudFormation pila puede tardar entre 15 y 20 minutos en crear estos recursos.	

Tarea	Descripción	Habilidades requeridas
Verifique la CloudFormation implementación.	Para comprobar que los datos de ejemplo de la CloudFormation plantilla se cargan en DynamoDB, haga lo siguiente: 1. Abra la consola de DynamoDB y, a continuación, seleccione Tablas en el panel de navegación. 2. En la sección Tablas, busque la tabla `DynamoDBTableDocklessVehicles` . 3. Una vez finalizada la creación del recurso, abra la consola de Athena y, a continuación, seleccione Grupos de trabajo en el panel de navegación. 4. Seleccione el grupo de trabajo `V2EngineWorkGroup` que quiere utilizar y seleccione Cambiar grupo de trabajo. 5. Si el sistema le solicita que guarde la ubicación de los resultados de la consulta, seleccione una ubicación de Amazon S3 en la que tenga permisos de escritura . 6. Seleccione Guardar. 7. En el panel de navegación, seleccione Query editor	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	(Editor de consultas) y, a continuación, la base de datos `athena-ml-db-<your-AWS-account-number>` .	

Cargue archivos de geolocalización en Athena

Tarea	Descripción	Habilidades requeridas
Cree una tabla de Athena con datos geoespaciales.	Para cargar los archivos de geolocalización en Athena, haga lo siguiente: 1. Abra la consola de Athena y seleccione Editor de consultas en el panel de navegación. 2. Seleccione la pestaña Sample queries (Consultas de muestra). 3. Busque y seleccione Q1: Neighborhoods. 4. Para volver al editor de consultas, seleccione la pestaña Editor. 5. Elija Ejecutar. Se creará una tabla con el nombre `louisville_ky_neighborhoods` en su base de datos. La tabla se crea en la base de datos `athena-ml-db-<your`	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	`-AWS-account-numbe r> .` La consulta crea una nueva tabla para datos geoespaci ales que representan los barrios urbanos. La tabla de datos se crea a partir de archivos shapefile de GIS. La instrucción `CREATE EXTERNAL TABLE` define el esquema de la tabla y la ubicación y el formato del archivo de datos subyacente. Para ver el código de Python usado para procesar los archivos shapefile y producir esta tabla, consulte Procesami ento geoespacial de archivos shapefile de GIS con Amazon Athena en AWS Samples. Para obtener información detallada sobre el código SQL, consulte create_neighborhoo d_table.sql en. GitHub	

Pronostique la demanda de patinetes en función del barrio a partir de los datos agregados de DynamoDB

Tarea	Descripción	Habilidades requeridas
Declare una función en Athena para consultarla. SageMaker	1. Abra la consola de Athena y seleccione Editor de consultas en el panel de navegación, y posterior mente seleccione la pestaña Editor. 2. Copie y pegue la instrucci ón DDL siguiente en el editor de consultas: `USING EXTERNAL FUNCTION predict_demand ( location_id BIGINT, hr BIGINT , dow BIGINT, n_pickup_1 BIGINT, n_pickup_2 BIGINT, n_pickup_3 BIGINT, n_pickup_4 BIGINT, n_dropoff_1 BIGINT, n_dropoff_2 BIGINT, n_dropoff_3 BIGINT, n_dropoff_4 BIGINT ) RETURNS DOUBLE SAGEMAKER '<Your SageMaker endpoint>'` La primera parte de la sentencia SQL declara que la función externa consultará las inferencias de aprendiza je automático desde el SageMaker punto final que	Científico de datos, ingeniero de datos

Tarea	Descripción	Habilidades requeridas
	aloja el modelo previamente entrenado. A continuación, proceda del modo siguiente: 1. Defina el orden y tipo de los parámetros de entrada y el tipo de valores devueltos. 2. Elija Ejecutar.	

Tarea	Descripción	Habilidades requeridas
Pronostique la demanda de patinetes en función del barrio a partir de los datos agregados de DynamoDB.	Ahora puede usar Athena para consultar datos transacci onales directamente desde DynamoDB y, a continuac ión, agregar los datos para su análisis y previsión. Esto no se consigue fácilmente consultan do directamente una base de datos NoSQL de DynamoDB. 1. Abra la consola de Athena y seleccione Editor de consultas en el panel de navegación. 2. Seleccione la pestaña Saved queries (Consultas guardadas). 3. Busque y seleccione Q2: DynamodBathEnaml. ScooterPredict 4. Para volver al editor de consultas, seleccione la pestaña Editor. 5. Elija Ejecutar. La instrucción SQL hace lo siguiente: • Usa una consulta federada de Athena para consultar la tabla de DynamoDB con los datos de viaje sin procesar • Coloca las coordenadas geográficas en los barrios	Desarrollador de aplicaciones, científico de datos

Tarea	Descripción	Habilidades requeridas
	mediante las funciones geoespaciales de Athena • Enriquece los datos con inferencias de aprendizaje automático mediante SageMaker Para obtener información sobre el uso de SQL para agregar datos de DynamoDB SageMaker y datos de inferencia en Athena, consulte athena_long.sql en. GitHub	
Verifique el resultado.	La tabla de resultados incluye el barrio, la longitud y la latitud de su centroide. También incluye la cantidad de vehículos que se prevé para la próxima hora. La consulta produce las predicciones para un momento determinado. Puede realizar predicciones para cualquier otro momento cambiando la expresión `TIMESTAMP '2019-09-07 15:00'` en todas las partes de la instrucción. Si tiene un origen de datos en tiempo real en la tabla de DynamoDB, cambie la marca temporal a `NOW()`.	Desarrollador de aplicaciones, científico de datos

Limpie el entorno

Tarea	Descripción	Habilidades requeridas
Delete resources (Eliminar recursos).	1. Abre la consola de Athena y vacía el cubo que has creado como parte de la CloudFormation pila. 2. Abre la CloudFormation consola y, a continuación, elimina la pila nombradabdb-1462-athena-dynamodb-ml-stack . 3. Abre la CloudWatch consola de Amazon y, a continuación, elimina el grupo de registros denominado/aws/sagemaker/Endpoints/Sg-athena-ml-dynamodb-model-endpoint .	Desarrollador de aplicaciones, AWS DevOps

Recursos relacionados

- SDK de Amazon Athena Query Federation () GitHub
- Consulta de datos geoespaciales (Guía del usuario de Amazon Athena)
- Use pronósticos de ML sobre datos de Amazon DynamoDB con ML de Amazon Athena (AWS Big Data Blog)
- Amazon ElastiCache para Redis (documentación de AWS)
- Amazon Neptune (documentación de AWS)

Asocie un CodeCommit repositorio de AWS en una cuenta de AWS con SageMaker Studio en otra cuenta

Creado por Laurens van der Maas (AWS) y Aubrey Oosthuizen (AWS)

Entorno: producción	Tecnologías: aprendizaje automático e inteligencia artificial; seguridad, identidad y DevOps cumplimiento; nativas de la nube	Servicios de AWS: AWS CodeCommit; Amazon SageMaker; AWS Identity and Access Management

Resumen

Este patrón proporciona instrucciones y código sobre cómo asociar un CodeCommit repositorio de AWS en una cuenta de AWS (cuenta A) con Amazon SageMaker Studio en otra cuenta de AWS (cuenta B). Para configurar la asociación, debe crear una política y un rol de AWS Identity and Access Management (IAM) en la cuenta A y una política integrada de IAM en la cuenta B. A continuación, debe utilizar un script de shell para clonar el CodeCommit repositorio de la cuenta A a SageMaker Studio en la cuenta B.

Requisitos previos y limitaciones

Requisitos previos

- Dos cuentas de AWS, una que contiene el CodeCommit repositorio y la otra que contiene un SageMaker dominio con un usuario
- SageMaker Dominio y usuario aprovisionados, con acceso a Internet o acceso a CodeCommit AWS Security Token Service (AWS STS) a través de puntos de enlace de red privada virtual (VPC)
- Conocimientos básicos de IAM
- Conocimientos básicos de Studio SageMaker
- Conocimientos básicos de Git y CodeCommit

Limitaciones

Este patrón se aplica únicamente a SageMaker Studio, no a RStudio en Amazon SageMaker.

Arquitectura

Pila de tecnología

- Amazon SageMaker
- Amazon SageMaker Studio
- AWS CodeCommit
- AWS Identity y Access Management (IAM)
- Git

Arquitectura de destino

El siguiente diagrama muestra una arquitectura que asocia un CodeCommit repositorio de la cuenta A a SageMaker Studio en la cuenta B.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un usuario asume el `MyCrossAccountRepositoryContributorRole` rol en la cuenta A a través del `sts:AssumeRole` rol, mientras que usa el rol de SageMaker ejecución en SageMaker Studio en la cuenta B. El rol asumido incluye los CodeCommit permisos para clonar e interactuar con el repositorio especificado.
2. El usuario ejecuta los comandos de Git desde el terminal del sistema en SageMaker Studio.

Automatizar y escalar

Este patrón consta de pasos manuales que se pueden automatizar mediante el AWS Cloud Development Kit (AWS CDK) CloudFormation, AWS o Terraform.

Herramientas

Herramientas de AWS

- Amazon SageMaker es un servicio de aprendizaje automático gestionado (ML) que le ayuda a crear y entrenar modelos de aprendizaje automático y, a continuación, a implementarlos en un entorno hospedado listo para la producción.

- Amazon SageMaker Studio es un entorno de desarrollo integrado (IDE) basado en la web para el aprendizaje automático que le permite crear, entrenar, depurar, implementar y supervisar sus modelos de aprendizaje automático.
- AWS CodeCommit es un servicio de control de versiones que le ayuda a almacenar y gestionar repositorios de Git de forma privada, sin necesidad de gestionar su propio sistema de control de código fuente.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.

Otras herramientas

- Git es un sistema de control de versiones distribuido que rastrea los cambios en el código fuente durante el desarrollo del software.

Epics

Cree una política y rol de IAM en la cuenta A

Tarea	Descripción	Habilidades requeridas
Crear una política de IAM de acceso al repositorio en Cuenta A.	1. Inicie sesión en la consola de administración de AWS y abra la consola de IAM. 2. En el panel de navegación, seleccione Políticas y, a continuación, Crear política. 3. Seleccione la pestaña JSON. 4. Copie la instrucción de política del ejemplo de política de IAM incluido en la sección de Información adicional de este patrón y, a continuación, pegue la instrucción en el editor	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	de JSON. Asegúrese de reemplazar todos los valores de los marcadores de posición de la política. 5. Seleccione Next:Tags (Siguiente: etiquetas) y, a continuación, Next:Review (Siguiente: revisar). 6. En Nombre, escriba un nombre para la política. Nota: en este patrón se hace referencia a la política de IAM como `CrossAccountAccessForMySharedDemoRepo` , pero puede elegir el nombre de política que prefiera. 7. Seleccione Crear política. Consejo: se recomienda restringir el alcance de las políticas de IAM a los permisos mínimos requeridos para cada caso de uso.	

Tarea	Descripción	Habilidades requeridas
Crear un rol de IAM para el acceso al repositorio en la Cuenta A.	1. En el panel de navegación de la consola de IAM, seleccione Roles y, a continuación, seleccione Crear rol. 2. En Tipo de entidad de confianza, seleccione Cuenta de AWS. 3. En la sección Cuenta de AWS, seleccione Otra cuenta de AWS. 4. En Account ID (ID de cuenta), escriba el ID de la cuenta B. 5. En la página Agregar permisos, busque y seleccione la política `CrossAccountAccessForMySharedDemoRepo` que creó anteriormente. 6. Seleccione Next (Siguiente). 7. En Role name (Nombre de rol), escriba un nombre. Nota: en este patrón se hace referencia al nombre de IAM como `MyCrossAccountRepositoryContributorRole`, pero puede elegir el nombre de rol que prefiera. 8. Seleccione Crear rol y, a continuación, copie el	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	Nombre de recurso de Amazon (ARN) del nuevo rol.	

Cree una política de IAM en línea en la cuenta B

Tarea	Descripción	Habilidades requeridas
Adjunte una política en línea a la función de ejecución asociada al usuario de su SageMaker dominio en la cuenta B.	1. En el panel de navegación de la consola de IAM, seleccione Roles. 2. Busca y elige la función de ejecución asociada a tu usuario de SageMaker dominio en la cuenta B. 3. Seleccione Agregar permisos y, a continuación, Crear política insertada. 4. Seleccione la pestaña JSON. 5. Copie la siguiente política y péguela en el editor de JSON. `{ "Version": "2012-10-17", "Statement": [ { "Sid": "VisualEditor0", "Effect": "Allow", "Action": "sts:AssumeRole",`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	<pre>"Resource": "arn:aws:iam::<Account_A_ID>:role/<Account_A_Role_Name>" }] }</pre> 6. Sustituya `<Account_A_ID>` por la ID de cuenta de la cuenta A. Sustituya `<Account_A_Role_Name>` por el nombre del rol de IAM que creó anteriormente. 7. Seleccione Revisar política. 8. En Nombre, escriba el nombre de la política insertada. 9. Elija Crear política.	

Clona el repositorio en SageMaker Studio para la cuenta B

Tarea	Descripción	Habilidades requeridas
Cree el script de shell en SageMaker Studio en la cuenta B.	1. En el panel de navegación de la SageMaker consola, selecciona Studio. 2. Seleccione su perfil de usuario y, a continuación, seleccione Open Studio. 3. En la sección Inicio, seleccione Open Launcher.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	4. En la sección Utilidades y archivos, seleccione Archivo de texto. 5. Copie el script de Example SageMaker shell script en la sección de información adicional de este patrón y, a continuación, pegue la sentencia en el nuevo archivo. Asegúrese de reemplazar todos los valores de los marcadores de posición en el script. 6. Haga clic derecho en la pestaña untitled.txt del nuevo archivo y, a continuación, seleccione Renombrar texto. En Nuevo nombre, escriba cross_account_git_clone.sh y, a continuación, seleccione Cambiar nombre.	

Tarea	Descripción	Habilidades requeridas
Invoque el script de intérprete de comandos desde el terminal del sistema.	1. En la sección de inicio de la SageMaker consola, selecciona Open Launcher. 2. En la sección Utilidades y archivos, seleccione Terminal del sistema. 3. En el terminal, ejecute el siguiente comando: `chmod u+x ./cross_account_git_clone.sh && ./cross_account_git_clone.sh` Has clonado tu CodeCommit repositorio en una cuenta cruzada de SageMaker Studio. Ahora puede ejecutar todos los comandos de Git desde el terminal del sistema.	AWS DevOps

Información adicional

Política de IAM de ejemplo

Para utilizar este ejemplo de política, debe hacer lo siguiente:

- Sustituya `<CodeCommit_Repository_Region>` por la región de AWS del repositorio.
- Sustituya `<Account_A_ID>` por la ID de cuenta para la cuenta A.
- `<CodeCommit_Repository_Name>`Sustitúyalo por el nombre de tu CodeCommit repositorio en la cuenta A.

```
{
```

```
"Version": "2012-10-17",
"Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "codecommit:BatchGet*",
            "codecommit:Create*",
            "codecommit:DeleteBranch",
            "codecommit:Get*",
            "codecommit:List*",
            "codecommit:Describe*",
            "codecommit:Put*",
            "codecommit:Post*",
            "codecommit:Merge*",
            "codecommit:Test*",
            "codecommit:Update*",
            "codecommit:GitPull",
            "codecommit:GitPush"
        ],
        "Resource": [

 "arn:aws:codecommit:<CodeCommit_Repository_Region>:<Account_A_ID>:<CodeCommit_Repository_Name>
        ]
    }
]
}
```

Ejemplo de script de SageMaker shell

Para utilizar este ejemplo de script, debe hacer lo siguiente:

- Sustituya <Account_A_ID> por la ID de cuenta para la cuenta A.
- Sustituya <Account_A_Role_Name> por el nombre del rol de IAM que ha creado anteriormente.
- Sustituya <CodeCommit_Repository_Region> por la región de AWS del repositorio.
- <CodeCommit_Repository_Name>Sustitúyalo por el nombre de tu CodeCommit repositorio en la cuenta A.

```
#!/usr/bin/env bash
#Launch from system terminal
pip install --quiet git-remote-codecommit
```

```
mkdir -p ~/.aws
touch ~/.aws/config

echo "[profile CrossAccountAccessProfile]
region = <CodeCommit_Repository_Region>
credential_source=EcsContainer
role_arn = arn:aws:iam::<Account_A_ID>:role/<Account_A_Role_Name>
output = json" > ~/.aws/config

echo '[credential "https://git-
codecommit.<CodeCommit_Repository_Region>.amazonaws.com"]
        helper = !aws codecommit credential-helper $@ --profile
 CrossAccountAccessProfile
        UseHttpPath = true' > ~/.gitconfig

git clone codecommit::<CodeCommit_Repository_Region>://
CrossAccountAccessProfile@<CodeCommit_Repository_Name>
```

Automatice la formación y el despliegue de Amazon Lookout for Vision para la detección de anomalías

Creado por Michael Wallner (AWS), Gabriel Rodríguez García (AWS), Kangkang Wang (AWS), Shukhrat Khodjaev (AWS), Sanjay Ashok (AWS), Yassine Zaafouri (AWS) y Gabriel Zylka (AWS)

automated-silicon-wafer-anomalydetection-using-amazon-lookoutRepositorio de código: - -for-vision	Entorno: producción	Tecnologías: aprendizaje automático e inteligencia artificial; nativas de la nube; DevOps
Servicios de AWS: AWS CloudFormation; AWS CodeBuild; AWS CodeCommit; AWS Lambda CodePipeline; Amazon Lookout for Vision		

Resumen

Este patrón le ayuda a automatizar la formación y el despliegue de los modelos de aprendizaje automático de Amazon Lookout for Vision para la inspección visual. Si bien este patrón se concentra en la detección de anomalías en las obleas de silicio, puede adaptar la solución para utilizarla en una amplia gama de productos e industrias.

En 2020, la capacidad anual de uno de los mayores fabricantes de semiconductores del mundo superó los 12 millones de obleas equivalentes a 12 pulgadas. Para garantizar la calidad y la fiabilidad de estas obleas, la inspección visual es un paso esencial en el proceso de producción. Los métodos tradicionales de inspección visual, como el muestreo manual o el uso de herramientas anticuadas y antiguas que se basan en medidas estadísticas, pueden llevar mucho tiempo y ser ineficientes. Dada la magnitud de este proceso y su importancia para la industria de los semiconductores en general, existe una gran oportunidad de optimizar y automatizar la inspección visual mediante el uso de tecnologías avanzadas de inteligencia artificial (IA).

Lookout for Vision ayuda a agilizar el proceso de inspección de imágenes y objetos, reduciendo la necesidad de realizar inspecciones manuales costosas e inconsistentes. Esta solución mejora el control de calidad, facilita una evaluación precisa de los defectos y daños y garantiza el cumplimiento

de los estándares del sector. Además, puede automatizar el proceso de inspección de Lookout for Vision sin necesidad de conocimientos especializados en aprendizaje automático.

Con esta solución, puede integrar su modelo de visión artificial en cualquier sistema. Por ejemplo, puede integrar un modelo en un sitio web en el que los usuarios suban imágenes y las analicen para detectar defectos. La siguiente imagen muestra un ejemplo de una oblea de silicio con defectos por rayado debidos a un proceso de pulido químico-mecánico (CMP). Puedes usar Lookout for Vision para detectar estas anomalías. Por ejemplo, Lookout for Vision detectó anomalías en esta imagen con un 99,04% de confianza.

Esta solución se basa en el código y el caso de uso descritos en la entrada del blog Cómo crear una solución de seguimiento basada en eventos con Amazon Lookout for Vision. Esta solución modifica el código original para permitir la automatización de las canalizaciones de CI/CD e integrar el SDK de Python de código abierto Amazon Lookout for Vision (). GitHub Para obtener más información sobre el SDK de Python, consulte la entrada del blog sobre cómo crear, entrenar e implementar modelos de Amazon Lookout for Vision mediante el SDK de Python.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Permisos administrativos en la cuenta de AWS
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada
- AWS CDK, instalado y configurado
- Python versión 3.10, instalada

Arquitectura

Arquitectura de destino

Esta arquitectura ilustra la automatización de la creación, el entrenamiento y el despliegue de los modelos de Amazon Lookout for Vision a través de una canalización de CI/CD. En el diagrama, se muestra el siguiente flujo de trabajo:

1. El código se almacena en un CodeCommit repositorio de Amazon. Los desarrolladores pueden modificar el código, cambiar las imágenes de entrada o añadir otros pasos al proceso de automatización.
2. Tras implementar la solución o actualizar la rama principal del CodeCommit repositorio, Amazon CodePipeline envía automáticamente el código a Amazon CodeBuild.
3. CodeBuild usa el SDK de Python de Lookout for Vision para entrenar e implementar el modelo de clasificación de imágenes. Las imágenes utilizadas para el entrenamiento se almacenan en un bucket de Amazon Simple Storage Service (Amazon S3). CodeBuild descarga automáticamente estas imágenes y las almacena. Para personalizar la solución según sus necesidades, puede importar sus propias imágenes.
4. El modelo Lookout for Vision se expone a los usuarios finales a través de AWS Lambda. Sin embargo, no está limitado a este enfoque. También puede implementar Lookout for Vision de forma remota en dispositivos IoT, o puede ejecutarlo como un proceso por lotes de forma programada para generar predicciones.

Herramientas

Servicios de AWS

- AWS CodeBuild es un servicio de compilación totalmente gestionado que le ayuda a compilar código fuente, ejecutar pruebas unitarias y producir artefactos listos para su implementación.
- AWS CodeCommit es un servicio de control de versiones que le ayuda a almacenar y gestionar repositorios de Git de forma privada, sin necesidad de gestionar su propio sistema de control de código fuente.
- AWS le CodePipeline ayuda a modelar y configurar rápidamente las diferentes etapas de una versión de software y a automatizar los pasos necesarios para publicar cambios de software de forma continua.
- AWS Key Management Service (AWS KMS) facilita poder crear y controlar claves criptográficas para proteger los datos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Lookout for Vision utiliza la visión artificial para encontrar detectores visuales en productos industriales, de forma precisa y a escala.

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Repositorio de código

El código de este patrón está disponible en el repositorio de formación e implementación de GitHub Automate Amazon Lookout for Vision para Silicon Wafer Anomaly Detection.

Prácticas recomendadas

Cuando ejecutes el código como un experimento, asegúrate de detener tu terminal Amazon Lookout for Vision.

Epics

Implementar la solución

Tarea	Descripción	Habilidades requeridas
Clona el GitHub repositorio.	Clona el GitHub repositorio de formación e implementación de Amazon Lookout for Vision para Silicon Wafer Anomaly Detection en tu estación de trabajo local. `git clone https://github.com/aws-samples/automated-silicon-wafer-anomaly-detection-using-amazon-lookout-for-vision.git`	Bash
Cree un entorno virtual.	Introduzca el siguiente comando para crear un entorno virtual en su estación de trabajo local.	Python

Tarea	Descripción	Habilidades requeridas
	`python3 -m venv .venv`	
Instale las dependencias.	Una vez creado el entorno virtual, introduzca el siguiente comando para instalar las dependencias necesarias. `pip install -r requirements.txt`	Python
(Solo para usuarios de Linux) Active el entorno virtual.	Una vez completada la inicialización y creado el entorno virtual, utilice el siguiente comando para activar el entorno virtual. `source .venv/bin/activate`	Bash
(Solo para usuarios de Windows) Active el entorno virtual.	Una vez completada la inicialización y creado el entorno virtual, utilice el siguiente comando para activar el entorno virtual. `.venv\Scripts\activate.bat`	PowerShell

Tarea	Descripción	Habilidades requeridas
Implemente la pila.	1. En la CLI de AWS CDK, introduzca el siguiente comando para sintetizar la plantilla de AWS CloudFormation . `cdk synth` 2. Introduzca el siguiente comando para implementar la CloudFormation pila. `cdk deploy --all --require-approval never` `--all flag`Esto garantiza que todos los componentes estén instalados a la vez. `--require-approval` nunca elimina la necesidad de aprobar el despliegue de cada componente.	Administrador de AWS

Pruebe la solución

Tarea	Descripción	Habilidades requeridas
Introduzca un ejemplo de evento de prueba.	1. Abra la página de Funciones en la consola de Lambda. 2. Elija la `amazon-lookout-for-vision-`	AWS general

Tarea	Descripción	Habilidades requeridas
	`project-lambda` función. 3. Elija la pestaña Prueba. 4. En Evento de prueba, selecciona Crear nuevo evento. 5. Introduce lo siguiente. 6. Seleccione Probar. `{ "tbd": "tbd" }` 7. En Execution result (Resultado de ejecución), expanda Details (Detalles) para ver los resultados.	

Recursos relacionados

Documentación de AWS

- Primeros pasos con Amazon Lookout for Vision
- Introducción a AWS CDK

Publicaciones del blog de AWS

- Cree, entrene e implemente modelos de Amazon Lookout for Vision con el SDK de Python
- Cree una solución de seguimiento basada en eventos con Amazon Lookout for Vision
- Amazon Lookout for Vision Python SDK: validación cruzada e integración con otros servicios de AWS

Extraer contenido de archivos PDF automáticamente con Amazon Textract

Creado por Tianxia Jia (AWS)

Entorno: producción	Tecnologías: machine learning e IA; análisis; macrodatos	Servicios de AWS: Amazon S3; Amazon Textract; Amazon SageMaker

Resumen

Muchas organizaciones necesitan extraer información de los archivos PDF que se cargan en sus aplicaciones empresariales. Por ejemplo, una organización podría necesitar extraer con precisión la información de archivos PDF fiscales o médicos para realizar análisis tributarios o procesar reclamaciones médicas.

En la nube de Amazon Web Services (AWS), Amazon Textract extrae automáticamente la información (por ejemplo, texto impreso, formularios y tablas) de los archivos PDF y produce un archivo en formato JSON que contiene información del archivo PDF original. Puede usar Amazon Textract en la consola de administración de AWS o mediante la implementación de llamadas a la API. Le recomendamos que utilice llamadas a la API mediante programación para escalar y procesar automáticamente grandes cantidades de archivos PDF.

Cuando Amazon Textract procesa un archivo, crea la siguiente lista de objetos `Block`: páginas, líneas y palabras de texto, formularios (pares clave-valor), tablas y celdas, y elementos de selección. También se incluye otra información de objetos, por ejemplo, cuadros delimitadores, intervalos de confianza, ID y relaciones. Amazon Textract extrae la información del contenido en forma de cadenas. Es necesario contar con valores de datos correctamente identificados y transformados para que las aplicaciones posteriores puedan utilizarlos más fácilmente.

Este patrón describe un step-by-step flujo de trabajo para usar Amazon Textract para extraer automáticamente el contenido de los archivos PDF y procesarlo para obtener un resultado limpio. El patrón utiliza una técnica de coincidencia de plantillas para identificar correctamente el campo, el nombre clave y las tablas requeridos y, a continuación, aplica correcciones posteriores al procesamiento a cada tipo de datos. Puede utilizar este patrón para procesar distintos tipos de

archivos PDF y, a continuación, escalar y automatizar este flujo de trabajo para procesar archivos PDF con un formato idéntico.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Un bucket de Amazon Simple Storage Service (Amazon S3) existente en el que almacenar los archivos PDF una vez convertidos a formato JPEG para su procesamiento por Amazon Textract. Para obtener más información sobre los buckets de S3, consulte la Información general de los buckets en la documentación de Amazon S3.
- El cuaderno de Jupyter `Textract_PostProcessing.ipynb` (adjunto), instalado y configurado. Para obtener más información sobre las libretas Jupyter, consulta Crear una libreta Jupyter en la documentación de Amazon. SageMaker
- Archivos PDF existentes que tengan un formato idéntico.
- Conocimientos de Python.

Limitaciones

- Sus archivos PDF deben ser de buena calidad y claramente legibles. Se recomiendan archivos PDF nativos, pero puede utilizar documentos escaneados y convertidos a formato PDF si todas las palabras individuales se leen con claridad. Para obtener más información al respecto, consulte Preprocesamiento de documentos PDF con Amazon Textract: detección y eliminación de imágenes en el blog de AWS Machine Learning.
- Con los archivos de varias páginas, puede utilizar una operación asíncrona o combinar los archivos PDF en una única página y utilizar una operación síncrona. Para obtener más información sobre estas dos opciones, consulte Detección y análisis de texto en documentos de varias páginas y Detección y análisis de texto en documentos de una sola página en la documentación de Amazon Textract.

Arquitectura

El flujo de trabajo de este patrón ejecuta primero Amazon Textract sobre un archivo PDF de muestra (Primera ejecución) y, a continuación, lo ejecuta en archivos PDF que tengan un formato idéntico al del primer PDF (Ejecución repetida). El siguiente diagrama muestra el flujo de trabajo combinado de

la Primera ejecución y la Ejecución repetida que extrae de forma automática y repetida el contenido de archivos PDF con idénticos formatos.

El diagrama muestra el siguiente flujo de trabajo de este patrón:

1. Convierta un archivo PDF a formato JPEG y almacénelo en un bucket de S3.
2. Llame a la API de Amazon Textract y analice el archivo JSON de respuesta de Amazon Textract.
3. Edite el archivo JSON añadiendo el par `KeyName:DataType` correcto para cada campo obligatorio. Cree un archivo `TemplateJSON` para la etapa de Ejecución repetida.
4. Defina las funciones de corrección posterior al procesamiento para cada tipo de datos (por ejemplo, flotante, entero y fecha).
5. Prepare los archivos PDF que tengan un formato idéntico al del primer archivo PDF.
6. Llame a la API de Amazon Textract y analice el JSON de respuesta de Amazon Textract.
7. Haga coincidir el archivo JSON analizado con el archivo `TemplateJSON`.
8. Implemente las correcciones posteriores al procesamiento.

El archivo de salida JSON final tiene el `KeyName` y el `Value` correctos para cada campo obligatorio.

Pila de tecnología de destino

- Amazon SageMaker
- Amazon S3
- Amazon Textract

Automatizar y escalar

Puede automatizar el flujo de trabajo de Ejecución repetida mediante una función de AWS Lambda que inicie Amazon Textract cuando se agregue un nuevo archivo PDF a Amazon S3. A continuación, Amazon Textract ejecuta los scripts de procesamiento y el resultado final se puede guardar en una ubicación de almacenamiento. Para obtener más información al respecto, consulte Uso de un desencadenador de Amazon S3 para invocar una función de Lambda en la documentación de Lambda.

Herramientas

- Amazon SageMaker es un servicio de aprendizaje automático totalmente gestionado que le ayuda a crear y entrenar modelos de aprendizaje automático de forma rápida y sencilla y, a continuación, a implementarlos directamente en un entorno hospedado listo para la producción.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Amazon Textract facilita la adición de detección y análisis de texto de documentos a sus aplicaciones.

Epics

Primera ejecución

Tarea	Descripción	Habilidades requeridas
Convertir el archivo PDF.	Para preparar el archivo PDF para la primera ejecución , combínelo en una única página y conviértalo a formato JPEG para la operación síncrona (`Syn API`) de Amazon Textract. Nota: también puede utilizar la operación asíncrona (`Asyn API`) de Amazon Textract para archivos PDF de varias páginas.	Científico de datos, desarroll ador
Analizar el JSON de respuesta de Amazon Textract.	Abra el cuaderno de Jupyter `Textract_PostProce ssing.ipynb` (adjunto) y llame a la API de Amazon Textract mediante el siguiente código:	Científico de datos, desarroll ador

Tarea	Descripción	Habilidades requeridas
	`response = textract.analyze_document( Document={ 'S3Object': { 'Bucket': BUCKET, 'Name': '{}'.format(filename) } }, FeatureTypes=["TABLES", "FORMS"])` Analice y transforme el JSON de respuesta en un formulario y una tabla mediante el siguiente código: `parseformKV=form_kv_from_JSON(response) parseformTables=get_tables_fromJSON(response)`	

Tarea	Descripción	Habilidades requeridas
Editar el archivo de TemplateJSON.	Edite el JSON analizado de cada `KeyName` y el `DataType` correspondiente (por ejemplo, cadena, flotante, entero o fecha) y las cabeceras de las tablas (por ejemplo, `ColumnNames` y `RowNames`). Esta plantilla se usa para cada tipo de archivo PDF individual, lo que significa que la plantilla se puede reutilizar para archivos PDF que tengan un formato idéntico.	Científico de datos, desarrollador
Definir las funciones de corrección posterior al procesamiento.	Los valores de la respuesta de Amazon Textract para el archivo `TemplateJSON` son cadenas. No hay diferenciación por fecha, flotante, entero o divisa. Estos valores se deben convertir al tipo de datos correcto para su caso de uso posterior. Corrija cada tipo de datos según el archivo `TemplateJSON` mediante el siguiente código: `finalJSON=postprocessingCorrection(parsedJSON,templateJSON)`	Científico de datos, desarrollador

Ejecución repetida

Tarea	Descripción	Habilidades requeridas
Preparar los archivos PDF.	Para preparar los archivos PDF, combínelos en una sola página y conviértalos a formato JPEG para la operación síncrona (`Syn API`) de Amazon Textract. Nota: también puede utilizar la operación asíncrona (`Asyn API`) de Amazon Textract para archivos PDF de varias páginas.	Científico de datos, desarrollador
Llamar a la API de Amazon Textract.	Para llamar a la API de Amazon Textract, utilice el siguiente código: `response = textract.analyze_document( Document={ 'S3Object': { 'Bucket': BUCKET, 'Name': '{}'.format(filename) } }, FeatureTypes=["TABLES", "FORMS"])`	Científico de datos, desarrollador
Analizar el JSON de respuesta de Amazon Textract.	Analice y transforme el JSON de respuesta en un formulario y una tabla mediante el siguiente código:	Científico de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
	`parseformKV=form_kv_from_JSON(response)` `parseformTables=get_tables_fromJSON(response)`	
Cargar el archivo TemplateJSON y hacerlo coincidir con el JSON analizado.	Utilice el archivo `TemplateJSON` para extraer los pares clave-valor y la tabla correctos mediante los siguientes comandos: `form_kv_corrected=form_kv_correction(parseformKV,templateJSON)` `form_table_corrected=form_Table_correction(parseformTables, templateJSON)` `form_kv_table_corrected_final={**form_kv_corrected , **form_table_corrected}`	Científico de datos, desarrollador
Correcciones posteriores al procesamiento.	Use `DataType` en el archivo `TemplateJSON` y funciones de procesamiento posterior para corregir los datos mediante el siguiente código: `finalJSON=postprocessingCorrection(form_kv_table_corrected_final,templateJSON)`	Científico de datos, desarrollador

Recursos relacionados

- Extracción automática de texto y datos estructurados de documentos con Amazon Textract
- Extracción de texto y datos estructurados con Amazon Textract
- Recursos de Amazon Textract

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Cree un flujo de trabajo de MLOps mediante Amazon SageMaker y Azure DevOps

Creado por Deepika Kumar (AWS) y Sara van de Moosdijk (AWS)

Entorno: producción	Tecnologías: aprendizaje automático e inteligencia artificial; operaciones DevOps	Carga de trabajo: Microsoft
Servicios de AWS: Amazon API Gateway; Amazon ECR; Amazon EventBridge; AWS Lambda; Amazon SageMaker		

Resumen

Las operaciones de aprendizaje automático (MLOP) son un conjunto de prácticas que automatizan y simplifican los flujos de trabajo y las implementaciones del aprendizaje automático (ML). MLOps se centra en automatizar el ciclo de vida del aprendizaje automático. Ayuda a garantizar que los modelos no solo se desarrollen, sino que también se implementen, monitoreen y reentrenen de manera sistemática y repetida. Aporta DevOps principios al aprendizaje automático. El MLOps se traduce en una implementación más rápida de los modelos de aprendizaje automático, una mayor precisión a lo largo del tiempo y una mayor seguridad de que proporcionan un valor empresarial real.

Las organizaciones suelen contar con DevOps herramientas y soluciones de almacenamiento de datos existentes antes de iniciar su viaje a la MLOP. Este patrón muestra cómo aprovechar los puntos fuertes de Microsoft Azure y AWS. Le ayuda a integrar Azure DevOps con Amazon SageMaker para crear un flujo de trabajo de MLOps.

La solución simplifica el trabajo entre Azure y AWS. Puede usar Azure para el desarrollo y AWS para el aprendizaje automático. Promueve un proceso eficaz para crear modelos de aprendizaje automático de principio a fin, que incluye la gestión de datos, la formación y la implementación en AWS. Para aumentar la eficiencia, debe administrar estos procesos a través de Azure DevOps Pipelines.

Requisitos previos y limitaciones

Requisitos previos

- Suscripción a Azure: acceso a los servicios de Azure, como Azure DevOps, para configurar las canalizaciones de integración e implementación continuas (CI/CD).
- Cuenta de AWS activa: permisos para usar los servicios de AWS utilizados en este patrón.
- Datos: acceso a datos históricos para entrenar el modelo de aprendizaje automático.
- Familiaridad con los conceptos de aprendizaje automático: comprensión de Python, Jupyter Notebooks y desarrollo de modelos de aprendizaje automático.
- Configuración de seguridad: configuración adecuada de las funciones, políticas y permisos en Azure y AWS para garantizar la transferencia y el acceso seguros a los datos.

Limitaciones

- Esta guía no proporciona orientación sobre la transferencia segura de datos entre nubes. Para obtener más información sobre las transferencias de datos entre nubes, consulte Soluciones de AWS para nubes híbridas y multicloud.
- Las soluciones multinube pueden aumentar la latencia para el procesamiento de datos en tiempo real y la inferencia de modelos.
- Esta guía proporciona un ejemplo de una arquitectura MLOps de múltiples cuentas. Los ajustes son necesarios en función de su estrategia de aprendizaje automático y de AWS.

Arquitectura

Arquitectura de destino

La arquitectura de destino integra Azure DevOps con Amazon SageMaker, lo que crea un flujo de trabajo de aprendizaje automático entre nubes. Utiliza Azure para los procesos de CI/CD y para el entrenamiento e implementación SageMaker de modelos de aprendizaje automático. Describe el proceso de obtención de datos (de fuentes como Amazon S3, Snowflake y Azure Data Lake) mediante la creación y la implementación de modelos. Los componentes clave incluyen las canalizaciones de CI/CD para la creación y el despliegue de modelos, la preparación de datos y la gestión de infraestructuras, y Amazon SageMaker para la formación, la evaluación y el despliegue de modelos de aprendizaje automático. Esta arquitectura está diseñada para proporcionar flujos de

trabajo de aprendizaje automático eficientes, automatizados y escalables en todas las plataformas en la nube.

La arquitectura consta de los siguientes componentes:

1. Los científicos de datos realizan experimentos de aprendizaje automático en la cuenta de desarrollo para explorar diferentes enfoques para los casos de uso del aprendizaje automático mediante el uso de diversas fuentes de datos. Los científicos de datos realizan pruebas y ensayos unitarios. Tras la evaluación del modelo, los científicos de datos insertan y combinan el código en el repositorio Model Build, que está alojado en Azure DevOps. Este repositorio contiene código para un proceso de creación de modelos de varios pasos.
2. En Azure DevOps, el Model Build Pipeline, que proporciona integración continua (CI), se puede activar automática o manualmente al fusionar el código con la rama principal. En la cuenta de automatización, esto activa la SageMaker canalización para el preprocesamiento de los datos, el entrenamiento y la evaluación de los modelos y el registro condicional de los modelos en función de la precisión.
3. La cuenta de automatización es una cuenta central en todas las plataformas de aprendizaje automático que aloja entornos de aprendizaje automático (Amazon ECR), modelos (Amazon S3), metadatos de SageMaker modelos (Model Registry), funciones (SageMaker Feature Store), canalizaciones automatizadas (SageMaker Pipelines) e información de registros de aprendizaje automático (CloudWatch y OpenSearch servicio). Esta cuenta permite la reutilización de los activos de aprendizaje automático y aplica las mejores prácticas para acelerar la entrega de casos de uso de aprendizaje automático.
4. La última versión del modelo se agrega al Registro de SageMaker modelos para su revisión. Realiza un seguimiento de las versiones de los modelos y los artefactos respectivos (linaje y metadatos). También administra el estado del modelo (aprobado, rechazado o pendiente) y administra la versión para su implementación posterior.
5. Una vez que se apruebe un modelo entrenado en Model Registry mediante la interfaz del estudio o una llamada a la API, se puede enviar un evento a Amazon EventBridge. EventBridge inicia la canalización de Model Deploy en Azure DevOps.
6. La canalización de Model Deploy, que proporciona una implementación continua (CD), extrae la fuente del repositorio de Model Deploy. La fuente contiene el código, la configuración para la implementación del modelo y los scripts de prueba para establecer puntos de referencia de calidad. La canalización de Model Deploy se puede adaptar a su tipo de inferencia.

7. Tras las comprobaciones de control de calidad, la canalización de Model Deploy implementa el modelo en la cuenta de Staging. La cuenta de ensayo es una copia de la cuenta de producción y se utiliza para las pruebas y la evaluación de la integración. En el caso de una transformación por lotes, la canalización de Model Deploy puede actualizar automáticamente el proceso de inferencia por lotes para utilizar la última versión del modelo aprobada. Para realizar una inferencia asíncrona, sin servidor o en tiempo real, configura o actualiza el punto final del modelo correspondiente.
8. Tras realizar correctamente las pruebas en la cuenta de Staging, se puede implementar un modelo en la cuenta de producción mediante una aprobación manual a través del proceso de implementación de modelos. Esta canalización proporciona un punto final de producción en la etapa de implementación y puesta en producción, que incluye la supervisión del modelo y un mecanismo de retroalimentación de datos.
9. Una vez que el modelo esté en producción, utilice herramientas como SageMaker Model Monitor y SageMaker Clarify para identificar los sesgos, detectar desviaciones y supervisar continuamente el rendimiento del modelo.

Automatizar y escalar

Utilice la infraestructura como código (IaC) para implementarla automáticamente en múltiples cuentas y entornos. Al automatizar el proceso de configuración de un flujo de trabajo de MLOps, es posible separar los entornos que utilizan los equipos de aprendizaje automático que trabajan en diferentes proyectos. AWS le CloudFormation ayuda a modelar, aprovisionar y administrar los recursos de AWS al tratar la infraestructura como código.

Herramientas

Servicios de AWS

- Amazon SageMaker es un servicio de aprendizaje automático gestionado que le ayuda a crear y entrenar modelos de aprendizaje automático y, a continuación, a implementarlos en un entorno hospedado listo para la producción.
- AWS Glue es un servicio de extracción, transformación y carga (ETL) completamente administrado. Ayuda a clasificar, limpiar, enriquecer y mover datos de forma fiable entre almacenes de datos y flujos de datos.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos. En

este patrón, Amazon S3 se utiliza para el almacenamiento de datos y se integra SageMaker para el entrenamiento de modelos y los objetos de modelo.

- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice. En este patrón, Lamdba se utiliza para tareas de preprocesamiento y posprocesamiento de datos.
- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable. En este patrón, almacena los contenedores Docker que se SageMaker utilizan como entornos de formación e implementación.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Siguiendo este patrón, EventBridge organiza flujos de trabajo basados en eventos o basados en el tiempo que inician el reentrenamiento o la implementación automáticos del modelo.
- Amazon API Gateway le ayuda a crear, publicar, mantener, supervisar y proteger REST, HTTP y WebSocket API a cualquier escala. En este patrón, se utiliza para crear un punto de entrada único orientado al exterior para los puntos de enlace de Amazon SageMaker .

Otras herramientas

- Azure le DevOps ayuda a administrar las canalizaciones de CI/CD y a facilitar la creación, las pruebas y la implementación del código.
- Azure Data Lake Storage o Snowflake son posibles fuentes de datos de entrenamiento de terceros para los modelos de aprendizaje automático.

Prácticas recomendadas

Antes de implementar cualquier componente de este flujo de trabajo de MLOps multinube, lleve a cabo las siguientes actividades:

- Defina y comprenda el flujo de trabajo del aprendizaje automático y las herramientas necesarias para respaldarlo. Los diferentes casos de uso requieren flujos de trabajo y componentes diferentes. Por ejemplo, es posible que se requiera un feature store para la reutilización de funciones y la inferencia de baja latencia en un caso de uso de personalización, pero puede que no sea necesario para otros casos de uso. Para personalizar correctamente la arquitectura, es

necesario comprender el flujo de trabajo objetivo, los requisitos de los casos de uso y los métodos de colaboración preferidos del equipo de ciencia de datos.

- Establezca una separación clara de responsabilidades para cada componente de la arquitectura. La distribución del almacenamiento de datos entre Azure Data Lake Storage, Snowflake y Amazon S3 puede aumentar la complejidad y los costes. Si es posible, elija un mecanismo de almacenamiento coherente. Del mismo modo, evite usar una combinación de DevOps servicios de Azure y AWS, o una combinación de servicios de aprendizaje automático de Azure y AWS.
- Elija uno o más modelos y conjuntos de datos existentes para realizar las end-to-end pruebas del flujo de trabajo de MLOps. Los artefactos de prueba deben reflejar los casos de uso reales que los equipos de ciencia de datos desarrollen cuando la plataforma entre en producción.

Epics

Diseñe su arquitectura MLOps

Tarea	Descripción	Habilidades requeridas
Identifique las fuentes de datos.	En función de los casos de uso actuales y futuros, las fuentes de datos disponibl es y los tipos de datos (como los datos confidenciales), documente las fuentes de datos que deben integrarse con la plataforma mLOps. Los datos se pueden almacenar en Amazon S3, Azure Data Lake Storage, Snowflake u otras fuentes. Cree un plan para integrar estas fuentes con su plataforma y garantiza r el acceso a los recursos correctos.	Ingeniero de datos, científico de datos, arquitecto de nube
Elija los servicios aplicables.	Personalice la arquitect ura añadiendo o quitando	Administrador de AWS, ingeniero de datos, científic

Tarea	Descripción	Habilidades requeridas
	servicios en función del flujo de trabajo deseado por el equipo de ciencia de datos, las fuentes de datos aplicables y la arquitectura de nube existente. Por ejemplo, los ingenieros de datos y los científicos de datos pueden realizar el preprocesamiento de datos y la ingeniería de características en SageMaker AWS Glue o Amazon EMR. Es poco probable que se necesiten los tres servicios.	o de datos, ingeniero de aprendizaje automático
Analice los requisitos de seguridad.	Recopile y documente los requisitos de seguridad. Esto incluye determinar: • Qué equipos o ingenieros pueden acceder a fuentes de datos específicas • Si los equipos pueden acceder al código y a los modelos de otros equipos • ¿Qué permisos (si los hay) deben tener los miembros del equipo para las cuentas que no son de desarrollo • ¿Qué medidas de seguridad deben implementarse para la transferencia de datos entre nubes	Administrador de AWS, arquitecto de la nube

Configuración de AWS Organizations

Tarea	Descripción	Habilidades requeridas
Configure AWS Organizations.	Configure AWS Organizations en la cuenta raíz de AWS. Esto le ayuda a administr ar las cuentas subsiguie ntes que cree como parte de una estrategia de MLOps multicuenta. Para obtener más información, consulte la documentación de AWS Organizations.	Administrador de AWS

Configure el entorno de desarrollo y el control de versiones

Tarea	Descripción	Habilidades requeridas
Cree una cuenta de desarrollo de AWS.	Cree una cuenta de AWS en la que los ingenieros y científicos de datos tengan permisos para experimentar y crear modelos de aprendiza je automático. Para obtener instrucciones, consulte Crear una cuenta de miembro en su organización en la documenta ción de AWS Organizations.	Administrador de AWS
Creación de un repositorio de `Model Build`.	Cree un repositorio de Git en Azure donde los científicos de datos puedan enviar el código de creación e implement ación de sus modelos una vez finalizada la fase de	DevOps ingeniero, ingeniero de aprendizaje automático

Tarea	Descripción	Habilidades requeridas
	experimentación. Para obtener instrucciones, consulte Configurar un repositorio de Git en la DevOps documentación de Azure.	
Creación de un repositorio de `Model Deploy`.	Cree un repositorio de Git en Azure que almacene el código y las plantillas de implementación estándar. Debe incluir código para cada opción de implementación que utilice la organización, tal como se identificó en la fase de diseño. Por ejemplo, debe incluir puntos finales en tiempo real, puntos finales asíncronos, inferencias sin servidor o transformaciones por lotes. Para obtener instrucciones, consulte Configurar un repositorio de Git en la DevOps documentación de Azure.	DevOps ingeniero, ingeniero de aprendizaje automático

Tarea	Descripción	Habilidades requeridas
Cree un repositorio de Amazon ECR.	Configure un repositorio de Amazon ECR que almacene los entornos de aprendiza je automático aprobados como imágenes de Docker. Permita que los científicos de datos y los ingenieros de aprendizaje automátic o definan nuevos entornos. Para obtener instrucciones, consulte Creación de un repositorio privado en la documentación de Amazon ECR.	Ingeniero de ML
Configure SageMaker Studio.	Configura SageMaker Studio en la cuenta de desarrollo de acuerdo con los requisito s de seguridad previamente definidos y las herramientas de ciencia de datos preferidas, como el entorno de desarroll o integrado (IDE) que elijas. Usa las configuraciones del ciclo de vida para automatizar la instalación de las funciones clave y crear un entorno de desarrollo uniforme para los científicos de datos. Para obtener más información, consulte Amazon SageMaker Studio en la SageMaker documentación.	Ingeniero de aprendizaje automático, científico de datos

Integre las canalizaciones de CI/CD

Tarea	Descripción	Habilidades requeridas
Cree una cuenta de automatización.	Cree una cuenta de AWS en la que se ejecuten las canalizaciones y los trabajos automatizados. Puede conceder a los equipos de ciencia de datos acceso de lectura a esta cuenta. Para obtener instrucciones, consulte Crear una cuenta de miembro en su organización en la documentación de AWS Organizations.	Administrador de AWS
Configure un registro modelo.	Configure el registro de SageMaker modelos en la cuenta de automatización. Este registro almacena los metadatos de los modelos de aprendizaje automático y ayuda a determinados científicos de datos o líderes de equipo a aprobar o rechazar modelos. Para obtener más información, consulte Registrar e implementar modelos con Model Registry en la SageMaker documentación.	Ingeniero de ML
Cree una `Model Build` canalización.	Cree una canalización de CI/CD en Azure que se inicie de forma manual o automática cuando el código se introduzc	DevOps ingeniero, ingeniero de aprendizaje automático

Tarea	Descripción	Habilidades requeridas
	a en el `Model Build` repositorio. La canalización debe comprobar el código fuente y crear o actualizar una SageMaker canalización en la cuenta de Automation. La canalización debería añadir un modelo nuevo al registro de modelos. Para obtener más información sobre la creación de una canalización, consulte la documentación de Azure Pipelines.	

Cree la pila de despliegue

Tarea	Descripción	Habilidades requeridas
Cree cuentas de implement ación y puesta en escena de AWS.	Cree cuentas de AWS para organizar e implementar modelos de aprendizaje automático. Estas cuentas deben ser idénticas para poder realizar pruebas precisas de los modelos durante la fase de preparaci ón antes de pasar a la fase de producción. Puede dar a los equipos de ciencia de datos acceso de lectura a la cuenta de ensayo. Para obtener instrucciones, consulte Crear una cuenta de miembro en su	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	organización en la documentación de AWS Organizations.	
Configure los buckets de S3 para la supervisión de los modelos.	Complete este paso si desea habilitar la supervisión de modelos para los modelos implementados que crea la `Model Deploy` canalización. Cree depósitos de Amazon S3 para almacenar los datos de entrada y salida. Para obtener más información sobre la creación de buckets de S3, consulte Creación de un bucket en la documentación de Amazon S3. Configure los permisos entre cuentas para que los trabajos de monitoreo de modelos automatizados se ejecuten en la cuenta de automatización. Para obtener más información, consulte Supervisar la calidad de los datos y los modelos en la SageMaker documentación.	Ingeniero de ML

Tarea	Descripción	Habilidades requeridas
Cree una `Model Deploy` canalización.	Cree una canalización de CI/CD en Azure que comience cuando se apruebe un modelo en el registro de modelos. La canalización debería comprobar el código fuente y el artefacto del modelo, crear las plantillas de infraestructura para implementar el modelo en las cuentas de ensayo y producción, implementar el modelo en la cuenta provision al, ejecutar pruebas automatiz adas, esperar a la aprobació n manual e implementar el modelo aprobado en la cuenta de producción. Para obtener más información sobre la creación de una canalización, consulte la documentación de Azure Pipelines.	DevOps ingeniero, ingeniero de aprendizaje automático

(Opcional) Automatice la infraestructura del entorno de aprendizaje automático

Tarea	Descripción	Habilidades requeridas
Cree CloudFormation plantilla s o CDK de AWS.	Defina el kit de desarrollo en la nube de AWS (AWS CDK) o las CloudFormation plantillas de AWS para todos los entornos que deben implementarse automátic amente. Esto podría incluir el entorno de desarrollo, el	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	entorno de automatización y los entornos de preparación e implementación. Para obtener más información, consulte la CDK y la CloudFormationdocumentación de AWS.	
Cree una `Infrastructure` canalización.	Cree una canalización de CI/CD en Azure para la implementación de la infraestructura. Un administrador puede iniciar esta canalización para crear nuevas cuentas de AWS y configurar los entornos que necesite el equipo de aprendizaje automático.	DevOps ingeniero

Solución de problemas

Problema	Solución
Supervisión y detección de desviaciones insuficientes: una supervisión inadecuada puede provocar que no se detecten los problemas de rendimiento del modelo o que se desvíen los datos.	Refuerce los marcos de monitoreo con herramientas como Amazon CloudWatch, SageMaker Model Monitor y SageMaker Clarify. Configure alertas para tomar medidas inmediatas en caso de problemas identificados.
Errores de activación de la canalización de CI: es DevOps posible que la canalización de CI de Azure no se active al fusionar el código debido a un error de configuración.	Compruebe la configuración del DevOps proyecto de Azure para asegurarse de que los webhooks estén correctamente configurados y apunten a los puntos finales correctos SageMaker .
Gobernanza: es posible que la cuenta central de automatización no aplique las	Audite la configuración de la cuenta de automatización y asegúrese de que todos los

Problema	Solución
mejores prácticas en todas las plataformas de aprendizaje automático, lo que provocará flujos de trabajo incoherentes.	entornos y modelos de aprendizaje automátic o se ajusten a las mejores prácticas y políticas predefinidas.
Retrasos en la aprobación del registro del modelo: esto ocurre cuando hay un retraso en la comprobación y aprobación del modelo, ya sea porque las personas tardan en revisarlo o por problemas técnicos.	Implemente un sistema de notificación para alertar a las partes interesadas sobre los modelos que están pendientes de aprobación y agilice el proceso de revisión.
Fallos en los eventos de despliegue del modelo: los eventos que se envían para iniciar los procesos de despliegue del modelo pueden fallar y provocar retrasos en el despliegue.	Confirma que Amazon EventBridge tiene los permisos y los patrones de eventos correctos para invocar las DevOps canalizaciones de Azure correctamente.
Cuellos de botella en el despliegue en producción: los procesos de aprobación manual pueden crear cuellos de botella y retrasar el despliegue de los modelos en producción.	Optimice el flujo de trabajo de aprobación dentro del proceso de implementación del modelo, promoviendo las revisiones oportunas y canales de comunicación claros.

Recursos relacionados

Documentación de AWS

- SageMaker Documentación de Amazon
- Machine Learning Lens (AWS Well Architected Framework)
- Planificación de una MLOP exitosa (AWS Prescriptive Guidance)

Otros recursos de AWS

- Hoja de ruta básica de MLOps para empresas con Amazon (entrada del blog de SageMaker AWS)
- AWS Summit ANZ 2022: nd-to-end MLOps electrónicos para arquitectos (vídeo) YouTube

Documentación de Azure

- DevOps Documentación de Azure
- Documentación de Azure Pipelines

Cree una imagen de contenedor Docker personalizada SageMaker y úsela para el entrenamiento de modelos en AWS Step Functions

Creado por Julia Bluszcz (AWS), Neha Sharma (AWS), Aubrey Oosthuizen (AWS), Mohan Gowda Purushothama (AWS) y Mateusz Zaremba (AWS)

Entorno: producción	Tecnologías: aprendizaje automático e inteligencia artificial; DevOps	Servicios de AWS: Amazon ECR; Amazon SageMaker; AWS Step Functions

Resumen

Este patrón muestra cómo crear una imagen de contenedor de Docker para Amazon SageMaker y utilizarla como modelo de formación en AWS Step Functions. Al empaquetar algoritmos personalizados en un contenedor, puede ejecutar prácticamente cualquier código del SageMaker entorno, independientemente del lenguaje de programación, el marco o las dependencias.

En la SageMaker libreta de ejemplo proporcionada, la imagen del contenedor Docker personalizado se almacena en Amazon Elastic Container Registry (Amazon ECR). A continuación, Step Functions utiliza el contenedor que está almacenado en Amazon ECR para ejecutar un script de procesamiento de Python. SageMaker A continuación, el contenedor exporta el modelo a Amazon Simple Storage Service (Amazon S3).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un rol de AWS Identity and Access Management (IAM) para SageMaker con permisos de Amazon S3
- Una función de IAM para Step Functions
- Conocimientos básicos sobre Python
- Familiaridad con el SDK de Amazon SageMaker Python
- Información de la interfaz de la línea de comandos de AWS (AWS CLI)

- Información de AWS SDK para Python (Boto3)
- Amazon ECR
- Familiaridad con Docker

Versiones de producto

- SDK de ciencia de datos AWS Step Functions, versión 2.3.0
- Amazon SageMaker Python SDK versión 2.78.0

Arquitectura

En el siguiente diagrama, se muestra un ejemplo de flujo de trabajo para crear una imagen de contenedor de Docker y utilizarla después como modelo de entrenamiento en Step Functions: SageMaker

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un científico o DevOps ingeniero de datos utiliza un SageMaker bloc de notas de Amazon para crear una imagen de contenedor Docker personalizada.
2. Un científico o DevOps ingeniero de datos almacena la imagen del contenedor de Docker en un repositorio privado de Amazon ECR que se encuentra en un registro privado.
3. Un científico o DevOps ingeniero de datos utiliza el contenedor de Docker para ejecutar un trabajo de SageMaker procesamiento de Python en un flujo de trabajo de Step Functions.

Automatizar y escalar

El ejemplo de SageMaker cuaderno de este patrón utiliza un tipo de instancia de `ml.m5.xlarge` bloc de notas. Puede cambiar el tipo de instancia para que se ajuste a su caso de uso. Para obtener más información sobre los tipos de instancias de SageMaker notebook, consulta SageMaker los precios de Amazon.

Herramientas

- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable.

- Amazon SageMaker es un servicio de aprendizaje automático gestionado (ML) que le ayuda a crear y entrenar modelos de aprendizaje automático y, a continuación, a implementarlos en un entorno hospedado listo para la producción.
- Amazon SageMaker Python SDK es una biblioteca de código abierto para entrenar e implementar modelos de aprendizaje automático en ellos. SageMaker
- AWS Step Functions es un servicio de orquestación sin servidor que le permite combinar funciones de Lambda AWS y otros servicios de AWS para crear aplicaciones esenciales desde el punto de vista empresarial.
- El SDK de Python para ciencia de datos de AWS Step Functions es una biblioteca de código abierto que le ayuda a crear flujos de trabajo de Step Functions que procesan y publican modelos de aprendizaje automático.

Epics

Crear una imagen de contenedor de Docker personalizada y guardarla en Amazon ECR

Tarea	Descripción	Habilidades requeridas
Configure Amazon ECR y cree un nuevo registro privado.	Si aún no lo ha hecho, configure Amazon ECR siguiendo las instrucciones de Configuración con Amazon ECR de la Guía del usuario de Amazon ECR. Cada cuenta de AWS se proporciona con un registro privado de Amazon ECR predeterminado.	DevOps ingeniero
Crear un repositorio privado de Amazon ECR.	Siga las instrucciones de Creación de un repositorio privado de la Guía del usuario de Amazon ECR. Nota: El repositorio que cree es donde almacenará sus	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	imágenes de contenedores de Docker personalizadas.	

Tarea	Descripción	Habilidades requeridas
Cree un Dockerfile que incluya las especificaciones necesarias para ejecutar su trabajo de SageMaker procesamiento.	Cree un Dockerfile que incluya las especificaciones necesarias para ejecutar su trabajo de SageMaker procesamiento configurando un Dockerfile. Para obtener instrucciones, consulta Cómo adaptar tu propio contenedor de formación en la Guía para SageMaker desarrolladores de Amazon. Para obtener más información sobre Dockerfiles, consulta la referencia de Dockerfile en la documentación de Docker. Ejemplo de celdas de código de un cuaderno de Jupyter para crear un Dockerfile Celda 1 `# Make docker folder` `!mkdir -p docker` Celda 2 `%%writefile docker/Dockerfile` `FROM python:3.7-slim-buster` `RUN pip3 install pandas==0.25.3 scikit-learn==0.21.3`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`` ENV PYTHONUNBUFFERED=T RUE ENTRYPOINT ["python3"] ```	

Tarea	Descripción	Habilidades requeridas
Cree la imagen del contenedor de Docker y enviarla a Amazon ECR.	1. Cree la imagen del contenedor con el Dockerfile que creó al ejecutar el comando `docker build` en la AWS CLI. 2. Ejecute el comando `docker push` para enviar la imagen del contenedor a Amazon ECR. Para obtener más información, consulte Crear y registrar el contenedor en Cómo crear su propio contenedor de algoritmos GitHub. Ejemplo de celdas de código del cuaderno de Jupyter para crear y registrar una imagen de Docker Importante: antes de ejecutar las siguientes celdas, asegúrate de haber creado un Dockerfile y de haberlo guardado en el directorio denominado `docker`. Además, asegúrese de haber creado un repositorio de Amazon ECR y de sustituir el valor `ecr_repository` de la primera celda por el nombre del repositorio. Celda 1	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`import boto3` `tag = ':latest'` `account_id = boto3.cli` `ent('sts').get_cal` `ler_identity().get` `('Account')` `region = boto3.Ses` `sion().region_name` `ecr_repository = 'byoc'` `image_uri = '{}.dkr.e` `cr.{}.amazonaws.com/` `{}'.format(account_id,` ` region, ecr_repository` ` + tag)` Celda 2 `# Build docker image` `!docker build -t` ` $image_uri docker` Celda 3 `# Authenticate to ECR` `!aws ecr get-login` `-password --region` ` {region} | docker` ` login --username` ` AWS --password-stdin` ` {account_id}.dkr.ecr.` `{region}.amazonaws.com` Celda 4 `# Push docker image` `!docker push $image_ur` `i`	

Tarea	Descripción	Habilidades requeridas
	Nota: Debe autenticar su cliente de Docker en su registro privado para poder utilizar los comandos `docker push` y `docker pull`. Estos comandos envían y extraen imágenes de los repositorios de su registro y las extraen de ellos.	

Cree un flujo de trabajo de Step Functions que utilice su imagen de contenedor de Docker personalizada

Tarea	Descripción	Habilidades requeridas
Cree un script de Python que incluya su procesamiento personalizado y su lógica de capacitación de modelos.	Escriba una lógica de procesamiento personalizada para ejecutarla en su script de procesamiento de datos. A continuación, guárdelo como un script de Python denominado `training.py` . Para obtener más informaci ón, consulte Utilice su propio modelo con el modo SageMaker script activado GitHub. Ejemplo de script de Python que incluye procesamiento personalizado y lógica de capacitación de modelos	Científico de datos

Tarea	Descripción	Habilidades requeridas
	`%%writefile training.py` `from numpy import empty` `import pandas as pd` `import os` `from sklearn import datasets, svm` `from joblib import dump, load` `if __name__ == '__main__':` `    digits = datasets.load_digits()` `    #create classifier object` `    clf = svm.SVC(gamma=0.001, C=100.)` `    #fit the model` `    clf.fit(digits.data[:-1], digits.target[:-1])` `    #model output in binary format` `    output_path = os.path.join('/opt/ml/processing/model', "model.joblib")` `    dump(clf, output_path)`	

Tarea	Descripción	Habilidades requeridas
Cree un flujo de trabajo de Step Functions que incluya su trabajo de SageMaker procesamiento como uno de los pasos.	Instale e importe el SDK de ciencia de datos de AWS Step Functions y cargue el archivo training.py en Amazon S3. A continuación, utilice el SDK de Amazon SageMaker Python para definir un paso de procesamiento en Step Functions. Importante: Asegúrese de haber creado un rol de ejecución de IAM para Step Functions en su cuenta de AWS. Ejemplo de configuración del entorno y script de capacitación personalizado para cargarlo en Amazon S3 `!pip install stepfunctions` `import boto3` `import stepfunctions` `import sagemaker` `import datetime` `from stepfunctions import steps` `from stepfunctions.inputs import ExecutionInput` `from stepfunctions.steps import (` `Chain` `)`	Científico de datos

Tarea	Descripción	Habilidades requeridas
	from stepfunct ions.workflow import Workflow from sagemaker .processing import ScriptProcessor, ProcessingInput, ProcessingOutput sagemaker_session = sagemaker.Session() bucket = sagemaker _session.default_b ucket() role = sagemaker .get_execution_role() prefix = 'byoc-tra ining-model' # See prerequisites section to create this role workflow_execution_rol e = f"arn:aws:iam:: {account_id}:role/Ama zonSageMaker-StepF unctionsWorkflowEx ecutionRole" execution_input = ExecutionInput(schema={ "Preproce ssingJobName": str}) input_code = sagemaker _session.upload_data("training.py", bucket=bucket, key_prefix="prepro cessing.py",	

Tarea	Descripción	Habilidades requeridas
	) Ejemplo SageMaker de definición de paso de procesamiento que utiliza una imagen personalizada de Amazon ECR y un script de Python Nota: Asegúrese de utilizar el parámetro `execution _input` para especificar el nombre del trabajo. El valor del parámetro debe ser único cada vez que se ejecute el trabajo. Además, el código del archivo training.py se pasa como parámetro `input` a `ProcessingStep` , lo que significa que se copiará dentro del contenedor. El destino del código `ProcessingInput` es el mismo que el del segundo argumento incluido en `container_entrypoi nt` . `script_processor = ScriptProcessor(co mmand=['python3'], image_uri=image_uri, role=role, instance_count=1,`	

Tarea	Descripción	Habilidades requeridas
	<pre>instance_type='ml.m5.xlarge') processing_step = steps.ProcessingStep("training-step", processor=script_processor, job_name=execution_input["PreprocessingJobName"], inputs=[ProcessingInput(source=input_code, destination="/opt/ml/processing/input/code", input_name="code",),], outputs=[ProcessingOutput(source='/opt/ml/processing/model', destination="s3://{}/{}".format(bucket, prefix), output_name='byoc-example')], container_entrypoint=["python3", "/opt/ml/processing/input/code/training.py"],</pre>	

Tarea	Descripción	Habilidades requeridas
	) Ejemplo de flujo de trabajo de Step Functions que ejecuta un trabajo SageMaker de procesamiento Nota: Este flujo de trabajo de ejemplo incluye solo el paso del trabajo de SageMaker procesamiento, no un flujo de trabajo completo de Step Functions. Para ver un ejemplo completo de flujo de trabajo, consulte Cuadernos de ejemplo SageMaker en la documentación del SDK de ciencia de datos de AWS Step Functions. `workflow_graph = Chain([processing_step])` `workflow = Workflow( name="ProcessingWorkflow", definition=workflow_graph, role=workflow_execution_role )` `workflow.create()` `# Execute workflow` `execution = workflow.execute( inputs={`	

Tarea	Descripción	Habilidades requeridas
	`"Preproce ssingJobName": str(datetime.datet ime.now().strftime ("%Y%m%d%H%M-%SS")), # Each pre processin g job (SageMaker processing job) requires a unique name, } ) execution_output = execution.get_outp ut(wait=True)`	

Recursos relacionados

- Procesar datos (Amazon SageMaker Developer Guide)
- Adaptación de tu propio contenedor de formación (Amazon SageMaker Developer Guide)

Implemente la lógica de preprocesamiento en un modelo de aprendizaje automático en un único punto final mediante una canalización de inferencias en Amazon SageMaker

Creado por Mohan Gowda Purushothama (AWS), Gabriel Rodríguez García (AWS) y Mateusz Zaremba (AWS)

Entorno: producción	Tecnologías: machine learning e inteligencia artificial; contenedores y microservicios	Servicios de AWS: Amazon SageMaker; Amazon ECR

Resumen

Este patrón explica cómo implementar varios objetos del modelo de canalización en un único punto final mediante una canalización de inferencia en Amazon SageMaker. El objeto del modelo de canalización representa diferentes etapas del flujo de trabajo del machine learning (ML), como el preprocesamiento, la inferencia de modelos y el posprocesamiento. Para ilustrar el despliegue de objetos del modelo de canalización conectados en serie, este patrón muestra cómo implementar un contenedor Scikit-learn de preprocesamiento y un modelo de regresión basado en el algoritmo de aprendizaje lineal incorporado. SageMaker La implementación se aloja en un único punto final. SageMaker

Nota: la implementación de este patrón utiliza el tipo de instancia ml.m4.2xlarge. Le recomendamos usar un tipo de instancia que se ajuste a sus requisitos de tamaño de datos y a la complejidad de su flujo de trabajo. Para obtener más información, consulta los SageMaker precios de Amazon. Este patrón usa imágenes de Docker prediseñadas para Scikit-learn, pero puede usar sus propios contenedores de Docker e integrarlos en su flujo de trabajo.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Python 3.9
- Amazon SageMaker Python SDK y biblioteca Boto3

- Función de AWS Identity and Access Management (AWS IAM) con SageMaker permisos básicos y permisos de Amazon Simple Storage Service (Amazon S3)

Versiones de producto

- Amazon SageMaker Python SDK 2.49.2

Arquitectura

Pila de tecnología de destino

- Amazon Elastic Container Registry (Amazon ECR)
- Amazon SageMaker
- Amazon SageMaker Studio
- Amazon Simple Storage Service (Amazon S3)
- Punto final de inferencia en tiempo real para Amazon SageMaker

Arquitectura de destino

El siguiente diagrama muestra la arquitectura para el despliegue de un objeto del modelo de SageMaker canalización de Amazon.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un SageMaker cuaderno despliega un modelo de canalización.
2. Un bucket de S3 almacena los artefactos del modelo.
3. Amazon ECR obtiene las imágenes del contenedor de origen del bucket de S3.

Herramientas

Herramientas de AWS

- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable.

- Amazon SageMaker es un servicio de aprendizaje automático gestionado que le ayuda a crear y entrenar modelos de aprendizaje automático para luego implementarlos en un entorno hospedado listo para la producción.
- Amazon SageMaker Studio es un entorno de desarrollo integrado (IDE) basado en la web para el aprendizaje automático que le permite crear, entrenar, depurar, implementar y supervisar sus modelos de aprendizaje automático.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Código

El código de este patrón está disponible en GitHub Inference Pipeline con los repositorios Scikit-learn y Linear Learner.

Epics

Prepare el conjunto de datos

Tarea	Descripción	Habilidades requeridas
Prepare el conjunto de datos para la tarea de regresión.	Abre una libreta en Amazon SageMaker Studio. Para importar todas las bibliotecas necesarias e inicializar su entorno de trabajo, utilice el siguiente código de ejemplo en su bloc de notas: `import sagemaker` `from sagemaker import get_execution_role` `sagemaker_session = sagemaker.Session()` `# Get a SageMaker-compatible role used`	Científico de datos

Tarea	Descripción	Habilidades requeridas
	<pre>by this Notebook Instance. role = get_execu tion_role() # S3 prefix bucket = sagemaker _session.default_b ucket() prefix = "Scikit-L inearLearner-pipel ine-abalone-example"</pre> Para descargar un conjunto de datos de muestra, añada el siguiente código a su bloc de notas: <pre>! mkdir abalone_data ! aws s3 cp s3://sage maker-sample-files /datasets/tabular/ uci_abalone/abalon e.csv ./abalone_data</pre> Nota: el ejemplo de este patrón utiliza el conjunto de datos Abalone del UCI Machine Learning Repository.	

Tarea	Descripción	Habilidades requeridas
Cargue el conjunto de datos en un bucket de S3.	En el bloc de notas en el que preparó su conjunto de datos anteriormente, añada el siguiente código para cargar los datos de muestra en un bucket de S3: `WORK_DIRECTORY = "abalone_data"` `train_input = sagemaker_session.upload_data( path="{}/{}".format(WORK_DIRECTORY, "abalone.csv"), bucket=bucket, key_prefix="{}/{}".format(prefix, "train"), )`	Científico de datos

Cree el preprocesador de datos con SKLearn

Tarea	Descripción	Habilidades requeridas
Prepare el script preprocesor.py.	1. Copie la lógica de preprocesamiento del archivo Python del repositorio GitHub sklearn_abalone_featurizer.py y, a continuación, pegue el código en un archivo Python independiente denominado`sklearn_abalone_featurizer.py`. Puede modificar el	Científico de datos

Tarea	Descripción	Habilidades requeridas
	código para que se adapte a su conjunto de datos y flujo de trabajo personalizados. 2. Guarde el `sklearn_abalone_featurizer.py` archivo en el directorio raíz del proyecto (es decir, en la misma ubicación en la que ejecuta el SageMaker bloc de notas).	

Tarea	Descripción	Habilidades requeridas
Cree el objeto del preprocesador SKLearn.	Para crear un objeto preprocesador de SKLearn (denominado Estimator de SKLearn) que pueda incorporar a su proceso de inferencia final, ejecute el siguiente código en su bloc de notas: SageMaker `from sagemaker.sklearn.estimator import SKLearn` `FRAMEWORK_VERSION = "0.23-1"` `script_path = "sklearn_abalone_featurizer.py"` `sklearn_preprocessor = SKLearn(` `entry_point=script_path,` `role=role,` `framework_version=FRAMEWORK_VERSION,` `instance_type="ml.c4.xlarge",` `sagemaker_session=sagemaker_session,` `)` `sklearn_preprocessor.fit({"train": train_input})`	Científico de datos

Tarea	Descripción	Habilidades requeridas
Pruebe la inferencia del preprocesador.	Para confirmar que su preprocesador está definido correctamente, inicie un trabajo de transformación por lotes introduciendo el siguiente código en su cuaderno: SageMaker `# Define a SKLearn Transformer from the trained SKLearn Estimator` `transformer = sklearn_preprocessor.transformer(` `instance_count=1, instance_type="ml.m5.xlarge", assemble_with="Line", accept="text/csv"` `)` `# Preprocess training input` `transformer.transform(train_input, content_type="text/csv")` `print("Waiting for transform job: " + transformer.latest_transform_job.job_name)` `transformer.wait()` `preprocessed_train = transformer.output_path`	

Cree un modelo de machine learning

Tarea	Descripción	Habilidades requeridas
Cree un objeto modelo.	Para crear un objeto modelo basado en el algoritmo de aprendizaje lineal, introduzc a el siguiente código en su SageMaker bloc de notas: `import boto3 from sagemaker .image_uris import retrieve` `ll_image = retrieve( "linear-learner", boto3.Session().re gion_name) s3_ll_output_key _prefix = "ll_train ing_output" s3_ll_output_location = "s3://{}/{}/{}/{}" .format( bucket, prefix, s3_ll_output_key_p refix, "ll_model" )` `ll_estimator = sagemaker.estimato r.Estimator( ll_image, role, instance_count=1, instance_type="ml. m4.2xlarge", volume_size=20, max_run=3600, input_mode="File",`	Científico de datos

Tarea	Descripción	Habilidades requeridas
	<pre> output_path=s3_ll_ output_location, sagemaker_session= sagemaker_session,) ll_estimator.s et_hyperparameters (feature_dim=10, predictor_type="re gressor", mini_batc h_size=32) ll_train_data = sagemaker.inputs.T rainingInput(preprocessed_train , distribution="Full yReplicated", content_type="text /csv", s3_data_type="S3Pr efix",) data_channels = {"train": ll_train_ data} ll_estimator.fit(inpu ts=data_channels, logs=True)</pre> El código anterior recupera la imagen de Docker de Amazon ECR correspon diente del registro público de Amazon ECR del modelo, crea un objeto estimador y, a continuación, utiliza ese objeto	

Tarea	Descripción	Habilidades requeridas
	para entrenar el modelo de regresión.	

Implemente la canalización final

Tarea	Descripción	Habilidades requeridas
Implemente el modelo de canalización.	Para crear un objeto de modelo de canalización (es decir, un objeto de preproces ador) e implementar el objeto, introduzca el siguiente código en su SageMaker bloc de notas: `from sagemaker.model import Model` `from sagemaker.pipeline import PipelineModel` `import boto3` `from time import gmtime, strftime` `timestamp_prefix = strftime("%Y-%m-%d-%H-%M-%S", gmtime())` `scikit_learn_inferencee_model = sklearn_preprocessor.create_model()` `linear_learner_model = ll_estimator.create_model()`	Científico de datos

Tarea	Descripción	Habilidades requeridas
	`` model_name = "inferenc e-pipeline-" + timestamp_prefix endpoint_name = "inference-pipeline- ep-" + timestamp_prefix sm_model = PipelineM odel(name=model_name, role=role, models= [scikit_learn_infe rencee_model, linear_learner_model]) sm_model.deploy(init ial_instance_count =1, instance_type="ml. c4.xlarge", endpoint_ name=endpoint_name) ``` Nota: puede ajustar el tipo de instancia utilizado en el objeto modelo para adaptarlo a sus necesidades.	

Tarea	Descripción	Habilidades requeridas
Pruebe la inferencia.	Para confirmar que el punto final funciona correctamente, ejecute el siguiente código de inferencia de ejemplo en su SageMaker bloc de notas: `from sagemaker.predicto r import Predictor from sagemaker.serializ ers import CSVSerial izer` `payload = "M, 0.44, 0.365, 0.125, 0.516, 0.2155, 0.114, 0.155" actual_rings = 10 predictor = Predictor( endpoint_name=endp oint_name, sagemaker _session=sagemaker _session, serialize r=CSVSerializer() )` `print(predictor .predict(payload))`	Científico de datos

Recursos relacionados

- Procese previamente los datos de entrada antes de realizar predicciones mediante las canalizaciones de SageMaker inferencia de Amazon y Scikit-learn (blog de AWS Machine Learning)
- Machine Learning de principio a fin con Amazon SageMaker (GitHub)

Desarrolle asistentes avanzados de IA generativa basados en chat mediante RAG y solicitudes ReAct

Creado por Praveen Kumar Jeyarajan (AWS), Jundong Qiao (AWS), Kara Yang (AWS), Kiowa Jackson (AWS), Noah Hamilton (AWS) y Shuai Cao (AWS)

Repositorio de código: genai-bedrock-chatbot	Entorno: PoC o piloto	Tecnologías: aprendizaje automático e inteligencia artificial; bases de datos DevOps; sin servidor
Servicios de AWS: Amazon Bedrock; Amazon ECS; Amazon Kendra; AWS Lambda		

Resumen

Una empresa típica tiene el 70 por ciento de sus datos atrapados en sistemas aislados. Puede utilizar asistentes generativos basados en el chat y basados en la inteligencia artificial para obtener información y relaciones entre estos silos de datos mediante interacciones en lenguaje natural. Para aprovechar al máximo la IA generativa, los resultados deben ser fiables, precisos e incluir los datos corporativos disponibles. El éxito de los asistentes basados en el chat depende de lo siguiente:

- Modelos de IA generativa (como Anthropic Claude 2)
- Vectorización de fuentes de datos
- Técnicas de razonamiento avanzadas, como el ReAct marco, para impulsar el modelo

Este patrón proporciona enfoques de recuperación de datos de fuentes de datos como los depósitos de Amazon Simple Storage Service (Amazon S3), AWS Glue y Amazon Relational Database Service (Amazon RDS). El valor se obtiene de esos datos intercalando la generación aumentada de recuperación (RAG) con los métodos. chain-of-thought Los resultados permiten mantener conversaciones complejas con asistentes por chat que se basan en la totalidad de los datos almacenados en su empresa.

Este patrón utiliza los SageMaker manuales de Amazon y las tablas de datos de precios como ejemplo para explorar las capacidades de un asistente generativo basado en el chat de IA. Crearás un asistente basado en el chat que ayude a los clientes a evaluar el SageMaker servicio respondiendo a preguntas sobre los precios y las capacidades del servicio. La solución utiliza una biblioteca Streamlit para crear la aplicación frontend y el LangChain marco para desarrollar el backend de la aplicación con la tecnología de un gran modelo de lenguaje (LLM).

Las consultas al asistente basado en el chat se responden con una clasificación inicial de intenciones para redirigirlas a uno de los tres posibles flujos de trabajo. El flujo de trabajo más sofisticado combina una orientación de asesoramiento general con un análisis de precios complejo. Puede adaptar el patrón para que se adapte a los casos de uso empresariales, corporativos e industriales.

Requisitos previos y limitaciones

Requisitos previos

- Instalación y configuración de la interfaz de línea de comandos de AWS (AWS CLI)
- Instalación y configuración del kit de herramientas AWS Cloud Development Kit (AWS CDK) 2.114.1 o posterior
- Familiaridad básica con Python y AWS CDK
- Git instalado
- Docker instalado
- Python 3.11 o posterior instalado y configurado (para obtener más información, consulte la sección Herramientas)
- Una cuenta de AWS activa iniciada mediante AWS CDK
- El acceso a los modelos Amazon Titan y Anthropic Claude está habilitado en el servicio Amazon Bedrock
- Credenciales de seguridad de AWS, incluida `AWS_ACCESS_KEY_ID`, correctamente configuradas en su entorno de terminal

Limitaciones

- LangChain no es compatible con todos los LLM para la transmisión. Los modelos Anthropic Claude son compatibles, pero los modelos de AI21 Labs no.
- Esta solución se implementa en una única cuenta de AWS.

- Esta solución solo se puede implementar en las regiones de AWS en las que estén disponibles Amazon Bedrock y Amazon Kendra. Para obtener información sobre la disponibilidad, consulte la documentación de Amazon Bedrock y Amazon Kendra.

Versiones de producto

- Python versión 3.11 o posterior
- Streamlit, versión 1.30.0 o posterior
- Streamlit-Chat versión 0.1.1 o posterior
- LangChain versión 0.1.12 o posterior
- AWS CDK versión 2.132.1 o posterior

Arquitectura

Pila de tecnología de destino

- Amazon Athena
- Amazon Bedrock
- Amazon Elastic Container Service (Amazon ECS)
- AWS Glue
- AWS Lambda
- Amazon S3
- Amazon Kendra
- Elastic Load Balancing

Arquitectura de destino

El código de AWS CDK implementará todos los recursos necesarios para configurar la aplicación de asistente basada en chat en una cuenta de AWS. La aplicación de asistente basada en el chat que se muestra en el siguiente diagrama está diseñada para responder a las consultas SageMaker relacionadas de los usuarios. Los usuarios se conectan a través de un Application Load Balancer a una VPC que contiene un clúster de Amazon ECS que aloja la aplicación Streamlit. Una función Lambda de orquestación se conecta a la aplicación. Las fuentes de datos del bucket S3 proporcionan datos a la función Lambda a través de Amazon Kendra y AWS Glue. La función

Lambda se conecta a Amazon Bedrock para responder a las consultas (preguntas) de los usuarios asistentes basados en el chat.

1. La función Lambda de orquestación envía la solicitud de solicitud LLM al modelo Amazon Bedrock (Claude 2).
2. Amazon Bedrock devuelve la respuesta LLM a la función Lambda de orquestación.

Flujo lógico dentro de la función Lambda de orquestación

Cuando los usuarios hacen una pregunta a través de la aplicación Streamlit, esta invoca directamente la función Lambda de orquestación. El siguiente diagrama muestra el flujo lógico cuando se invoca la función Lambda.

- Paso 1: La entrada `query` (pregunta) se clasifica en una de las tres intenciones:
  - Preguntas de SageMaker orientación general
  - Preguntas generales SageMaker sobre precios (formación/inferencia)
  - Preguntas complejas relacionadas con los precios SageMaker
- Paso 2: La entrada `query` inicia uno de los tres servicios:
  - `RAG Retrieval service`, que recupera el contexto relevante de la base de datos vectorial de Amazon Kendra y llama al LLM a través de Amazon Bedrock para resumir el contexto recuperado como respuesta.
  - `Database Query service`, que utiliza el LLM, los metadatos de la base de datos y las filas de muestra de las tablas relevantes para convertir la entrada en una consulta SQL. `query` El servicio Database Query ejecuta la consulta SQL en la base de datos de SageMaker precios a través de Amazon Athena y resume los resultados de la consulta como respuesta.
  - `In-context ReACT Agent service`, que divide la entrada `query` en varios pasos antes de proporcionar una respuesta. El agente utiliza `RAG Retrieval service` y `Database Query service` como herramientas para recuperar información relevante durante el proceso de razonamiento. Una vez completados los procesos de razonamiento y acción, el agente genera la respuesta final como respuesta.
- Paso 3: La respuesta de la función Lambda de orquestación se envía a la aplicación Streamlit como salida.

Herramientas

Servicios de AWS

- Amazon Athena es un servicio interactivo de consultas que le permite analizar datos directamente en Amazon Simple Storage Service (Amazon S3) usando SQL estándar.
- Amazon Bedrock es un servicio totalmente gestionado que pone a su disposición modelos básicos (FM) de alto rendimiento de las principales empresas emergentes de IA y Amazon a través de una API unificada.
- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura de la nube de AWS en código.
- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.
- Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores escalable y rápido que ayuda a ejecutar, detener y administrar contenedores en un clúster.
- AWS Glue es un servicio de extracción, transformación y carga (ETL) completamente administrado. Ayuda a clasificar, limpiar, enriquecer y mover datos de forma fiable entre almacenes de datos y flujos de datos. Este patrón emplea un rastreador de AWS Glue y una tabla del catálogo de datos de AWS Glue.
- Amazon Kendra es un servicio de búsqueda inteligente que utiliza el procesamiento del lenguaje natural y algoritmos avanzados de aprendizaje automático para devolver respuestas específicas a las preguntas de búsqueda a partir de sus datos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Elastic Load Balancing (ELB) distribuye el tráfico entrante de aplicaciones o redes entre varios destinos. Así, por ejemplo, puede distribuir el tráfico a través de instancias de Amazon Elastic Compute Cloud (Amazon EC2), contenedores y direcciones IP de una o varias zonas de disponibilidad.

Repositorio de código

El código de este patrón está disponible en el GitHub genai-bedrock-chatbotrepositorio.

El repositorio de código contiene los siguientes archivos y carpetas:

- `assets`carpeta: los activos estáticos, el diagrama de arquitectura y el conjunto de datos público
- `code/lambda-container`folder: el código de Python que se ejecuta en la función Lambda
- `code/streamlit-app`folder: el código Python que se ejecuta como imagen del contenedor en Amazon ECS
- `tests`folder: los archivos de Python que se ejecutan para realizar pruebas unitarias de las construcciones de AWS CDK
- `code/code_stack.py`— El CDK de AWS construye los archivos Python que se utilizan para crear recursos de AWS
- `app.py`— Los archivos Python de la pila de CDK de AWS que se utilizan para implementar los recursos de AWS en la cuenta de AWS de destino
- `requirements.txt`— La lista de todas las dependencias de Python que se deben instalar para AWS CDK
- `requirements-dev.txt`— La lista de todas las dependencias de Python que se deben instalar para que AWS CDK ejecute el conjunto de pruebas unitarias
- `cdk.json` – El archivo de entrada que proporciona los valores necesarios para activar los recursos

Nota: El código CDK de AWS utiliza estructuras de nivel 3 (capa 3) y políticas de AWS Identity and Access Management (IAM) administradas por AWS para implementar la solución.

Prácticas recomendadas

- El ejemplo de código que se proporciona aquí es únicamente para una demostración proof-of-concept (PoC) o piloto. Si desea llevar el código a producción, asegúrese de seguir las siguientes prácticas recomendadas:
  - El registro de acceso a Amazon S3 está activado.
  - Los registros de flujo de VPC están habilitados.

  - El índice Amazon Kendra Enterprise Edition está activado.
- Configure la supervisión y las alertas para las funciones de Lambda de AWS. Para obtener más información, consulte Supervisión y solución de problemas de funciones de Lambda. Para obtener más información sobre las prácticas recomendadas generales en el uso de funciones de Lambda, consulte la documentación de AWS.

Epics

Configuración de las credenciales de AWS en su máquina local

Tarea	Descripción	Habilidades requeridas
Exporte las variables de la cuenta y la región de AWS en las que se implementará la pila.	Para proporcionar las credenciales de AWS para AWS CDK mediante variables de entorno, ejecute los siguientes comandos. `export CDK_DEFAU LT_ACCOUNT=<12 Digit AWS Account Number>` `export CDK_DEFAU LT_REGION=<region>`	DevOps ingeniero, AWS DevOps
Configure el perfil de AWS CLI.	Para configurar el perfil de AWS CLI para la cuenta, siga las instrucciones de la documentación de AWS.	DevOps ingeniero, AWS DevOps

Configure su entorno

Tarea	Descripción	Habilidades requeridas
Clone el repositorio en su máquina local.	Para clonar el repositorio, ejecuta el siguiente comando en tu terminal.	DevOps ingeniero, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`git clone https://github.com/awslabs/genai-bedrock-chatbot.git`	
Configure el entorno virtual de Python e instale las dependencias necesarias.	Para configurar y activar el entorno virtual de Python, ejecute el siguiente comando. `cd genai-bedrock-chatbot` `python3 -m venv .venv` `source .venv/bin/activate` Para configurar las dependencias necesarias, ejecute el siguiente comando. `pip3 install -r requirements.txt`	DevOps ingeniero, AWS DevOps
Configure el entorno de AWS CDK y sintetice el código de AWS CDK.	1. Para configurar el entorno CDK de AWS en su cuenta de AWS, ejecute el siguiente comando. `cdk bootstrap aws://ACCOUNT-NUMBER/REGION` 2. Para convertir el código en una configuración de CloudFormation pila de AWS, ejecute el comando`cdk synth`.	DevOps ingeniero, AWS DevOps

Configure e implemente la aplicación de asistente basada en el chat

Tarea	Descripción	Habilidades requeridas
Proporcione acceso al modelo Claude.	Para habilitar el acceso al modelo Anthropic Claude en su cuenta de AWS, siga las instrucciones de la documentación de Amazon Bedrock.	AWS DevOps
Implementar recursos en la cuenta.	Para implementar recursos en la cuenta de AWS mediante la AWS CDK, haga lo siguiente: 1. En la raíz del repositorio clonado, en el `cdk.json` archivo, introduzca las entradas para los `logging` parámetros. Los valores de ejemplo son `INFO`,`DEBUG`,`WARN`, y`ERROR`. Estos valores definen los mensajes a nivel de registro para la función Lambda y la aplicación Streamlit. 2. El `app.py` archivo de la raíz del repositorio clonado contiene el nombre de la CloudFormation pila de AWS utilizada para la implementación. El nombre predeterminado de la pila es`chatbot-stack` . 3. Ejecute el `cdk deploy` comando para implementar los recursos.	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	El `cdk deploy` comando usa construcciones L3 para crear varias funciones Lambda para copiar documentos y archivos de conjuntos de datos CSV en depósitos de S3. 4. Una vez completado el comando, inicie sesión en la consola de administración de AWS, abra la CloudFormation consola y compruebe que la pila se ha implementado correctamente. Tras una implementación correcta, puede acceder a la aplicación de asistente basada en el chat mediante la URL proporcionada en la sección de CloudFormation resultados.	

Tarea	Descripción	Habilidades requeridas
Ejecute el rastreador de AWS Glue y cree la tabla del catálogo de datos.	El rastreador de AWS Glue se usa para mantener el esquema de datos dinámico. La solución crea y actualiza las particiones en la tabla del catálogo de datos de AWS Glue mediante la ejecución del rastreador a petición. Una vez copiados los archivos del conjunto de datos CSV en el depósito de S3, ejecute el rastreador AWS Glue y cree el esquema de tablas del catálogo de datos para realizar las pruebas: 1. Navegue hasta la consola de AWS Glue. 2. En el panel de navegació n, en Catálogo de datos, seleccione rastreador. 3. Seleccione el rastreador con el sufijo`sagemaker-pricing-crawler` . 4. Ejecute el rastreador. 5. Una vez que el rastreador se ejecuta correctamente, crea una tabla de Catálogo de datos de AWS Glue. Nota: El código CDK de AWS configura el rastreador AWS Glue para que se ejecute bajo demanda, pero también	DevOps ingeniero, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	puede programarlo para que se ejecute periódicamente.	
Inicie la indexación de documentos.	Una vez copiados los archivos en el bucket de S3, utilice Amazon Kendra para rastrearl os e indexarlos: 1. Navegue hasta la consola de Amazon Kendra. 2. Seleccione el índice con el sufijo`chatbot-index` . 3. En el panel de navegació n, elija Fuentes de datos y seleccione el conector de fuentes de datos con el sufijo`chatbot-index` . 4. Seleccione Sincroniz ar ahora para iniciar el proceso de indexación. Nota: El código CDK de AWS configura la sincroniz ación de índices de Amazon Kendra para que se ejecute bajo demanda, pero también puede ejecutarse periódica mente mediante el parámetro Schedule.	AWS DevOps, DevOps ingeniero

Limpie todos los recursos de AWS de la solución

Tarea	Descripción	Habilidades requeridas
Elimine los recursos de AWS.	Después de probar la solución, limpie los recursos: 1. Para eliminar los recursos de AWS implementados por la solución, ejecute el comando `cdk destroy`. 2. Elimine todos los objetos de los dos buckets de S3 y, a continuación, elimine los buckets. Para obtener más información, consulte Eliminación de un bucket.	DevOps ingeniero, AWS DevOps

Solución de problemas

Problema	Solución
AWS CDK devuelve errores.	Para obtener ayuda con los errores de AWS CDK, consulte Solución de problemas comunes de AWS CDK.

Recursos relacionados

- Amazon Bedrock:
  - Acceso modelo
  - Parámetros de inferencia para modelos básicos
- Creación de funciones de Lambda con Python
- Comience a utilizar el AWS CDK

- Trabajar con el CDK de AWS en Python
- Creador de aplicaciones de IA generativa en AWS
- LangChain documentación
- Documentación simplificada

Información adicional

Comandos de AWS CDK

Cuando trabaje con AWS CDK, recuerde los siguientes comandos útiles:

- Muestra todas las pilas de la aplicación

```
cdk ls
```

- Emite la plantilla de AWS CloudFormation sintetizada

```
cdk synth
```

- Implementa la pila en la cuenta y región de AWS predeterminadas

```
cdk deploy
```

- Compara la pila implementada con el estado actual

```
cdk diff
```

- Abre la documentación de AWS CDK

```
cdk docs
```

- Elimina la CloudFormation pila y elimina los recursos desplegados por AWS

```
cdk destroy
```

Desarrolle un asistente totalmente automatizado basado en el chat con los agentes y las bases de conocimiento de Amazon Bedrock

Creado por Jundong Qiao (AWS), Kara Yang (AWS), Kiowa Jackson (AWS), Noah Hamilton (AWS), Praveen Kumar Jeyarajan (AWS) y Shuai Cao (AWS)

Repositorio de código: genai-bedrock-agent-chatbot	Entorno: PoC o piloto	Tecnologías: aprendizaje automático e inteligencia artificial; sin servidor
Servicios de AWS: Amazon Bedrock; AWS CDK; AWS Lambda		

Resumen

Muchas organizaciones se enfrentan a desafíos a la hora de crear un asistente basado en el chat que sea capaz de organizar diversas fuentes de datos para ofrecer respuestas integrales. Este patrón presenta una solución para desarrollar un asistente basado en el chat que sea capaz de responder a consultas tanto de la documentación como de las bases de datos, con una implementación sencilla.

Empezando por Amazon Bedrock, este servicio de inteligencia artificial generativa (IA) totalmente gestionado ofrece una amplia gama de modelos básicos (FM) avanzados. Esto facilita la creación eficiente de aplicaciones de IA generativa con un fuerte enfoque en la privacidad y la seguridad. En el contexto de la recuperación de documentación, la generación aumentada de recuperación (RAG) es una característica fundamental. Utiliza bases de conocimiento para complementar las solicitudes de FM con información relevante desde el punto de vista contextual procedente de fuentes externas. Un índice de Amazon OpenSearch Serverless sirve como base de datos vectorial detrás de las bases de conocimiento de Amazon Bedrock. Esta integración se mejora mediante una ingeniería cuidadosa y rápida para minimizar las imprecisiones y garantizar que las respuestas estén ancladas en la documentación fáctica. Para las consultas de bases de datos, las máquinas virtuales de Amazon Bedrock transforman las consultas textuales en consultas SQL estructuradas e incorporan parámetros específicos. Esto permite la recuperación precisa de los datos de las bases

de datos administradas por las bases de datos de AWS Glue. Para estas consultas se utiliza Amazon Athena.

Para gestionar consultas más complejas, lograr respuestas integrales exige información procedente tanto de la documentación como de las bases de datos. Agents for Amazon Bedrock es una función de IA generativa que le ayuda a crear agentes autónomos que puedan entender tareas complejas y dividirlas en tareas más sencillas para su organización. La combinación de información obtenida de las tareas simplificadas, facilitada por los agentes autónomos de Amazon Bedrock, mejora la síntesis de la información y permite obtener respuestas más completas y exhaustivas. Este patrón demuestra cómo crear un asistente basado en chat mediante Amazon Bedrock y los servicios y funciones de IA generativa relacionados dentro de una solución automatizada.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Docker, instalado
- Kit de desarrollo en la nube de AWS (AWS CDK), instalado y arrancado en las regiones o `us-east-1` regiones de AWS `us-west-2`
- AWS CDK Toolkit versión 2.114.1 o posterior, instalada
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada
- Python versión 3.11 o posterior, instalada
- En Amazon Bedrock, habilite el acceso a Claude 2, Claude 2.1, Claude Instant y Titan Embeddings G1 — Text

Limitaciones

- Esta solución se implementa en una única cuenta de AWS.
- Esta solución solo se puede implementar en las regiones de AWS en las que se admiten Amazon Bedrock y Amazon OpenSearch Serverless. Para obtener más información, consulte la documentación de Amazon Bedrock y Amazon OpenSearch Serverless.

Versiones de producto

- LLAMA-index versión 0.10.6 o posterior

- Sqlalchemy versión 2.0.23 o posterior
- OpenSearch-py versión 2.4.2 o posterior
- Requests_AWS4Auth versión 1.2.3 o posterior
- AWS SDK para Python (Boto3) versión 1.34.57 o posterior

Arquitectura

Pila de tecnología de destino

El AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software de código abierto para definir la infraestructura de nube en el código y aprovisionarla a través de AWS. CloudFormation La pila de CDK de AWS utilizada en este patrón implementa los siguientes recursos de AWS:

- AWS Key Management Service (AWS KMS)
- Amazon Simple Storage Service (Amazon S3)
- Catálogo de datos de AWS Glue, para el componente de base de datos de AWS Glue
- AWS Lambda
- AWS Identity y Access Management (IAM)
- Amazon OpenSearch Serverless
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon Elastic Container Service (Amazon ECS)
- AWS Fargate
- Amazon Virtual Private Cloud (Amazon VPC)
- Equilibrador de carga de aplicación

Arquitectura de destino

El diagrama muestra una completa configuración nativa de la nube de AWS en una sola región de AWS, que utiliza varios servicios de AWS. La interfaz principal del asistente basado en chat es una aplicación Streamlit alojada en un clúster de Amazon ECS. Un Application Load Balancer gestiona la accesibilidad. Las consultas realizadas a través de esta interfaz activan la función `Invocation`

Lambda, que luego interactúa con los agentes de Amazon Bedrock. Este agente responde a las consultas de los usuarios consultando las bases de conocimiento de Amazon Bedrock o invocando una función LambdaAgent executor. Esta función desencadena un conjunto de acciones asociadas al agente, siguiendo un esquema de API predefinido. Las bases de conocimiento de Amazon Bedrock utilizan un índice OpenSearch sin servidor como base de base de datos vectorial. Además, la Agent executor función genera consultas SQL que se ejecutan en la base de datos de AWS Glue a través de Amazon Athena.

Herramientas

Servicios de AWS

- Amazon Athena es un servicio interactivo de consultas que le permite analizar datos directamente en Amazon Simple Storage Service (Amazon S3) usando SQL estándar.
- Amazon Bedrock es un servicio totalmente gestionado que pone a su disposición modelos básicos (FM) de alto rendimiento de las principales empresas emergentes de IA y Amazon a través de una API unificada.
- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura de la nube de AWS en código.
- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que le ayuda a interactuar con los servicios de AWS mediante comandos en su shell de línea de comandos.
- Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores escalable y rápido que ayuda a ejecutar, detener y administrar contenedores en un clúster.
- Elastic Load Balancing (ELB) distribuye el tráfico entrante de aplicaciones o redes entre varios destinos. Así, por ejemplo, puede distribuir el tráfico a través de instancias de Amazon Elastic Compute Cloud (Amazon EC2), contenedores y direcciones IP de una o varias zonas de disponibilidad.
- AWS Glue es un servicio de extracción, transformación y carga (ETL) completamente administrado. Ayuda a clasificar, limpiar, enriquecer y mover datos de forma fiable entre almacenes de datos y flujos de datos. Este patrón emplea un rastreador de AWS Glue y una tabla del catálogo de datos de AWS Glue.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.

- Amazon OpenSearch Serverless es una configuración sin servidor bajo demanda para Amazon OpenSearch Service. En este patrón, un índice OpenSearch sin servidor sirve como base de datos vectorial para las bases de conocimiento de Amazon Bedrock.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Otras herramientas

- Streamlit es un marco de Python de código abierto para crear aplicaciones de datos.

Repositorio de código

El código de este patrón está disponible en el GitHub genai-bedrock-agent-chatbotrepositorio. El repositorio de código contiene los siguientes archivos y carpetas:

- `assets`carpeta: los activos estáticos, como el diagrama de arquitectura y el conjunto de datos público.
- `code/lambdas/action-lambda`folder: el código de Python de la función Lambda que actúa como acción para el agente de Amazon Bedrock.
- `code/lambdas/create-index-lambda`folder: el código de Python de la función Lambda que crea el índice OpenSearch Serverless.
- `code/lambdas/invoke-lambda`folder: el código de Python de la función Lambda que invoca al agente Amazon Bedrock, al que se llama directamente desde la aplicación Streamlit.
- `code/lambdas/update-lambda`folder: el código de Python de la función Lambda que actualiza o elimina los recursos después de que los recursos de AWS se hayan implementado a través de la CDK de AWS.
- `code/layers/boto3_layer`folder: la pila de CDK de AWS que crea una capa de Boto3 que se comparte entre todas las funciones de Lambda.
- `code/layers/opensearch_layer`folder: la pila de CDK de AWS que crea una capa OpenSearch sin servidor que instala todas las dependencias para crear el índice.
- `code/streamlit-app`folder: el código Python que se ejecuta como imagen del contenedor en Amazon ECS
- `code/code_stack.py`— La CDK de AWS crea archivos de Python que crean recursos de AWS.
- `app.py`— Las CDK de AWS apilan archivos Python que implementan los recursos de AWS en la cuenta de AWS de destino.

- `requirements.txt`— La lista de todas las dependencias de Python que se deben instalar para la AWS CDK.
- `cdk.json`— El archivo de entrada para proporcionar los valores necesarios para crear los recursos. Además, en los `context/config` campos, puede personalizar la solución en consecuencia. Para obtener más información sobre la personalización, consulte la sección Información adicional.

Prácticas recomendadas

- El ejemplo de código que se proporciona aquí es únicamente para fines proof-of-concept (PoC) o piloto. Si desea llevar el código a producción, asegúrese de seguir las siguientes prácticas recomendadas:
  - Habilitar el registro de acceso a Amazon S3
  - Habilitar los registros de flujo de VPC
- Configure la supervisión y las alertas para las funciones de Lambda. Para obtener más información, consulte Supervisión y solución de problemas de funciones de Lambda. Para obtener información sobre las prácticas recomendadas, consulte las prácticas recomendadas para trabajar con las funciones de AWS Lambda.

Epics

Configure las credenciales de AWS en su estación de trabajo local

Tarea	Descripción	Habilidades requeridas
Exporte variables para la cuenta y la región.	Para proporcionar las credenciales de AWS para la CDK de AWS mediante variables de entorno, ejecute los siguientes comandos. `export CDK_DEFAU LT_ACCOUNT=<12-digit AWS account number>`	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`export CDK_DEFAU LT_REGION=<Region>`	
Configure el perfil con nombre de la CLI de AWS.	Para configurar el perfil con nombre de la CLI de AWS para la cuenta, siga las instrucciones de Configuración y configuración del archivo de credenciales.	AWS DevOps, DevOps ingeniero

Configure su entorno

Tarea	Descripción	Habilidades requeridas
Clona el repositorio en tu estación de trabajo local.	Para clonar el repositorio, ejecute el siguiente comando en su terminal. `git clone https://g ithub.com/awslabs/ genai-bedrock-agent- chatbot.git`	DevOps ingeniero, AWS DevOps
Configure el entorno virtual de Python.	Para configurar y activar el entorno virtual de Python, ejecute el siguiente comando. `cd genai-bedrock-agen t-chatbot python3 -m venv .venv source .venv/bin/ activate` Para configurar las dependenc ias necesarias, ejecute el siguiente comando.	DevOps ingeniero, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`pip3 install -r requirements.txt`	
Configure el entorno AWS CDK.	Para convertir el código en una CloudFormation plantilla de AWS, ejecute el comando`cdk synth`.	AWS DevOps, DevOps ingeniero

Configure e implemente la aplicación

Tarea	Descripción	Habilidades requeridas
Implementar recursos en la cuenta.	Para implementar recursos en la cuenta de AWS mediante la CDK de AWS, haga lo siguiente: 1. En la raíz del repositorio clonado, en el `cdk.json` archivo, introduzca las entradas para los parámetros de registro. Los valores de ejemplo son `INFO`,`DEBUG`,`WARN`, y`ERROR`. Estos valores definen los mensajes a nivel de registro para las funciones de Lambda y la aplicación Streamlit. 2. El `cdk.json` archivo de la raíz del repositorio clonado contiene el nombre de la CloudFormation pila	DevOps ingeniero, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	de AWS utilizada para la implementación. El nombre predeterminado de la pila es `chatbot-stack` . El nombre predeterminado del agente de Amazon Bedrock es `ChatbotBedrockAgent` y el alias predeterminado del agente de Amazon Bedrock es. `Chatbot_Agent` 3. Ejecute el `cdk deploy` comando para implementar los recursos. El `cdk deploy` comando usa construcciones de capa 3 para crear varias funciones Lambda para copiar documentos y archivos de conjuntos de datos CSV en depósitos de S3. También implement a el agente de Amazon Bedrock, las bases de conocimiento y la función `Action group` Lambda para el agente de Amazon Bedrock. 4. Inicie sesión en la consola de administración de AWS y, a continuación, abra la CloudFormation consola en https://console.aw	

Tarea	Descripción	Habilidades requeridas
	s.amazon.com/cloud formation/. 5. Confirme que la pila se implementó correctamente. Para obtener instrucciones, consulte Revisar la pila en la CloudFormation consola de AWS. Tras una implementación correcta, puede acceder a la aplicación de asistente basada en el chat mediante la URL proporcionada en la pestaña Resultados de la CloudForm ation consola.	

Limpie todos los recursos de AWS de la solución

Tarea	Descripción	Habilidades requeridas
Elimine los recursos de AWS.	Después de probar la solución, ejecute el comando para limpiar los recursos`cdk destroy`.	AWS DevOps, DevOps ingeniero

Recursos relacionados

Documentación de AWS

- Recursos de Amazon Bedrock:
  - Acceso a modelos
  - Parámetros de inferencia para modelos básicos

  - Agentes de Amazon Bedrock
  - Bases de conocimiento de Amazon Bedrock
- Creación de funciones de Lambda con Python
- Recursos de AWS CDK:
  - Comience a utilizar el AWS CDK
  - Solución de problemas comunes de AWS CDK
  - Trabajar con el CDK de AWS en Python
- Creador de aplicaciones de IA generativa en AWS

Otros recursos de AWS

- Motor vectorial para Amazon OpenSearch Serverless

Otros recursos

- LlamaIndex documentación
- Documentación simplificada

Información adicional

Personalice el asistente basado en el chat con sus propios datos

Para integrar sus datos personalizados para implementar la solución, siga estas pautas estructuradas. Estos pasos están diseñados para garantizar un proceso de integración eficiente y fluido, lo que le permitirá implementar la solución de manera efectiva con sus datos personalizados.

Para la integración de datos de la base de conocimientos

Preparación de datos

1. Localice el `assets/knowledgebase_data_source/` directorio.
2. Coloque el conjunto de datos en esta carpeta.

Ajustes de configuración

1. Abra el archivo `cdk.json`.

2. Navegue hasta el `context/configure/paths/knowledgebase_file_name` campo y, a continuación, actualícelo en consecuencia.
3. Navegue hasta el `bedrock_instructions/knowledgebase_instruction` campo y, a continuación, actualícelo para que refleje con precisión los matices y el contexto de su nuevo conjunto de datos.

Para la integración de datos estructurales

Organización de datos

1. Dentro del `assets/data_query_data_source/` directorio, cree un subdirectorio, como`tabular_data`.
2. Coloque el conjunto de datos estructurado (los formatos aceptables incluyen CSV, JSON, ORC y Parquet) en esta subcarpeta recién creada.
3. Si se está conectando a una base de datos existente, actualice la función `create_sql_engine()` `code/lambda/action-lambda/build_query_engine.py` para conectarse a su base de datos.

Actualizaciones de configuración y código

1. En el `cdk.json` archivo, actualice el `context/configure/paths/athena_table_data_prefix` campo para alinearlo con la nueva ruta de datos.
2. Realice la revisión `code/lambda/action-lambda/dynamic_examples.csv` incorporando nuevos ejemplos de conversión de texto a SQL que se correspondan con su conjunto de datos.
3. Revise `code/lambda/action-lambda/prompt_templates.py` para reflejar los atributos de su conjunto de datos estructurado.
4. En el `cdk.json` archivo, actualice el `context/configure/bedrock_instructions/action_group_description` campo para explicar el propósito y la funcionalidad de la función `Action group` Lambda.
5. En el `assets/agent_api_schema/artifacts_schema.json` archivo, explique las nuevas funcionalidades de la función `Action group` Lambda.

Actualización general

En el `cdk.json` archivo, en la `context/configure/bedrock_instructions/agent_instruction` sección, proporcione una descripción completa de la funcionalidad y el

propósito de diseño previstos por el agente de Amazon Bedrock, teniendo en cuenta los datos recién integrados.

Documente el conocimiento institucional a partir de las entradas de voz mediante Amazon Bedrock y Amazon Transcribe

Creado por Praveen Kumar Jeyarajan (AWS), Jundong Qiao (AWS), Megan Wu (AWS) y Rajiv Upadhyay (AWS)

Repositorio de código: genai-knowledge-capture	Entorno: PoC o piloto	Tecnologías: aprendizaje automático e inteligencia artificial; productividad empresarial; nativa de la nube
Servicios de AWS: Amazon Bedrock; AWS CDK; AWS Lambda; Amazon SNS; AWS Step Functions; Amazon Transcribe		

Resumen

Capturar el conocimiento institucional es fundamental para garantizar el éxito y la resiliencia de la organización. El conocimiento institucional representa la sabiduría, los conocimientos y las experiencias colectivos acumulados por los empleados a lo largo del tiempo, a menudo de naturaleza tácita y transmitidos de manera informal. Esta gran cantidad de información abarca enfoques únicos, mejores prácticas y soluciones para problemas complejos que podrían no estar documentados en otros lugares. Al formalizar y documentar este conocimiento, las empresas pueden preservar la memoria institucional, fomentar la innovación, mejorar los procesos de toma de decisiones y acelerar las curvas de aprendizaje de los nuevos empleados. Además, promueve la colaboración, empodera a las personas y cultiva una cultura de mejora continua. En última instancia, aprovechar el conocimiento institucional ayuda a las empresas a utilizar su activo más valioso, la inteligencia colectiva de su fuerza laboral, para superar los desafíos, impulsar el crecimiento y mantener una ventaja competitiva en entornos empresariales dinámicos.

Este patrón explica cómo captar el conocimiento institucional a través de grabaciones de voz de los empleados sénior. Utiliza Amazon Transcribe y Amazon Bedrock para la documentación y verificación sistemáticas. Al documentar este conocimiento informal, puede conservarlo y compartirlo

con otros grupos de empleados. Este esfuerzo apoya la excelencia operativa y mejora la eficacia de los programas de formación mediante la incorporación de los conocimientos prácticos adquiridos a través de la experiencia directa.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Docker, instalado
- Kit de desarrollo en la nube de AWS (AWS CDK) versión 2.114.1 o posterior, instalado y arrancado en las regiones de AWS `us-east-1` `us-west-2`
- AWS CDK Toolkit versión 2.114.1 o posterior, instalada
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada
- Python versión 3.12 o posterior, instalada
- Permisos para crear recursos de Amazon Transcribe, Amazon Bedrock, Amazon Simple Storage Service (Amazon S3) y AWS Lambda

Limitaciones

- Esta solución se implementa en una única cuenta de AWS.
- Esta solución solo se puede implementar en las regiones de AWS en las que estén disponibles Amazon Bedrock y Amazon Transcribe. Para obtener información sobre la disponibilidad, consulte la documentación de Amazon Bedrock y Amazon Transcribe.
- Los archivos de audio deben estar en un formato compatible con Amazon Transcribe. Para obtener una lista de los formatos compatibles, consulte Formatos multimedia en la documentación de Transcribe.

Versiones de producto

- AWS SDK para Python (Boto3) versión 1.34.57 o posterior
- LangChain versión 0.1.12 o posterior

Arquitectura

La arquitectura representa un flujo de trabajo sin servidor en AWS. AWS Step Functions organiza las funciones de Lambda para el procesamiento de audio, el análisis de texto y la generación de documentos. El siguiente diagrama muestra el flujo de trabajo de Step Functions, también conocido como máquina de estados.

Cada paso de la máquina de estados es gestionado por una función Lambda distinta. Los siguientes son los pasos del proceso de generación de documentos:

1. La función `preprocess` Lambda valida la entrada pasada a Step Functions y muestra todos los archivos de audio presentes en la ruta de la carpeta URI de Amazon S3 proporcionada. Las funciones Lambda descendentes del flujo de trabajo utilizan la lista de archivos para validar, resumir y generar el documento.
2. La función `transcribe` Lambda usa Amazon Transcribe para convertir archivos de audio en transcripciones de texto. Esta función Lambda es responsable de iniciar el proceso de transcripción y transformar con precisión la voz en texto, que luego se almacena para su posterior procesamiento.
3. La función `validate` Lambda analiza las transcripciones del texto y determina la relevancia de las respuestas a las preguntas iniciales. Al utilizar un modelo de lenguaje amplio (LLM) a través de Amazon Bedrock, identifica y separa las respuestas relacionadas con el tema de las respuestas no relacionadas con el tema.
4. La función `summarize` Lambda utiliza Amazon Bedrock para generar un resumen coherente y conciso de las respuestas relacionadas con el tema.
5. La función `generate` Lambda agrupa los resúmenes en un documento bien estructurado. Puede formatear el documento de acuerdo con plantillas predefinidas e incluir cualquier contenido o dato adicional necesario.
6. Si alguna de las funciones de Lambda falla, recibirá una notificación por correo electrónico a través de Amazon Simple Notification Service (Amazon SNS).

A lo largo de este proceso, AWS Step Functions se asegura de que cada función de Lambda se inicie en la secuencia correcta. Esta máquina de estados tiene la capacidad de procesamiento en paralelo para mejorar la eficiencia. Un bucket de Amazon S3 actúa como repositorio de

almacenamiento central y respalda el flujo de trabajo mediante la administración de los distintos formatos multimedia y de documentos involucrados.

Herramientas

Servicios de AWS

- Amazon Bedrock es un servicio totalmente gestionado que pone a su disposición modelos básicos (FM) de alto rendimiento de las principales empresas emergentes de IA y Amazon a través de una API unificada.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Step Functions es un servicio de orquestación sin servidor que le permite combinar funciones de Lambda AWS y otros servicios de AWS para crear aplicaciones esenciales desde el punto de vista empresarial.
- Amazon Transcribe es un servicio de reconocimiento de voz automático que utiliza modelos de aprendizaje automático para convertir audio en texto.

Otras herramientas

- LangChaines un marco para desarrollar aplicaciones que funcionan con modelos de lenguaje de gran tamaño (LLM).

Repositorio de código

El código de este patrón está disponible en el GitHub genai-knowledge-capturerepositorio.

El repositorio de código contiene los siguientes archivos y carpetas:

- `assets`carpeta: los activos estáticos de la solución, como el diagrama de arquitectura y el conjunto de datos público
- `code/lambdas`folder: el código de Python para todas las funciones de Lambda
  - `code/lambdas/generate`carpeta: el código Python que genera un documento a partir de los datos resumidos en el depósito de S3
  - `code/lambdas/preprocess`folder: el código Python que procesa las entradas de la máquina de estados Step Functions
  - `code/lambdas/summarize`folder: el código Python que resume los datos transcritos mediante el servicio Amazon Bedrock
  - `code/lambdas/transcribe`carpeta: el código Python que convierte los datos de voz (archivo de audio) en texto mediante Amazon Transcribe
  - `code/lambdas/validate`carpeta: el código de Python que valida si todas las respuestas pertenecen al mismo tema
- `code/code_stack.py`— El archivo Python de construcción de AWS CDK que se utiliza para crear recursos de AWS
- `app.py`— El archivo Python de la aplicación AWS CDK que se utiliza para implementar los recursos de AWS en la cuenta de AWS de destino
- `requirements.txt`— La lista de todas las dependencias de Python que se deben instalar para la AWS CDK
- `cdk.json`— El archivo de entrada para proporcionar los valores necesarios para crear recursos

Prácticas recomendadas

El ejemplo de código proporcionado es únicamente para fines proof-of-concept (PoC) o piloto. Si desea llevar la solución a producción, utilice las siguientes prácticas recomendadas:

- Habilitar el registro de acceso a Amazon S3
- Habilitar los registros de flujo de VPC

Epics

Configure las credenciales de AWS en su estación de trabajo local

Tarea	Descripción	Habilidades requeridas
Exporte variables para la cuenta y la región de AWS.	Para proporcionar las credenciales de AWS para la CDK de AWS mediante variables de entorno, ejecute los siguientes comandos. `export CDK_DEFAU LT_ACCOUNT=<12-digit AWS account number> export CDK_DEFAU LT_REGION=<Region>`	AWS DevOps, DevOps ingeniero
Configure el perfil con nombre de la CLI de AWS.	Para configurar el perfil con nombre de la CLI de AWS para la cuenta, siga las instrucciones de Configuración y configuración del archivo de credenciales.	AWS DevOps, DevOps ingeniero

Configure su entorno

Tarea	Descripción	Habilidades requeridas
Clona el repositorio en tu estación de trabajo local.	Para clonar el genai-knowledge-capturerepositorio, ejecute el siguiente comando en su terminal. `git clone https://github.com/aws-samp`	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`les/genai-knowledge-capture`	
(Opcional) Sustituya los archivos de audio.	Para personalizar la aplicación de ejemplo para que incorpore sus propios datos, haga lo siguiente: 1. Navegue hasta la `assets/audio_samples` carpeta del repositorio clonado. 2. Elimine las carpetas que contienen los archivos de audio de muestra. 3. Cree una carpeta para cada tema que desee analizar. 4. Transfiera sus archivos de audio a sus carpetas respectivas.	AWS DevOps, DevOps ingeniero
Configure el entorno virtual de Python.	Para configurar y activar el entorno virtual de Python, ejecute el siguiente comando. `cd genai-knowledge-capture` `python3 -m venv .venv` `source .venv/bin/activate` `pip install -r requirements.txt`	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Sintetice el código CDK de AWS.	Para convertir el código en una configuración de CloudFormation pila de AWS, ejecute el siguiente comando. `cdk synth`	AWS DevOps, DevOps ingeniero

Configure e implemente la solución

Tarea	Descripción	Habilidades requeridas
Aprovisione el acceso al modelo básico.	Habilite el acceso al modelo Anthropic Claude 3 Sonnet para su cuenta de AWS. Para obtener instrucciones, consulte Añadir un modelo de acceso en la documentación de Bedrock.	AWS DevOps
Implementar recursos en la cuenta.	Para implementar recursos en la cuenta de AWS mediante la CDK de AWS, haga lo siguiente: 1. (Opcional) En la raíz del repositorio clonado, en el `app.py` archivo, actualiza el nombre de la CloudFormation pila de AWS. El nombre predeterminado de la pila es `genai-knowledge-capture-stack` .	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	2. Ejecute el `cdk deploy` comando para implementar los recursos. El `cdk deploy` comando usa construcciones de capa 3 para crear un conjunto de funciones Lambda, un bucket de S3, un tema de Amazon SNS y una máquina de estados Step Functions. Los archivos de audio de la `assets/audio_samples` carpeta se copian en el bucket de S3 durante la implement ación. 3. Inicie sesión en la consola de administración de AWS y, a continuación, abra la CloudFormation consola en https://console.aws.amazon.com/cloudformation/. 4. Confirme que la pila se implementó correctamente. Para obtener instrucciones, consulte Revisar la pila en la CloudFormation consola de AWS.	

Tarea	Descripción	Habilidades requeridas
Suscríbase al tema de Amazon SNS.	Para suscribirse al tema de Amazon SNS para recibir notificaciones, haga lo siguiente: 1. En la CloudFormation consola, en el panel de navegación, selecciona Stacks. 2. Elige la `genai-knowledge-capture-stack` pila. 3. Elija la pestaña Salidas. 4. Busque el nombre del tema de Amazon SNS con la clave. `SNSTopicName` 5. Configure una dirección de correo electrónico para recibir notificaciones siguiendo las instrucciones del tema Suscribir una dirección de correo electrónico a un tema de Amazon SNS.	AWS general

Pruebe la solución

Tarea	Descripción	Habilidades requeridas
Ejecuta la máquina de estado.	1. Abra la consola de Step Functions. 2. En la página State machines, elija genai-kno	Desarrollador de aplicaciones, AWS general

Tarea	Descripción	Habilidades requeridas
	wledge-capture-stack-state-machine. 3. Seleccione Iniciar ejecución. 4. (Opcional) En el cuadro Nombre, introduzca un nombre para la ejecución. 5. En el área de entrada, introduzca el siguiente objeto JSON sustituyendo el texto del marcador de posición, donde: • <Name>es el nombre que desea asignar al documento. • <S3 bucket name>es el nombre del depósito de Amazon S3 que contiene los archivos de audio. • <Folder path>es el directorio que contiene los archivos de audio. `{ "documentName": "<Name>", "audioFileFolderUri": "s3://<S3 bucket name>/<Folder path>" }` 6. Seleccione Iniciar ejecución. 7. En la página de detalles de la ejecución, revise los	

Tarea	Descripción	Habilidades requeridas
	resultados y espere a que se complete la ejecución.	

Limpie todos los recursos de AWS de la solución

Tarea	Descripción	Habilidades requeridas
Elimine los recursos de AWS.	Después de probar la solución, limpie los recursos: 1. Elimine todos los objetos del depósito de S3 y, a continuación, elimine el depósito. Para obtener más información, consulte Eliminación de un bucket. 2. Desde el repositorio clonado, ejecute el comando`cdk destroy`.	AWS DevOps, DevOps ingeniero

Recursos relacionados

Documentación de AWS

- Recursos de Amazon Bedrock:
  - Acceso a modelos
  - Parámetros de inferencia para modelos básicos
- Recursos de AWS CDK:
  - Comience a utilizar el AWS CDK
  - Trabajar con el CDK de AWS en Python
  - Solución de problemas comunes de AWS CDK
  - Comandos del kit de herramientas
- Recursos de AWS Step Functions:

  - Introducción a AWS Step Functions
  - Solución de problemas
- Creación de funciones de Lambda con Python
- Creador de aplicaciones de IA generativa en AWS

Otros recursos

- LangChain documentación

Genere recomendaciones personalizadas y reclasificadas con Amazon Personalize

Creado por Mason Cahill (AWS), Matthew Chasse (AWS) y Tayo Olajide (AWS)

Repositorio de código: personalize-pet-recommendations	Entorno: PoC o piloto	Tecnologías: aprendizaje automático e inteligencia artificial; nativas de la nube; infraestructura DevOps; sin servidor
Carga de trabajo: código abierto	Servicios de AWS: AWS CloudFormation; Amazon Kinesis Data Firehose; AWS Lambda; Amazon Personalize; AWS Step Functions	

Resumen

Este patrón le muestra cómo usar Amazon Personalize para generar recomendaciones personalizadas, incluidas las recomendaciones reclasificadas, para sus usuarios en función de la ingesta de datos de interacción de los usuarios en tiempo real por parte de esos usuarios. El escenario de ejemplo utilizado en este patrón se basa en un sitio web de adopción de mascotas que genera recomendaciones para sus usuarios en función de sus interacciones (por ejemplo, qué mascotas visita un usuario). Siguiendo el escenario de ejemplo, aprenderá a utilizar Amazon Kinesis Data Streams para ingerir datos de interacción, AWS Lambda para generar recomendaciones y reordenar las recomendaciones, y Amazon Data Firehose para almacenar los datos en un bucket de Amazon Simple Storage Service (Amazon S3). También aprenderá a usar AWS Step Functions para crear una máquina de estados que administre la versión de la solución (es decir, un modelo entrenado) que genera sus recomendaciones.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa con un AWS Cloud Development Kit (AWS CDK) arrancado.

- Interfaz de la línea de comandos de AWS (AWS CLI) con credenciales configuradas
- Python 3.9

Versiones de producto

- Python 3.9
- CDK de AWS 2.23.0 o posterior
- AWS SDK: 2.7.27 o posterior

Arquitectura

Pila de tecnología

- Amazon Data Firehose
- Amazon Kinesis Data Streams
- Amazon Personalize
- Amazon Simple Storage Service (Amazon S3)
- AWS Cloud Development Kit (AWS CDK)
- Interfaz de la línea de comandos de AWS (AWS CLI)
- AWS Lambda
- AWS Step Functions

Arquitectura de destino

El siguiente diagrama ilustra una canalización para incorporar datos en tiempo real a Amazon Personalize. Luego, la canalización utiliza esos datos para generar recomendaciones personalizadas y reclasificadas para los usuarios.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Kinesis Data Streams ingiere datos de usuarios en tiempo real (por ejemplo, eventos como visitas de mascotas) para que Lambda y Firehose los procesen.

2. Una función de Lambda procesa los registros de flujo de datos de Kinesis y realiza una llamada a la API para añadir la interacción del usuario en el registro a un rastreador de eventos de Amazon Personalize.
3. Una regla basada en el tiempo invoca un equipo de estados de Step Functions y genera nuevas versiones de soluciones para los modelos de recomendación y reclasificación mediante los eventos del rastreador de eventos de Amazon Personalize.
4. El equipo de estados actualiza las campañas de Amazon Personalize para usar la nueva versión de la solución.
5. Lambda cambia el orden de la lista de artículos recomendados mediante la campaña Amazon Personalize de reclasificación.
6. Lambda devuelve la lista de artículos recomendados mediante la campaña de recomendaciones de Amazon Personalize.
7. Firehose guarda los eventos en un bucket de S3 donde se puede acceder a ellos como datos históricos.

Herramientas

Herramientas de AWS

- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura de la nube de AWS en código.
- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.
- Amazon Data Firehose le ayuda a entregar datos de streaming en tiempo real a otros servicios de AWS, puntos de enlace HTTP personalizados y puntos de enlace HTTP propiedad de proveedores de servicios externos compatibles.
- Amazon Kinesis Data Streams le ayuda a recopilar y procesar grandes secuencias de registros de datos en tiempo real.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Personalize es un servicio de machine learning (ML) totalmente gestionado que le ayuda a generar recomendaciones de artículos para sus usuarios en función de sus datos.

- AWS Step Functions es un servicio de orquestación sin servidor que le permite combinar funciones de Lambda y otros servicios de AWS para crear aplicaciones esenciales desde el punto de vista empresarial.

Otras herramientas

- pytest es un marco de Python para escribir pruebas pequeñas y legibles.
- Python es un lenguaje de programación informático de uso general.

Código

El código de este patrón está disponible en el repositorio GitHub Animal Recommender. Puede usar la CloudFormation plantilla de AWS de este repositorio para implementar los recursos de la solución de ejemplo.

Nota: Las versiones de la solución Amazon Personalize, el rastreador de eventos y las campañas están respaldadas por recursos personalizados (dentro de la infraestructura) que amplían CloudFormation los recursos nativos.

Epics

Creación de la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree un entorno Python aislado.	Configuración de Mac/Linux 1. Para crear manualmente un entorno virtual, ejecute el comando `$ python3 -m venv .venv` desde su terminal. 2. Una vez finalizado el proceso de inicio, ejecute el comando `$ source .venv/bin/activate` para activar el entorno virtual.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Configuración en Windows Para crear manualmente un entorno virtual, ejecute el comando `% .venv\Scripts\activate.bat` desde su terminal.	

Tarea	Descripción	Habilidades requeridas
Sintetiza la CloudFormation plantilla.	1. Ejecute el comando `$ pip install -r requirements.txt` desde su terminal para asegurarse de que dispone de todas las dependencias necesarias. 2. En el shell de la CLI de AWS, configure las siguientes variables de entorno: • `export ACCOUNT_ID=123456789` • `export CDK_DEPLOY_REGION=us-east-1` • `export CDK_ENVIRONMENT=dev` 3. En el archivo `config/{env}.yml` , actualice `vpcId` para que coincida con su ID de nube privada virtual (VPC). 4. Para sintetizar la CloudFormation plantilla de este código, ejecute el `$ cdk synth` comando. Nota: En el paso 2, `CDK_ENVIRONMENT` hace referencia al archivo `config/{env}.yml` .	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Implemente recursos y cree infraestructura.	Desde su terminal, ejecute el comando `./deploy.sh` para implementar todos los recursos. Este script instala las dependencias requerida s de Python. Un script de Python crea un bucket de S3 y una clave de AWS Key Management Service (AWS KMS) y, a continuación, agrega los datos de base para las creaciones iniciales del modelo. Por último, el script se ejecuta `cdk deploy` para crear la infraestructura restante. Nota: El entrenamiento inicial del modelo se lleva a cabo durante la creación de la pila. La pila puede tardar hasta dos horas en terminar de crearse.	DevOps ingeniero

Recursos relacionados

- Recomendador de animales () GitHub
- Documentación de referencia de AWS SDK
- Documentación de Boto3
- Optimice las recomendaciones personalizadas para una métrica empresarial de su elección con Amazon Personalize (blog de AWS Machine Learning)

Información adicional

Ejemplos de cargas útiles y respuestas

Función de Lambda de recomendación

Para recuperar las recomendaciones, envíe una solicitud a la función de Lambda de recomendaciones con una carga útil en el siguiente formato:

```
{
  "userId": "3578196281679609099",
  "limit": 6
}
```

El siguiente ejemplo de respuesta contiene una lista de grupos de animales:

```
[{"id": "1-domestic short hair-1-1"},
{"id": "1-domestic short hair-3-3"},
{"id": "1-domestic short hair-3-2"},
{"id": "1-domestic short hair-1-2"},
{"id": "1-domestic short hair-3-1"},
{"id": "2-beagle-3-3"},
```

Si omite el campo `userId`, la función devuelve recomendaciones generales.

Reordenación de la función de Lambda

Para utilizar la reclasificación, envíe una solicitud a la función de Lambda de reclasificación. La carga útil contiene el `userId` todos los identificadores de los elementos que se van a reclasificar y sus metadatos. Los siguientes datos de ejemplo utilizan las clases de Oxford Pets para `animal_species_id` (1=gato, 2=perro) y los números enteros del 1 al 5 para `animal_age_id` y `animal_size_id`:

```
{
   "userId":"12345",
   "itemMetadataList":[
      {
         "itemId":"1",
         "animalMetadata":{
            "animal_species_id":"2",
            "animal_primary_breed_id":"Saint_Bernard",
```

```
            "animal_size_id":"3",
            "animal_age_id":"2"
         }
      },
      {
         "itemId":"2",
         "animalMetadata":{
            "animal_species_id":"1",
            "animal_primary_breed_id":"Egyptian_Mau",
            "animal_size_id":"1",
            "animal_age_id":"1"
         }
      },
      {
         "itemId":"3",
         "animalMetadata":{
            "animal_species_id":"2",
            "animal_primary_breed_id":"Saint_Bernard",
            "animal_size_id":"3",
            "animal_age_id":"2"
         }
      }
   ]
}
```

La función de Lambda vuelve a clasificar estos artículos y, a continuación, devuelve una lista ordenada que incluye los ID de los artículos y la respuesta directa de Amazon Personalize. Esta es una lista ordenada de los grupos de animales en los que se encuentran los artículos y su puntuación. Amazon Personalize utiliza recetas de Personalización por usuario y Clasificación personalizada para incluir una puntuación para cada artículo en las recomendaciones. Estas puntuaciones representan la certeza relativa que tiene Amazon Personalize respecto a qué elemento va a seleccionar el usuario a continuación. Las puntuaciones más altas representan una mayor certeza.

```
{
   "ranking":[
      "1",
      "3",
      "2"
   ],
   "personalizeResponse":{
      "ResponseMetadata":{
         "RequestId":"a2ec0417-9dcd-4986-8341-a3b3d26cd694",
```

```
         "HTTPStatusCode":200,
         "HTTPHeaders":{
            "date":"Thu, 16 Jun 2022 22:23:33 GMT",
            "content-type":"application/json",
            "content-length":"243",
            "connection":"keep-alive",
            "x-amzn-requestid":"a2ec0417-9dcd-4986-8341-a3b3d26cd694"
         },
         "RetryAttempts":0
      },
      "personalizedRanking":[
         {
            "itemId":"2-Saint_Bernard-3-2",
            "score":0.8947961
         },
         {
            "itemId":"1-Siamese-1-1",
            "score":0.105204
         }
      ],
      "recommendationId":"RID-d97c7a87-bd4e-47b5-a89b-ac1d19386aec"
   }
}
```

Carga de Amazon Kinesis

La carga que se va a enviar a Amazon Kinesis tiene el formato siguiente:

```
{
    "Partitionkey": "randomstring",
    "Data": {
        "userId": "12345",
        "sessionId": "sessionId4545454",
        "eventType": "DetailView",
        "animalMetadata": {
            "animal_species_id": "1",
            "animal_primary_breed_id": "Russian_Blue",
            "animal_size_id": "1",
            "animal_age_id": "2"
        },
        "animal_id": "98765"

    }
```

```
}
```

Nota: El campo `userId` se elimina para un usuario no autenticado.

Entrena e implementa un modelo de aprendizaje automático personalizado compatible con GPU en Amazon SageMaker

Entorno: PoC o piloto	Tecnologías: machine learning e IA; contenedores y microservicios	Servicios de AWS: Amazon ECS; Amazon SageMaker

Resumen

El entrenamiento y la implementación de un modelo de machine learning (ML) compatible con unidades de procesamiento de gráficos (GPU) requieren de la configuración e inicialización de determinadas variables de entorno para aprovechar al máximo las ventajas de las GPU NVIDIA. Sin embargo, configurar el entorno y hacerlo compatible con la SageMaker arquitectura de Amazon en la nube de Amazon Web Services (AWS) puede llevar mucho tiempo.

Este patrón te ayuda a entrenar y crear un modelo de aprendizaje automático personalizado compatible con GPU mediante Amazon. SageMaker Proporciona los pasos para entrenar e implementar un CatBoost modelo personalizado creado a partir de un conjunto de datos de Amazon reviews de código abierto. Podrá comparar su rendimiento en una instancia `p3.16xlarge` de Amazon Elastic Compute Cloud (Amazon EC2).

Este patrón es útil si tu organización quiere implementar modelos de aprendizaje automático compatibles con la GPU existentes en él. SageMaker Sus científicos de datos pueden seguir los pasos de este patrón para crear contenedores compatibles con las GPU de NVIDIA e implementar modelos de ML en dichos contenedores.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Un bucket de origen de Amazon Simple Storage Service (Amazon S3) para almacenar artefactos y predicciones del modelo.
- Conocimiento de las instancias de cuadernos y de los SageMaker cuadernos de Jupyter.

- Comprensión de cómo crear un rol de AWS Identity and Access Management (IAM) con permisos de SageMaker rol básicos, permisos de acceso y actualización al bucket de S3 y permisos adicionales para Amazon Elastic Container Registry (Amazon ECR).

Limitaciones

- Este patrón está diseñado para cargas de trabajo de aprendizaje supervisadas con código de entrenamiento e implementación en Python.

Arquitectura

Pila de tecnología

- SageMaker
- Amazon ECR

Herramientas

Herramientas

- Amazon ECR: Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado por AWS que es seguro, escalable y fiable.
- Amazon SageMaker: SageMaker es un servicio de aprendizaje automático totalmente gestionado.
- Docker: Docker es una plataforma de software para crear, probar e implementar aplicaciones rápidamente.
- Python: es un lenguaje de programación.

Código

El código de este patrón está disponible en el repositorio GitHub Implementación de un modelo de clasificación de reseñas con Catboost y el SageMaker repositorio.

Epics

Prepare los datos

Tarea	Descripción	Habilidades requeridas
Cree un rol de IAM y adjunte las políticas necesarias.	Inicie sesión en la consola de administración de AWS, abra la consola de IAM y cree el rol de IAM. Adjunte las políticas siguientes al rol de IAM: • `AmazonEC2ContainerRegistryFullAccess` • `AmazonS3FullAccess` • `AmazonSageMakerFullAccess` Para obtener más información al respecto, consulta Crear una instancia de bloc de notas en la SageMaker documentación de Amazon.	Científico de datos
Cree la instancia de SageMaker bloc de notas.	Abre la SageMaker consola, selecciona Instancias de Notebook y, a continuación, selecciona Crear instancia de Notebook. En Rol de IAM, seleccione el rol de IAM que creó anteriormente. Configure la instancia de cuaderno según sus necesidades y seleccione Crear instancia de cuaderno.	Científico de datos

Tarea	Descripción	Habilidades requeridas
	Para obtener instrucciones y pasos detallados, consulta Crear una instancia de bloc de notas en la SageMaker documentación de Amazon.	
Clonar el repositorio.	Abre el terminal en la instancia del SageMaker portátil y clona el SageMaker repositorio GitHub Implementación de un modelo de clasificación de reseñas con Catboost y ejecuta el siguiente comando: `git clone https://github.com/aws-samples/review-classification-using-catboost-sagemaker.git`	
Inicio del servidor de cuaderno de Jupyter.	Inicie el cuaderno de Jupyter `Review classification model with Catboost and SageMaker.ipynb` , que contiene los pasos predefinidos.	Científico de datos

Ingeniería de características

Tarea	Descripción	Habilidades requeridas
Ejecute comandos en el cuaderno de Jupyter.	Abra el cuaderno de Jupyter y ejecute los comandos de las siguientes historias para preparar los datos que	Científico de datos

Tarea	Descripción	Habilidades requeridas
	entrenarán a su modelo de ML.	
Lea los datos del bucket de S3.	`import pandas as pd` `import csv` `fname = 's3://ama` `zon-reviews-pds/ts` `v/amazon_reviews_u` `s_Digital_Video_Do` `wnload_v1_00.tsv.gz'` `df = pd.read_csv(fname,` `sep='\t',delimiter` `='\t',error_bad_li` `nes=False)`	Científico de datos

Tarea	Descripción	Habilidades requeridas
Preprocese los datos.	`import numpy as np` `def pre_process(df):` `  df.fillna(value={'` `review_body': '',` `'review_headline':` `''}, inplace=True)` `df.fillna( value={'v` `erified_purchase':` `'Unk'}, inplace=True)` `df.fillna(0,` `inplace=True)` `return df` `df = pre_process(df)` `df.review_date =` `pd.to_datetime(df.` `review_date)` `df['target'] =` `np.where(df['star_` `rating']>=4,1,0)` Nota: Este código reemplaza los valores nulos de `'review_body'` por una cadena vacía, y reemplaza la columna `'verified_purchase'` por `'Unk'`, que significa “desconocido”.	Científico de datos

Tarea	Descripción	Habilidades requeridas
Divida los datos en conjuntos de datos de entrenamiento, validación y prueba.	Para mantener la distribución de la etiqueta de destino idéntica en los conjuntos divididos, debe estratificar el muestreo mediante la biblioteca scikit-learn. `from sklearn.model_selection import StratifiedShuffleSplit` `sss = StratifiedShuffleSplit(n_splits=2, test_size=0.10, random_state=0)` `sss.get_n_splits(df, df['target'])` `for train_index, test_index in sss.split(df, df['target']):` `  X_train_vallid , X_test = df.iloc[train_index], df.iloc[test_index]` `sss.get_n_splits(X_train_vallid, X_train_vallid['target'])` `for train_index, test_index in sss.split(X_train_vallid, X_train_vallid['target']):` `  X_train , X_valid = X_train_vallid.iloc[train_index],`	Científico de datos

Tarea	Descripción	Habilidades requeridas
	`X_train_vallid.ilo c[test_index]`	

Cree, ejecute y envíe la imagen de Docker a Amazon ECR

Tarea	Descripción	Habilidades requeridas
Cree y envíe imágenes de Docker.	En el cuaderno de Jupyter, ejecute los comandos de las siguientes historias para preparar la imagen de Docker e insertarla en Amazon ECR.	Ingeniero de ML
Cree un repositorio en Amazon ECR.	`%%sh` `algorithm_name=s agemaker-catboost- github-gpu-img` `chmod +x code/train` `chmod +x code/serve` `account=$(aws sts get- caller-identity -- query Account --output text)` `# Get the region defined in the current configuration (default to us-west-2 if none defined)` `region=$(aws configure get region)` `region=${region:-us- east-1}`	Ingeniero de ML

Tarea	Descripción	Habilidades requeridas
	`fullname="${accou nt}.dkr.ecr.${regi on}.amazonaws.com/ ${algorithm_name}: latest"` `aws ecr create-re pository --repository- name "${algorithm_name} " > /dev/nul`	
Cree una imagen de Docker de forma local.	`docker build -t "${algorithm_name}" . docker tag ${algorit hm_name} ${fullname}`	Ingeniero de ML
Ejecute la imagen de Docker y envíela a Amazon ECR.	`docker push ${fullname}`	Ingeniero de ML

Formación

Tarea	Descripción	Habilidades requeridas
Cree un trabajo de ajuste de SageMaker hiperparámetros.	En el cuaderno de Jupyter, ejecute los comandos de las siguientes historias para crear un trabajo de ajuste de SageMaker hiperparámetros con su imagen de Docker.	Científico de datos
Crea un estimador. SageMaker	Cree un SageMaker estimador con el nombre de la imagen de Docker. `import sagemaker as sage from time import gmtime, strftime`	Científico de datos

Tarea	Descripción	Habilidades requeridas
	sess = sage.Session() from sagemaker.tuner import IntegerPa rameter, Categoric alParameter, Continuou sParameter, Hyperpara meterTuner account = sess.boto _session.client('s ts').get_caller_id entity()['Account'] region = sess.boto _session.region_name image = '{}.dkr.e cr.{}.amazonaws.co m/sagemaker-catboo st-github-gpu-img: latest'.format(acc ount, region) tree_hpo = sage.esti mator.Estimator(im age, role, 1, 'ml.p3.16xlarge', train_volume_size = 100, output_path="s3:// {}/sagemaker/DEMO- GPU-Catboost/outpu t".format(bucket), sagemaker_session= sess)	

Tarea	Descripción	Habilidades requeridas
Cree un trabajo de HPO.	Cree un trabajo de ajuste de optimización de hiperpará metros (HPO) con rangos de parámetros y pase el tren y los conjuntos de validación como parámetros a la función. `hyperparameter_ran ges = {'iterations': IntegerParameter(8 0000, 130000),` `'max_depth': IntegerPa rameter(6, 10),` `'max_ctr_complexity': IntegerParameter(4, 10),` `'learning_rate': ContinuousParamete r(0.01, 0.5)}` `objective_metric_name = 'auc' metric_definitions = [{'Name': 'auc',` `'Regex': 'auc: ([0-9\ \.]+)'}]` `tuner = Hyperpara meterTuner(tree_hpo,` `objective_metric_n ame,` `hyperparameter_ran ges,`	Científico de datos

Tarea	Descripción	Habilidades requeridas
	`metric_definitions,` `objective_type='Maximize',` `max_jobs=50,` `max_parallel_jobs=2)`	
Ejecute el trabajo de HPO.	`train_location = 's3://'+bucket+'/sagemaker/DEMO-GPU-Catboost/data/train/'` `valid_location = 's3://'+bucket+'/sagemaker/DEMO-GPU-Catboost/data/valid/'` `tuner.fit({'train': train_location, 'validation': valid_location})`	Científico de datos
Reciba el trabajo de entrenamiento de mayor rendimiento.	`import sagemaker as sage` `from time import gmtime, strftime` `sess = sage.Session()` `best_job =tuner.best_training_job()`	Científico de datos

Transformación por lotes

Tarea	Descripción	Habilidades requeridas
Cree un trabajo de transformación SageMaker por lotes en los datos de las pruebas para la predicción del modelo.	En el cuaderno de Jupyter, ejecute los comandos de las siguientes historias para crear el modelo a partir de su trabajo de ajuste de SageMaker hiperparámetros y envíe un trabajo de transformación SageMaker por lotes con los datos de la prueba para la predicción del modelo.	Científico de datos
Cree el modelo. SageMaker	Cree un modelo dentro del SageMaker modelo utilizando el mejor trabajo de entrenamiento. `attached_estimator = sage.estimator.Estimator.attach(best_job)` `output_path ='s3://'+bucket+'/sagemaker/DEMO-GPU-Catboost/data/test-predictions/'` `input_path ='s3://'+bucket+'/sagemaker/DEMO-GPU-Catboost/data/test/'` `transformer = attached_estimator.transformer(instance_count=1,`	Científico de datos

Tarea	Descripción	Habilidades requeridas
	`instance_type='ml.p3.16xlarge', assemble_with='Line', accept='text/csv', max_payload=1, output_path=output_path, env = {'SAGEMAKER_MODEL_SERVER_TIMEOUT' : '3600' })`	
Crear trabajos de transformación por lotes.	Cree un trabajo de transformación por lotes en el conjunto de datos de prueba. `transformer.transform(input_path, content_type='text/csv', split_type='Line')`	Científico de datos

Analice los resultados

Tarea	Descripción	Habilidades requeridas
Lea los resultados y evalúe el rendimiento del modelo.	En el cuaderno de Jupyter, ejecute los comandos de las siguientes historias para leer los resultados y evaluar el rendimiento del modelo según las métricas del modelo Área bajo la curva ROC (ROC-AUC) y Área bajo la curva de recuperación de precisión (PR-AUC). Para obtener más información, consulte Conceptos clave de machine learning de Amazon en la documentación de Amazon Machine Learning (Amazon ML).	Científico de datos
Lea los resultados del trabajo de transformación por lotes.	Lea los resultados del trabajo de transformación por lotes en un marco de datos. `file_name = 's3://'+b ucket+'/sagemaker/ DEMO-GPU-Catboost/ data/test-predicti ons/file_1.out'` `results = pd.read_csv(file_n ame, names=['r eview_id','target' ,'score'] ,sep='\t' ,escapechar ='\\' , quoting=csv.QUOTE_ NONE,`	Científico de datos

Tarea	Descripción	Habilidades requeridas
	<pre>lineterminator='\n',quotechar='"').dropna()</pre>	

Tarea	Descripción	Habilidades requeridas
Evalúe las métricas de rendimiento.	Evalúe el rendimiento del modelo en ROC-AUC y PR-AUC. `from sklearn import metrics` `import matplotlib` `import pandas as pd` `matplotlib.use('agg', warn=False, force=True)` `from matplotlib import pyplot as plt` `%matplotlib inline` `def analyze_results(labels, predictions):` `precision, recall, thresholds = metrics.precision_recall_curve(labels, predictions)` `auc = metrics.auc(recall, precision)` `fpr, tpr, _ = metrics.roc_curve(labels, predictions)` `roc_auc_score = metrics.roc_auc_score(labels, predictions)` `print('Neural-Nets: ROC auc=%.3f' % ( roc_auc_score))` `plt.plot(fpr, tpr, label="data 1, auc=" + str(roc_auc_score))`	Científico de datos

Tarea	Descripción	Habilidades requeridas
	`    plt.xlabel('1-Specificity')` `    plt.ylabel('Sensitivity')` `    plt.legend(loc=4)` `    plt.show()` `    lr_precision, lr_recall, _ = metrics.precision_recall_curve(labels, predictions)` `    lr_auc = metrics.auc(lr_recall, lr_precision)` `    # summarize scores` `    print('Neural-Nets: PR auc=%.3f' % ( lr_auc))` `    # plot the precision-recall curves` `    no_skill = len(labels[labels==1.0]) / len(labels)` `    plt.plot([0, 1], [no_skill, no_skill], linestyle='--', label='No Skill')` `    plt.plot(lr_recall, lr_precision, marker='.', label='Neural-Nets')` `    # axis labels` `    plt.xlabel('Recall')` `    plt.ylabel('Precision')` `    # show the legend` `    plt.legend()` `    # show the plot`	

Tarea	Descripción	Habilidades requeridas
	plt.show() return auc analyze_results(results['target'].values,results['score'].values)	

Recursos relacionados

- Entrena y aloja modelos Scikit-Learn en Amazon SageMaker mediante la creación de un contenedor Scikit Docker

Información adicional

La siguiente lista muestra los diferentes elementos de Dockerfile que se ejecutan en la épica Compilar, ejecutar y enviar la imagen de Docker a Amazon ECR.

Instale Python con aws-cli.

```
FROM amazonlinux:1

 RUN yum update -y && yum install -y python36 python36-devel python36-libs python36-tools python36-pip && \
 yum install gcc tar make wget util-linux kmod man sudo git -y && \
 yum install wget -y && \
 yum install aws-cli -y && \
 yum install nginx -y && \
yum install gcc-c++.noarch -y && yum clean all
```

Instale los paquetes de Python

```
RUN pip-3.6 install --no-cache-dir --upgrade pip && \pip3 install --no-cache-dir --upgrade setuptools && \
```

```
pip3 install Cython && \
pip3 install --no-cache-dir numpy==1.16.0 scipy==1.4.1 scikit-learn==0.20.3
 pandas==0.24.2 \
flask gevent gunicorn boto3 s3fs  matplotlib joblib catboost==0.20.2
```

Instale CUDA y CuDNN

```
RUN wget https://developer.nvidia.com/compute/cuda/9.0/Prod/local_installers/
cuda_9.0.176_384.81_linux-run \
&& chmod u+x cuda_9.0.176_384.81_linux-run \
&& ./cuda_9.0.176_384.81_linux-run --tmpdir=/data --silent --toolkit --override \
&& wget https://custom-gpu-sagemaker-image.s3.amazonaws.com/installation/cudnn-9.0-
linux-x64-v7.tgz \
&& tar -xvzf cudnn-9.0-linux-x64-v7.tgz \
&& cp /data/cuda/include/cudnn.h /usr/local/cuda/include \
&& cp /data/cuda/lib64/libcudnn* /usr/local/cuda/lib64 \

&& chmod a+r /usr/local/cuda/include/cudnn.h /usr/local/cuda/lib64/libcudnn* \
&&  rm -rf /data/*
```

Cree la estructura de directorios requerida para SageMaker

```
RUN mkdir /opt/ml /opt/ml/input /opt/ml/input/config /opt/ml/input/data /opt/ml/input/
data/training /opt/ml/model /opt/ml/output /opt/program
```

Establezca las variables de entorno NVIDIA

```
ENV PYTHONPATH=/opt/program
ENV PYTHONUNBUFFERED=TRUE
ENV PYTHONDONTWRITEBYTECODE=TRUE
ENV PATH="/opt/program:${PATH}"

# Set NVIDIA mount environments
ENV LD_LIBRARY_PATH=/usr/local/nvidia/lib:/usr/local/nvidia/lib64:$LD_LIBRARY_PATH
ENV NVIDIA_VISIBLE_DEVICES="all"
ENV NVIDIA_DRIVER_CAPABILITIES="compute,utility"
ENV NVIDIA_REQUIRE_CUDA "cuda>=9.0"
```

Copie los archivos de entrenamiento e inferencia en la imagen de Docker

```
COPY code/* /opt/program/
```

```
WORKDIR /opt/program
```

Utilice el SageMaker procesamiento para la ingeniería de características distribuidas de conjuntos de datos de aprendizaje automático a escala de terabytes

Creado por Chris Boomhower (AWS)

Entorno: producción	Tecnologías: machine learning e inteligencia artificial; macrodatos	Servicios de AWS: Amazon SageMaker

Resumen

Muchos conjuntos de datos a escala de terabytes o más grandes suelen constar de una estructura jerárquica de carpetas y, en ocasiones, los archivos del conjunto de datos comparten interdependencias. Por este motivo, los ingenieros de machine learning (ML) y los científicos de datos deben tomar decisiones de diseño bien pensadas a fin de preparar dichos datos para el entrenamiento y la inferencia de modelos. Este patrón demuestra cómo puede utilizar técnicas manuales de macrofragmentación y microfragmentación en combinación con Amazon SageMaker Processing y la paralelización de CPU virtual (vCPU) para escalar de manera eficiente los procesos de ingeniería de características para conjuntos de datos de aprendizaje automático de big data complicados.

Este patrón define la macrofragmentación como la división de los directorios de datos en varias máquinas para su procesamiento, y la microfragmentación como la división de los datos de cada máquina en varios subprocesos de procesamiento. El patrón demuestra estas técnicas mediante el uso de Amazon SageMaker con ejemplos de registros de formas de onda de series temporales del conjunto de datos PhysioNet MIMIC-III. Al implementar las técnicas en este patrón, puede minimizar el tiempo y los costos de procesamiento de la ingeniería de características y, al mismo tiempo, maximizar la utilización de los recursos y la eficiencia del rendimiento. Estas optimizaciones se basan en el SageMaker procesamiento distribuido en las instancias y vCPU de Amazon Elastic Compute Cloud (Amazon EC2) para conjuntos de datos grandes y similares, independientemente del tipo de datos.

Requisitos previos y limitaciones

Requisitos previos

- Acceda a instancias de SageMaker notebook o a SageMaker Studio, si desea implementar este patrón en su propio conjunto de datos. Si es la primera vez que utiliza Amazon SageMaker , consulte Comenzar con Amazon SageMaker en la documentación de AWS.
- SageMaker Studio, si quiere implementar este patrón con los datos de muestra del PhysioNet MIMIC-III.
- El patrón usa SageMaker Processing, pero no requiere experiencia en la ejecución SageMaker de trabajos de Processing.

Limitaciones

- Este patrón se adapta bien a los conjuntos de datos de machine learning que incluyen archivos interdependientes. Estas interdependencias son las que más se benefician de la fragmentación manual de macros y de la ejecución en paralelo de varios trabajos de procesamiento de una sola instancia SageMaker . Para los conjuntos de datos en los que no existen dichas interdependencias, la `ShardedByS3Key` función de SageMaker procesamiento podría ser una mejor alternativa a la macrofragmentación, ya que envía los datos fragmentados a varias instancias administradas por el mismo trabajo de procesamiento. Sin embargo, puede implementar la estrategia de microfragmentación de este patrón en ambos escenarios para utilizar mejor las vCPU de instancia.

Versiones de producto

- Amazon SageMaker Python SDK versión 2

Arquitectura

Pila de tecnología de destino

- Amazon Simple Storage Service (Amazon S3)
- Amazon SageMaker

Arquitectura de destino

Macrofragmentación e instancias EC2 distribuidas

Los 10 procesos paralelos representados en esta arquitectura reflejan la estructura del conjunto de datos MIMIC-III. (Los procesos se representan mediante elipses para simplificar el diagrama). Cuando se utiliza la macrofragmentación manual, se aplica una arquitectura similar a cualquier conjunto de datos. En el caso de MIMIC-III, puede aprovechar la estructura sin procesar del conjunto de datos procesando la carpeta de cada grupo de pacientes por separado, con un esfuerzo mínimo. En el siguiente diagrama, el bloque de grupos de registros aparece a la izquierda (1). Dada la naturaleza distribuida de los datos, tiene sentido dividirlos por grupo de pacientes.

Sin embargo, la fragmentación manual por grupo de pacientes significa que se requiere un trabajo de procesamiento independiente para cada carpeta del grupo de pacientes, como puede ver en la sección central del diagrama (2), en lugar de un solo trabajo de procesamiento con varias instancias de EC2. Como los datos de MIMIC-III incluyen tanto archivos de forma de onda binarios como archivos de encabezados basados en texto coincidentes, y existe una dependencia obligatoria de la biblioteca wfdb para la extracción de datos binarios, todos los registros de un paciente específico deben estar disponibles en la misma instancia. La única forma de asegurarse de que el archivo de cabecera asociado a cada archivo de forma de onda binaria también esté presente es implementar la fragmentación manual para ejecutar cada fragmento dentro de su propio trabajo de procesamiento y especificar `s3_data_distribution_type='FullyReplicated'` cuándo se define la entrada del trabajo de procesamiento. Como alternativa, si todos los datos estuvieran disponibles en un único directorio y no existieran dependencias entre los archivos, una opción más adecuada podría ser lanzar un único trabajo de procesamiento con varias instancias de EC2 y se ha especificado `s3_data_distribution_type='ShardedByS3Key'`. Si `ShardedByS3Key` se especifica el tipo de distribución de datos de Amazon S3, se SageMaker gestionará automáticamente la fragmentación de datos en todas las instancias.

Lanzar un trabajo de procesamiento para cada carpeta es una forma rentable de preprocesar los datos, ya que la ejecución simultánea de varias instancias ahorra tiempo. Para ahorrar costos y tiempo adicionales, puede utilizar la microfragmentación en cada trabajo de procesamiento.

Microfragmentación y vCPU paralelas

Dentro de cada trabajo de procesamiento, los datos agrupados se dividen aún más para maximizar el uso de todas las vCPU disponibles en SageMaker la instancia EC2 totalmente gestionada. Los bloques de la sección central del diagrama (2) muestran lo que ocurre en cada trabajo de procesamiento principal. El contenido de las carpetas de registros de pacientes se aplana y se divide

de manera uniforme en función del número de vCPU disponibles en la instancia. Una vez dividido el contenido de la carpeta, el conjunto de archivos de tamaño uniforme se distribuye en todas las VCPU para su procesamiento. Cuando se completa el procesamiento, los resultados de cada vCPU se combinan en un único archivo de datos para cada trabajo de procesamiento.

En el código adjunto, estos conceptos se representan en la siguiente sección del archivo `src/feature-engineering-pass1/preprocessing.py`.

```
def chunks(lst, n):
    """
    Yield successive n-sized chunks from lst.

    :param lst: list of elements to be divided
    :param n: number of elements per chunk
    :type lst: list
    :type n: int
    :return: generator comprising evenly sized chunks
    :rtype: class 'generator'
    """
    for i in range(0, len(lst), n):
        yield lst[i:i + n]


# Generate list of data files on machine
data_dir = input_dir
d_subs = next(os.walk(os.path.join(data_dir, '.')))[1]
file_list = []
for ds in d_subs:
    file_list.extend(os.listdir(os.path.join(data_dir, ds, '.')))
dat_list = [os.path.join(re.split('_|\.', f)[0].replace('n', ''), f[:-4]) for f in
 file_list if f[-4:] == '.dat']

# Split list of files into sub-lists
cpu_count = multiprocessing.cpu_count()
splits = int(len(dat_list) / cpu_count)
if splits == 0: splits = 1
dat_chunks = list(chunks(dat_list, splits))

# Parallelize processing of sub-lists across CPUs
ws_df_list = Parallel(n_jobs=-1, verbose=0)(delayed(run_process)(dc) for dc in
 dat_chunks)

# Compile and pickle patient group dataframe
```

```
ws_df_group = pd.concat(ws_df_list)
ws_df_group = ws_df_group.reset_index().rename(columns={'index': 'signal'})
ws_df_group.to_json(os.path.join(output_dir, group_data_out))
```

Una función, `chunks`, se define primero para consumir una lista dada dividiéndola en trozos de longitud de tamaño uniforme `n` y devolviendo estos resultados como un generador. A continuación, los datos se agrupan en las carpetas de los pacientes mediante la compilación de una lista de todos los archivos de forma de onda binaria presentes. Una vez hecho esto, se obtiene la cantidad de vCPU disponibles en la instancia EC2. La lista de archivos de forma de onda binaria se divide equitativamente entre estas vCPU mediante una llamada de `chunks` y, a continuación, cada sublista de formas de onda se procesa en su propia vCPU mediante la clase Parallel de joblib. El trabajo de procesamiento combina automáticamente los resultados en una sola lista de marcos de datos, que SageMaker luego los procesa más antes de escribirlos en Amazon S3 al finalizar el trabajo. En este ejemplo, los trabajos de procesamiento escriben 10 archivos en Amazon S3 (uno para cada trabajo).

Cuando se hayan completado todos los trabajos de procesamiento iniciales, un trabajo de procesamiento secundario, que se muestra en el bloque a la derecha del diagrama (3), combina los archivos de salida generados por cada trabajo de procesamiento principal y escribe el resultado combinado en Amazon S3 (4).

Herramientas

Herramientas

- Python: el código de ejemplo utilizado para este patrón es Python (versión 3).
- SageMaker Studio: Amazon SageMaker Studio es un entorno de desarrollo integrado (IDE) basado en la web para el aprendizaje automático que le permite crear, entrenar, depurar, implementar y supervisar sus modelos de aprendizaje automático. Los trabajos de SageMaker procesamiento se ejecutan con los cuadernos de Jupyter incluidos en Studio. SageMaker
- SageMaker Procesamiento: Amazon SageMaker Processing proporciona una forma simplificada de ejecutar sus cargas de trabajo de procesamiento de datos. En este patrón, el código de ingeniería de funciones se implementa a escala mediante tareas SageMaker de procesamiento.

Código

El archivo .zip adjunto proporciona el código completo de este patrón. En la siguiente sección se describen los pasos para crear la arquitectura para este patrón. Cada paso se ilustra con un ejemplo de código del archivo adjunto.

Epics

Configura tu entorno de SageMaker estudio

Tarea	Descripción	Habilidades requeridas
Accede a Amazon SageMaker Studio.	Inicie sesión en SageMaker Studio en su cuenta de AWS siguiendo las instrucciones que se proporcionan en la SageMaker documentación de Amazon.	Científico de datos, ingeniero de machine learning
Instale la utilidad wget.	Instala wget si has incorpora do una nueva configuración de SageMaker Studio o si nunca has utilizado estas utilidades en SageMaker Studio. Para instalarlo, abre una ventana de terminal en la consola de SageMaker Studio y ejecuta el siguiente comando: `sudo yum install wget`	Científico de datos, ingeniero de machine learning
Descargue y descomprima el código de muestra.	Descargue el archivo `attachments.zip` en la sección Adjuntos. En una ventana de terminal, navegue hasta la carpeta en la que descargó el archivo y extraiga su contenido: `unzip attachment.zip`	Científico de datos, ingeniero de machine learning

Tarea	Descripción	Habilidades requeridas
	Desplácese hasta la ubicación donde descargó el archivo .zip y extraiga el contenido del archivo `Scaled-Processing.zip` . `unzip Scaled-Processing.zip`	
Descargue el conjunto de datos de muestra de physionet.org y cárguelo en Amazon S3.	Ejecute el cuaderno de Jupyter `get_data.ipynb` dentro de la carpeta que contiene los archivos `Scaled-Processing` . Este bloc de notas descarga un conjunto de datos MIMIC-III de muestra de physionet.org y lo carga en el bucket de sesión SageMaker de Studio en Amazon S3.	Científico de datos, ingeniero de machine learning

Configure el primer script de preprocesamiento

Tarea	Descripción	Habilidades requeridas
Aplane la jerarquía de archivos en todos los subdirectorios.	En conjuntos de datos grandes, como MIMIC-III, los archivos suelen distribuirse en varios subdirectorios, incluso dentro de un grupo principal lógico. El script debe estar configurado para aplanar todos los archivos del grupo en todos los subdirect	Científico de datos, ingeniero de machine learning

Tarea	Descripción	Habilidades requeridas
	orios, como se muestra en el siguiente código. `# Generate list of .dat files on machine` `data_dir = input_dir` `d_subs = next(os.walk(os.path.join(data_dir, '.')))[1]` `file_list = []` `for ds in d_subs:` `  file_list.extend(os.listdir(os.path.join(data_dir, ds, '.')))` `dat_list = [os.path.join(re.split('_|\.', f)[0].replace('n', ''), f[:-4]) for f in file_list if f[-4:] == '.dat']` Nota Los fragmentos de código de ejemplo de esta epopeya provienen del archivo `src/feature-engineering-pass1/preprocessing.py` que se proporciona en el archivo adjunto.	

Tarea	Descripción	Habilidades requeridas
Divida los archivos en subgrupos según el recuento de vCPU.	Los archivos deben dividirse en subgrupos o fragmentos de tamaño uniforme, según la cantidad de vCPU presentes en la instancia que ejecuta el script. Para este paso, puede implementar código similar al siguiente. `# Split list of files into sub-lists` `cpu_count = multiprocessing.cpu_count()` `splits = int(len(dat_list) / cpu_count)` `if splits == 0: splits = 1` `dat_chunks = list(chunks(dat_list, splits))`	Científico de datos, ingeniero de machine learning
Paralelice el procesamiento de subgrupos en las vCPU.	La lógica del script debe configurarse para procesar todos los subgrupos en paralelo. Para ello, utilice la clase `Parallel` y el método `delayed` de la biblioteca Joblib de la siguiente manera. `# Parallelize processing of sub-lists across CPUs` `ws_df_list = Parallel(n_jobs=-1, verbose=0)(delayed(run_process)(dc) for dc in dat_chunks)`	Científico de datos, ingeniero de machine learning

Tarea	Descripción	Habilidades requeridas
Guarde la salida de un solo grupo de archivos en Amazon S3.	Cuando se complete el procesamiento de la vCPU paralela, los resultados de cada vCPU deben combinarse y cargarse en la ruta del bucket S3 del grupo de archivos. Para este paso, puede utilizar código similar al siguiente. `# Compile and pickle patient group dataframe` `ws_df_group = pd.concat(ws_df_list)` `ws_df_group = ws_df_group.reset_index().rename(columns={'index': 'signal'})` `ws_df_group.to_json(os.path.join(output_dir, group_data_out))`	Científico de datos, ingeniero de machine learning

Configure el segundo script de preprocesamiento

Tarea	Descripción	Habilidades requeridas
Combine los archivos de datos generados en todos los trabajos de procesamiento en los que se ejecutó el primer script.	El script anterior genera un único archivo para cada trabajo de SageMaker procesamiento que procesa un grupo de archivos del conjunto de datos. A continuación, debe combinar estos archivos de salida en	Científico de datos, ingeniero de machine learning

Tarea	Descripción	Habilidades requeridas
	un único objeto y escribir un único conjunto de datos de salida en Amazon S3. Esto se demuestra en el archivo `src/feature-engineering-pass1p5/preprocessing.py` , que se proporciona en el archivo adjunto, de la siguiente manera. `def write_parquet(wavs_df, path):` `"""` `Write waveform summary dataframe to S3 in parquet format.` `:param wavs_df: waveform summary dataframe` `:param path: S3 directory prefix` `:type wavs_df: pandas dataframe` `:type path: str` `:return: None` `"""` `extra_args = {"ServerSideEncryption": "aws:kms"}` `wr.s3.to_parquet(` `df=wavs_df,` `path=path,` `compression='snappy',` `s3_additional_kwargs=extra_args)`	

Tarea	Descripción	Habilidades requeridas
	<pre>def combine_data(): """ Get combined data and write to parquet. :return: waveform summary dataframe :rtype: pandas dataframe """ wavs_df = get_data( ) wavs_df = normalize _signal_names(wavs _df) write_parquet(wavs _df, "s3://{}/{}/ {}".format(buck et_xform, dataset_p refix, pass1p5ou t_data)) return wavs_df wavs_df = combine_d ata()</pre>	

Ejecutar trabajos de procesamiento

Tarea	Descripción	Habilidades requeridas
Ejecute el primer trabajo de procesamiento.	Para realizar la fragmentación de macros, ejecute un trabajo de procesamiento independiente para cada grupo de archivos.	Científico de datos, ingeniero de machine learning

Tarea	Descripción	Habilidades requeridas
	La microfragmentación se realiza dentro de cada trabajo de procesamiento, ya que cada trabajo ejecuta el primer script. El código siguiente muestra cómo iniciar un trabajo de procesami ento para cada directorio de grupos de archivos en el siguiente fragmento (incluido en `notebooks/FeatExtr act_Pass1.ipynb`). `pat_groups = list(rang e(30,40))` `ts = str(int(time.time( )))` `for group in pat_group s:` `sklearn_processor = SKLearnProcessor(f ramework_version=' 0.20.0',` `role=role,` `instance_ type='ml.m5.4xlarge',` `instance_ count=1,` `volume_si ze_in_gb=5)` `sklearn_processor. run(` `code='../src/ feature-engineering-`	

Tarea	Descripción	Habilidades requeridas
	pass1/preprocessing.py', job_name='-'.join(['scaled-processing-p1', str(group), ts]), arguments=["input_path", "/opt/ml/processing/input", "output_path", "/opt/ml/processing/output", "group_data_out", "ws_df_group.json"], inputs= [ProcessingInput(source=f's3://{sess.default_bucket()}/data_inputs/{group}', destination='/opt/ml/processing/input', s3_data_distribution_type='FullyReplicated')], outputs= [ProcessingOutput(source='/opt/ml/processing/output',	

Tarea	Descripción	Habilidades requeridas
	<pre>destination=f's3://{sess.default_bucket()}/data_outputs/{group}')], wait=False)</pre>	

Tarea	Descripción	Habilidades requeridas
Ejecute el segundo trabajo de procesamiento.	Para combinar los resultados generados por el primer conjunto de trabajos de procesamiento y realizar cualquier cálculo adicional para el preprocesamiento, ejecute el segundo script mediante un único trabajo de SageMaker procesamiento. El siguiente código lo demuestra (incluido en `notebooks/FeatExtract_Pass1p5.ipynb`). `ts = str(int(time.time()))` `bucket = sess.default_bucket()` `sklearn_processor = SKLearnProcessor(framework_version='0.20.0',` `role=role,` `instance_type='ml.t3.2xlarge',` `instance_count=1,` `volume_size_in_gb=5)` `sklearn_processor.run(` `code='../src/feature-engineering-pass1p5/preprocessing.py',`	Científico de datos, ingeniero de machine learning

Tarea	Descripción	Habilidades requeridas
	<pre>job_name='-'.join(['scaled-processing', 'p1p5', ts]), arguments=['bucket ', bucket, 'pass1out _prefix', 'data_out puts', 'pass1out _data', 'ws_df_gr oup.json', 'pass1p5o ut_data', 'waveform _summary.parquet', 'statsdat a_name', 'signal_s tats.csv'], wait=True)</pre>	

Recursos relacionados

- Incorporarse a Amazon SageMaker Studio mediante Quick Start (SageMaker documentación)
- Datos del proceso (SageMaker documentación)
- Procesamiento de datos con scikit-learn (documentación) SageMaker
- Documentación de JobLib.Parallel
- Moody, B., Moody, G., Villarroel, M., Clifford, G. D., & Silva, I. (2020). Base de datos de formas de onda MIMIC-III (versión 1.0). PhysioNet.
- Johnson, A. E. W., Pollard, T. J., Shen, L., Lehman, L. H., Feng, M., Ghassemi, M., Moody, B., Szolovits, P., Celi, L. A., & Mark, R. G. (2016). MIMIC-III, una base de datos de cuidados intensivos de acceso gratuito. Scientific Data, 3, 160035.
- Licencia de MIMIC-III Waveform Database

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Visualizar los resultados del modelo de IA/ML mediante Flask y AWS Elastic Beanstalk

Creado por Chris Caudill (AWS) y Durga Sury

Entorno: PoC o piloto	Tecnologías: aprendizaje automático e inteligencia artificial; análisis DevOps; aplicaciones web y móviles	Carga de trabajo : código abierto
Servicios de AWS: Amazon Comprehend; AWS Elastic Beanstalk		

Resumen

La visualización de los resultados de los servicios de inteligencia artificial y machine learning (IA/ML) suele requerir llamadas complejas a la API, que los desarrolladores e ingenieros deben personalizar. Esto puede ser un inconveniente si sus analistas desean explorar rápidamente un nuevo conjunto de datos.

Para mejorar la accesibilidad de sus servicios y ofrecer una forma de análisis de datos más interactiva puede utilizar una interfaz de usuario (UI) basada en la web que permite a los usuarios cargar sus propios datos y visualizar los resultados del modelo en un panel de control.

Este patrón utiliza Flask y Plotly para integrar Amazon Comprehend en una aplicación web personalizada y visualizar opiniones y entidades a partir de los datos proporcionados por los usuarios. El patrón también indica los pasos para implementar una aplicación mediante AWS Elastic Beanstalk. Puede adaptar la aplicación mediante los servicios de IA de Amazon Web Services (AWS) o con un modelo entrenado personalizado alojado en un punto final (por ejemplo, un SageMaker punto final de Amazon).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.

- Interfaz de la línea de comandos de AWS (AWS CLI), instalada y configurada en su equipo local. Para obtener más información, consulte la sección Aspectos básicos de configuración en la documentación de la CLI de AWS. También puede usar un entorno de desarrollo integrado (IDE) de AWS Cloud9; para obtener más información, consulte el Python tutorial for AWS Cloud9 y Previewing running applications in the AWS Cloud9 IDE en la documentación de AWS Cloud9.
- Comprensión de la estructura de aplicaciones web de Flask. Para obtener más información acerca de Flask, consulte Quickstart en la documentación de Flask.
- Python 3.6 o una versión posterior, instalada y configurada. Puede instalar Python siguiendo las instrucciones de Configuración del entorno de desarrollo de Python en la documentación de AWS Elastic Beanstalk.
- Interfaz de la línea de comandos de Elastic Beanstalk (CLI de EB), instalada y configurada. Para obtener más información, consulte Instalación de la CLI de EB y Configuración de la CLI de EB en la documentación de AWS Elastic Beanstalk.

Limitaciones

- La aplicación Flask de este patrón está diseñada para funcionar con archivos .csv que utilizan una sola columna de texto y están limitados a 200 filas. El código de la aplicación se puede adaptar para gestionar otros tipos de archivos y volúmenes de datos.
- La aplicación no tiene en cuenta la retención de datos y continúa agregando los archivos de usuario cargados hasta que se eliminan manualmente. Puede integrar la aplicación con Amazon Simple Storage Service (Amazon S3) para el almacenamiento persistente de objetos o utilizar una base de datos como Amazon DynamoDB para el almacenamiento de valores clave sin servidor.
- La aplicación solo tiene en cuenta documentos en inglés. Sin embargo, puede utilizar Amazon Comprehend para detectar el idioma principal de un documento. Para obtener más información acerca de los idiomas admitidos para cada acción, consulte la Referencia de la API en la documentación de Amazon Comprehend.
- En la sección Información adicional encontrará una lista de resolución de problemas con los errores más comunes y sus soluciones.

Arquitectura

Arquitectura de aplicaciones Flask

Flask es una estructura ligera para desarrollar aplicaciones web en Python. Está diseñada para combinar el potente procesamiento de datos de Python con una interfaz de usuario web enriquecida.

La aplicación Flask del patrón muestra cómo crear una aplicación web que permita a los usuarios cargar datos, enviar los datos a Amazon Comprehend para su inferencia y, a continuación, visualizar los resultados. La aplicación tiene la estructura siguiente:

- `static`— Contiene todos los archivos estáticos compatibles con la interfaz de usuario web (por ejemplo JavaScript, CSS e imágenes)
- `templates` – Contiene todas las páginas HTML de la aplicación
- `userData` – Almacena los datos cargados por el usuario
- `application.py` – El archivo de la aplicación Flask
- `comprehend_helper.py` – Funciones para realizar llamadas de API a Amazon Comprehend
- `config.py` – Archivo de configuración de la aplicación
- `requirements.txt` – Las dependencias de Python que requiere la aplicación

El script `application.py` contiene la funcionalidad principal de la aplicación web, que consta de cuatro rutas de Flask. En el diagrama siguiente se muestran estas rutas de Flask.

- `/` es la raíz de la aplicación y dirige a los usuarios a la página `upload.html` (almacenada en el directorio `templates`).
- `/saveFile` es una ruta que se invoca después de que un usuario cargue un archivo. Esta ruta recibe una solicitud `POST` a través de un formulario HTML, que contiene el archivo cargado por el usuario. El archivo se guarda en el directorio `userData` y la ruta redirige a los usuarios a la ruta `/dashboard`.
- `/dashboard` envía a los usuarios a la página `dashboard.html`. Dentro del HTML de esta página, ejecuta el JavaScript código `static/js/core.js` que lee los datos de la `/data` ruta y, a continuación, crea visualizaciones para la página.
- `/data` es una API de JSON que presenta los datos que se van a visualizar en el panel de control. Esta ruta lee los datos proporcionados por el usuario y utiliza las funciones en `comprehend_helper.py` para enviar los datos del usuario a Amazon Comprehend para el análisis de opiniones y el reconocimiento de entidades nombradas (NER). La respuesta de Amazon Comprehend se formatea y se devuelve como un objeto JSON.

Arquitectura de implementación

Para obtener más información sobre las consideraciones de diseño de las aplicaciones implementadas con Elastic Beanstalk en la nube de AWS, consulte la documentación de AWS Elastic Beanstalk.

Consideraciones sobre el diseño

Pila de tecnología

- Amazon Comprehend
- Elastic Beanstalk
- Flask

Automatizar y escalar

Las implementaciones de Elastic Beanstalk se configuran automáticamente con equilibradores de carga y grupos de escalado automático. Para obtener más opciones de configuración, consulte Configuración de entornos de Elastic Beanstalk en la documentación de AWS Elastic Beanstalk.

Herramientas

- La interfaz de línea de comandos de AWS (AWS CLI) es una herramienta unificada que proporciona una interfaz coherente para interactuar con todas las partes de AWS.
- Amazon Comprehend utiliza el procesamiento del lenguaje natural (NLP) para extraer información sobre el contenido de los documentos sin necesidad de un procesamiento previo especial.
- AWS Elastic Beanstalk le ayuda a implementar y administrar aplicaciones rápidamente en la nube de AWS sin tener que conocer la infraestructura en la que se ejecutan esas aplicaciones.
- La CLI de Elastic Beanstalk (EB CLI) es una interfaz de línea de comandos para AWS Elastic Beanstalk que proporciona comandos interactivos para simplificar la creación, la actualización y la supervisión de los entornos desde un repositorio local.
- El marco Flask realiza el procesamiento de datos y las llamadas a la API mediante Python y ofrece una visualización web interactiva con Plotly.

Código

El código de este patrón está disponible en los resultados del modelo AI/ML de GitHub Visualize mediante Flask y el repositorio AWS Elastic Beanstalk.

Epics

Configurar la aplicación Flask

Tarea	Descripción	Habilidades requeridas
Clone el repositorio. GitHub	Extraiga el código de la aplicación de los resultados del modelo AI/ML de GitHub Visualize mediante Flask y el repositorio AWS Elastic Beanstalk ejecutando el siguiente comando: `git clone git@github.com:aws-samples/aws-comprehend-elasticbeanstalk-for-flask.git` Nota: Asegúrese de configurar sus claves SSH con. GitHub	Desarrollador
Instale los módulos de Python.	Una vez clonado el repositorio, se crea un nuevo directorio `aws-comprehend-elasticbeanstalk-for-flask` local. En ese directorio, el archivo `requirements.txt` contiene los módulos y las versiones de Python que ejecutan la aplicación. Utilice los comandos siguientes para instalar los módulos:	Python developer

Tarea	Descripción	Habilidades requeridas
	`cd aws-comprehend-elasticbeanstalk-for-flask` `pip install -r requirements.txt`	
Pruebe la aplicación localmente.	Ejecute el siguiente comando para iniciar el servidor de Flask: `python application.py` Esto devuelve información sobre el servidor en ejecución. Debería poder acceder a la aplicación si abre un navegador y visita http://localhost:5000 Nota: Si ejecuta la aplicación en un IDE de AWS Cloud9, debe reemplazar el comando `application.run()` del archivo `application.py` por la línea siguiente: `application.run(host=os.getenv('IP', '0.0.0.0'),port=int(os.getenv('PORT', 8080)))` Debe revertir este cambio antes de la implementación.	Python developer

Implementar la aplicación en Elastic Beanstalk

Tarea	Descripción	Habilidades requeridas
Inicie la aplicación Elastic Beanstalk.	Para lanzar el proyecto como una aplicación de Elastic Beanstalk, ejecute el comando siguiente desde el directorio raíz de la aplicación: `eb init -p python-3.6 comprehend_flask --region us-east-1` Importante: • `comprehend_flask` es el nombre de la aplicación de Elastic Beanstalk y se puede cambiar según las necesidades. • Puede sustituir la región de AWS por una región de su elección. Se utiliza la región predeterminada de AWS CLI si no se especifica ninguna región. • La aplicación se creó con la versión de Python 3.6. Es posible que se produzcan errores si utiliza otras versiones de Python. Ejecute el comando `eb init -i` para obtener más opciones	Arquitecto, desarrollador

Tarea	Descripción	Habilidades requeridas
	de configuración de implement ación.	
Implemente el entorno de Elastic Beanstalk.	Ejecute el comando siguiente desde el directorio raíz de la aplicación: `eb create comprehend-flask-env` Nota: `comprehend-flask-env` Es el nombre del entorno de Elastic Beanstalk y se puede cambiar según las necesidades. El nombre solo puede contener letras, números y guiones.	Arquitecto, desarrollador

Tarea	Descripción	Habilidades requeridas
Autorice su implementación para usar Amazon Comprehend.	Si bien es posible que su aplicación se haya implementado correctamente, debe proporcionar a su implementación acceso a Amazon Comprehend. `ComprehendFullAccess` es una política administrada de AWS que proporciona a la aplicación implementada los permisos para realizar llamadas de API a Amazon Comprehend. Adjunte la política `ComprehendFullAccess` a `aws-elasticbeanstalk-ec2-role` (esta función se crea automáticamente para las instancias de Amazon Elastic Compute Cloud (Amazon EC2) de la implementación) al ejecutar el comando siguiente: `aws iam attach-role-policy --policy-arn arn:aws:iam::aws:policy/ComprehendFullAccess --role-name aws-elasticbeanstalk-ec2-role` Importante: `aws-elasticbeanstalk-ec2-role` se crea cuando se	Desarrollador, arquitecto de seguridad

Tarea	Descripción	Habilidades requeridas
	implementa la aplicación. Debe completar el proceso de implementación para poder adjuntar la política de AWS Identity and Access Management (IAM).	
Visite su aplicación implement ada.	Una vez que la aplicación se haya implementado correctam ente, puede visitarla mediante la ejecución del comando `eb open`. También puede ejecutar el comando `eb status` para recibir detalles sobre su implementación. La URL de la implementación aparece en `CNAME`.	Arquitecto, desarrollador

(Opcional) Personalizar la aplicación según su modelo de ML

Tarea	Descripción	Habilidades requeridas
Autorice que Elastic Beanstalk acceda al nuevo modelo.	Asegúrese de que Elastic Beanstalk tenga los permisos de acceso necesarios para el nuevo modelo de punto de conexión. Por ejemplo, si utilizas un SageMaker punto de conexión de Amazon, tu implementación debe tener permiso para invocar el punto de conexión.	Desarrollador, arquitecto de seguridad

Tarea	Descripción	Habilidades requeridas
	Para obtener más información al respecto, consulta InvokeEndpointla SageMaker documentación de Amazon.	

Tarea	Descripción	Habilidades requeridas
Envíe los datos del usuario a un nuevo modelo.	Para cambiar el modelo de ML subyacente en esta aplicación, debe cambiar los archivos siguientes: • `comprehend_helper.py` : Este es el script de Python que se conecta con Amazon Comprehend, procesa la respuesta y devuelve el resultado final a la aplicación. En este script, puede enrutar los datos hacia otro servicio de IA en la nube de AWS o enviar los datos a un punto de conexión de modelo personalizado. Es recomendable formatear también los resultados de este script para separarlos lógicamente y poder reutilizar este patrón. • `application.py` : Si cambia el nombre del script `comprehend_helper.py` o de las funciones, debe actualizar el script `application.py` de la aplicación para que refleje esos cambios.	Científico de datos

Tarea	Descripción	Habilidades requeridas
Actualice las visualizaciones del panel de control.	Por lo general, la incorporación de un nuevo modelo de ML significa que las visualizaciones deben actualizarse para reflejar los nuevos resultados. Se han realizado estos cambios en los archivos siguientes: • `templates/dashboard.html` : La aplicación prediseñada solo tiene en cuenta dos visualizaciones básicas. El diseño completo de la página se puede ajustar en este archivo. • `static/js/core.js` : Este script captura la salida formateada de la ruta `/data` del servidor Flask y usa Plotly para crear visualizaciones. Puede añadir o actualizar los gráficos de la página.	Desarrollador web

(Opcional) Implementar la aplicación actualizada

Tarea	Descripción	Habilidades requeridas
Actualice el archivo de requisitos de su solicitud.	Antes de enviar los cambios a Elastic Beanstalk, actualice el archivo `requirements.txt` para que refleje los nuevos módulos de Python. Para ello,	Python developer

Tarea	Descripción	Habilidades requeridas
	ejecute el siguiente comando en el directorio raíz de la aplicación: `pip freeze > requirements.txt`	
Vuelva a implementar el entorno de Elastic Beanstalk.	Para asegurarse de que los cambios en la aplicación se reflejen en la implementación de Elastic Beanstalk, navegue hasta el directorio raíz de la aplicación y ejecute el comando siguiente: `eb deploy` Esto envía la versión más reciente del código de la aplicación a la implementación de Elastic Beanstalk existente.	Administrador de sistemas, arquitecto

Recursos relacionados

- Llame a un punto de conexión SageMaker modelo de Amazon mediante Amazon API Gateway y AWS Lambda
- Implementación de una aplicación Flask en Elastic Beanstalk
- Referencia de los comandos de EB CLI
- Configuración del entorno de desarrollo de Python

Información adicional

Lista de solución de problemas

A continuación, se presentan seis errores comunes y sus soluciones.

Error 1

```
Unable to assume role "arn:aws:iam::xxxxxxxxxx:role/aws-elasticbeanstalk-ec2-role".
 Verify that the role exists and is configured correctly.
```

Solución: Si este error se produce al ejecutar `eb create`, cree una aplicación de muestra en la consola de Elastic Beanstalk para crear el perfil de instancia predeterminado. Para obtener más información al respecto, consulte Creación de un entorno de Elastic Beanstalk en la documentación de AWS Elastic Beanstalk.

Error 2

```
Your WSGIPath refers to a file that does not exist.
```

Solución: Este error se produce en los registros de implementación porque Elastic Beanstalk espera que el código de Flask se denomine `application.py`. Si eligió un nombre diferente, ejecute `eb config` y edite WSGIPath como se muestra en el ejemplo de código siguiente:

```
aws:elasticbeanstalk:container:python:
     NumProcesses: '1'
     NumThreads: '15'
     StaticFiles: /static/=static/
     WSGIPath: application.py
```

Asegúrese de reemplazar `application.py` con el nombre de su archivo.

También puede aprovechar Gunicorn y un Procfile. Para obtener más información sobre este enfoque, consulte Configuración del servidor WSGI con un Procfile en la documentación de AWS Elastic Beanstalk.

Error 3

```
Target WSGI script '/opt/python/current/app/application.py' does not contain WSGI
 application 'application'.
```

Solución: Elastic Beanstalk espera que la variable que representa la aplicación Flask se denomine `application`. Asegúrese de que el archivo `application.py` utilice `application` como nombre de la variable:

```
application = Flask(__name__)
```

Error 4

```
The EB CLI cannot find your SSH key file for keyname
```

Solución: Utilice la EB CLI para especificar qué par de claves usar o para crear un par de claves para las instancias EC2 de la implementación. Para resolver el error, ejecute `eb init -i` y una de las opciones le solicitará lo siguiente:

```
Do you want to set up SSH for your instances?
```

Responda Y para crear un par de claves o especificar un par de claves existente.

Error 5

He actualizado mi código y lo he vuelto a implementar, pero mi implementación no refleja los cambios.

Solución: Si utiliza un repositorio de Git con su implementación, asegúrese de añadir y confirmar los cambios antes de volver a implementarlos.

Error 6

Está previsualizando la aplicación Flask desde un IDE de AWS Cloud9 y se produce un error.

Solución: Para obtener más información al respecto, consulte Vista previa de las aplicaciones en ejecución en el IDE de AWS Cloud9 en la documentación de AWS Cloud9.

Uso de Amazon Comprehend para el procesamiento de lenguaje natural

Al elegir Amazon Comprehend, puede detectar entidades personalizadas en documentos de texto individuales mediante la ejecución de análisis en tiempo real o trabajos por lotes asíncronos. Amazon Comprehend también le permite entrenar modelos personalizados de reconocimiento de entidades y clasificación de texto que se pueden utilizar en tiempo real mediante la creación de un punto de conexión.

Este patrón utiliza trabajos por lotes asíncronos para detectar opiniones y entidades en un archivo de entrada que contiene varios documentos. La aplicación de ejemplo que proporciona este patrón

está diseñada para que los usuarios carguen un archivo .csv que contenga una sola columna con un documento de texto por fila. El `comprehend_helper.py` archivo del modelo AI/ML de GitHub Visualize con Flask y el repositorio de AWS Elastic Beanstalk lee el archivo de entrada y lo envía a Amazon Comprehend para su procesamiento.

BatchDetectEntidades

Amazon Comprehend inspecciona el texto de un lote de documentos en busca de entidades nombradas y devuelve la entidad detectada, la ubicación, el tipo de entidad y una puntuación que indica el nivel de confianza de Amazon Comprehend. Se puede enviar un máximo de 25 documentos en una llamada de API, y cada documento tiene un tamaño inferior a 5000 bytes. Puede filtrar los resultados para mostrar solo determinadas entidades en función del caso de uso. Así, por ejemplo, puede omitir el tipo de entidad `'quantity'` y establecer una puntuación límite para la entidad detectada (por ejemplo, 0,75). Le recomendamos que explore los resultados para su caso de uso específico antes de elegir un valor umbral. Para obtener más información al respecto, consulte BatchDetectEntidades en la documentación de Amazon Comprehend.

BatchDetectSentimiento

Amazon Comprehend inspecciona un lote de documentos entrantes y devuelve la opinión predominante para cada documento (`POSITIVE`, `NEUTRAL`, `MIXED` o `NEGATIVE`). Se puede enviar un máximo de 25 documentos en una llamada de API, y cada documento tiene un tamaño inferior a 5000 bytes. Analizar la opinión es sencillo y se puede elegir aquella que tiene la puntuación más alta para que aparezca en los resultados finales. Para obtener más información al respecto, consulte BatchDetectSentiment en la documentación de Amazon Comprehend.

Manejo de la configuración de Flask

Los servidores Flask utilizan una serie de variables de configuración para controlar el funcionamiento del servidor. Estas variables pueden contener el resultado de la depuración, tokens de sesión u otros ajustes de la aplicación. También puede definir variables personalizadas a las que se puede acceder mientras la aplicación se está ejecutando. Existen varios enfoques para establecer las variables de configuración.

En este patrón, la configuración se define `config.py` y se hereda dentro de `application.py`.

- `config.py` contiene las variables de configuración que se configuran al iniciar la aplicación. En esta aplicación, se define una variable `DEBUG` para indicar a la aplicación que ejecute el servidor

en modo de depuración. Nota: El modo de depuración no debe utilizarse cuando se ejecuta una aplicación en un entorno de producción. `UPLOAD_FOLDER` es una variable personalizada que se define para hacer referencia a ella más adelante en la aplicación e indicar dónde deben almacenarse los datos de usuario cargados.

- `application.py` inicia la aplicación Flask y hereda los ajustes de configuración definidos en `config.py`. Esto se lleva a cabo mediante el código siguiente:

```
application = Flask(__name__)
application.config.from_pyfile('config.py')
```

Más patrones

- Genere información de datos mediante AWS Mainframe Modernization y Amazon Q en QuickSight
- Otorgue a las instancias de SageMaker notebook acceso temporal a un CodeCommit repositorio de otra cuenta de AWS
- Migre cargas de trabajo de aprendizaje automático: cree, entrene e implemente a Amazon SageMaker con las herramientas para desarrolladores de AWS
- Realizar análisis avanzados mediante Amazon Redshift ML

Unidad central

Temas

- Realice copias de seguridad y archive los datos del mainframe en Amazon S3 mediante AMI Cloud Data de BMC
- Cree un visor de archivos de unidad central avanzada en la nube de AWS
- Almacenamiento en contenedores de las cargas de trabajo de mainframe que Blu Age ha modernizado
- Convierta y desempaquete datos EBCDIC a ASCII en AWS mediante Python
- Convertir archivos de mainframe del formato EBCDIC al formato ASCII delimitado por caracteres en Amazon S3 con AWS Lambda
- Convertir archivos de datos de mainframe con diseños de registros complejos mediante Micro Focus
- Implementar un entorno para aplicaciones de Blu Age en contenedores mediante Terraform
- Genere información de datos mediante AWS Mainframe Modernization y Amazon Q en QuickSight
- Integrar el controlador universal Stonebranch con AWS Mainframe Modernization
- Migre y replique archivos VSAM a Amazon RDS o Amazon MSK mediante Connect de Precisely
- Modernice la administración de la producción de mainframe en AWS mediante OpenText Micro Focus Enterprise Server y LRS X PageCenter
- Modernice las cargas de trabajo de impresión por lotes de mainframe en AWS mediante Micro Focus Enterprise Server y LRS VPSX/MFI
- Modernizar las cargas de trabajo de impresión en línea de mainframe en AWS mediante Micro Focus Enterprise Server y LRS VPSX/MFI
- Mover los archivos de mainframe directamente a Amazon S3 mediante Transfer Family
- Transfiera datos de Db2 z/OS a gran escala a Amazon S3 en archivos CSV
- Más patrones

Realice copias de seguridad y archive los datos del mainframe en Amazon S3 mediante AMI Cloud Data de BMC

Creado por Santosh Kumar Singh (AWS), Mikhael Liberman (software de mainframe Model9), Gilberto Biondo (AWS) y Maggie Li (AWS)

Entorno: PoC o piloto	Origen: Mainframe	Destino: Amazon S3
Tipo R: N/D	Tecnologías: Mainframe; almacenamiento y copia de seguridad; modernización	Servicios de AWS: Amazon EC2; Amazon EFS; Amazon S3; AWS Direct Connect

Resumen

Este patrón muestra cómo hacer copias de seguridad y archivar los datos del mainframe directamente en Amazon Simple Storage Service (Amazon S3) y, a continuación, recuperar y restaurar esos datos en el mainframe mediante AMI Cloud Data de BMC (anteriormente conocido como Model9 Manager). Si busca una forma de modernizar su solución de copia de seguridad y archivado como parte de un proyecto de modernización de un mainframe o de cumplir con los requisitos de conformidad, este patrón puede ayudarle a cumplir esos objetivos.

Por lo general, las organizaciones que ejecutan aplicaciones empresariales principales en mainframes utilizan una biblioteca de cintas virtuales (VTL) para hacer copias de seguridad de los almacenes de datos, como archivos y registros. Este método puede resultar caro porque consume MIPS facturables y no se puede acceder a los datos almacenados en cintas fuera del mainframe. Para evitar estos problemas, puede utilizar AMI Cloud Data de BMC para transferir de forma rápida y rentable datos operativos e históricos del mainframe directamente a Amazon S3. Puede utilizar BMC AMI Cloud Data para realizar copias de seguridad y archivar datos a través de TCP/IP y, al AWS mismo tiempo, aprovechar los motores del procesador de información integrado (zIIP) de IBM z para reducir los costes, el paralelismo y los tiempos de transferencia.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa

- BMC AMI Cloud Data con una clave de licencia válida
- Conectividad TCP/IP entre el mainframe y AWS
- Una función AWS Identity and Access Management (IAM) para el acceso de lectura y escritura a un bucket de S3
- Acceso al producto de seguridad de mainframe (RACF) implementado para ejecutar los procesos de BMC AMI Cloud
- Un agente AMI Cloud z/OS de BMC (Java versión 8, SR5 FP16 de 64 bits o posterior) que tenga puertos de red disponibles, reglas de firewall que permitan el acceso a los depósitos de S3 y un sistema de archivos z/FS dedicado
- Requisitos cumplidos para el servidor de administración AMI Cloud de BMC

Limitaciones

- AMI Cloud Data de BMC almacena sus datos operativos en una base de datos PostgreSQL que se ejecuta como un contenedor Docker en la misma instancia de Amazon Elastic Compute Cloud (Amazon EC2) que el servidor de administración. Actualmente, Amazon Relational Database Service (Amazon RDS) no es compatible como backend para AMI Cloud Data de BMC. Para obtener más información sobre las últimas actualizaciones de productos, consulte ¿Qué hay de nuevo? en la documentación de BMC.
- Este patrón solo realiza copias de seguridad y archiva los datos del mainframe z/OS. BMC AMI Cloud Data realiza copias de seguridad y archiva solo archivos de mainframe.
- Este patrón no convierte los datos a formatos abiertos estándar, como JSON o CSV. Utilice un servicio de transformación adicional, como AMI Cloud Analytics de BMC (anteriormente conocido como Model9 Gravity) para convertir los datos en formatos abiertos estándar. Las aplicaciones nativas de la nube y las herramientas de análisis de datos pueden acceder a los datos una vez que se hayan escrito en la nube.

Versiones de producto

- BMC AMI Cloud Data versión 2.x

Arquitectura

Pila de tecnología de origen

- Mainframe que ejecuta z/OS
- Archivos de mainframe, como conjuntos de datos y archivos de z/OS UNIX System Services (USS)
- Disco de mainframe, como un dispositivo de almacenamiento de acceso directo (DASD)
- Cinta de mainframe (biblioteca de cintas físicas o virtuales)

Pila de tecnología de destino

- Amazon S3
- Instancia de Amazon EC2 en una nube privada virtual (VPC)
- AWS Direct Connect
- Amazon Elastic File System (Amazon EFS)

Arquitectura de destino

El siguiente diagrama muestra una arquitectura de referencia en la que los agentes de software AMI Cloud Data de BMC en un mainframe controlan los procesos heredados de copia de seguridad y archivado de datos que almacenan los datos en Amazon S3.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Los agentes de software AMI Cloud Data de BMC se ejecutan en particiones lógicas de mainframe (LPAR). Los agentes de software leen y escriben datos del mainframe desde el DASD o en cinta directamente en Amazon S3 a través de TCP/IP.
2. AWS Direct Connect establece una conexión física y aislada entre la red local y. AWS Para mejorar la seguridad, ejecute una site-to-site VPN sobre ella AWS Direct Connect para cifrar los datos en tránsito.
3. El depósito S3 almacena los archivos del mainframe como datos de almacenamiento de objetos y los agentes AMI Cloud Data de BMC se comunican directamente con los depósitos S3. Los certificados se utilizan para el cifrado HTTPS de todas las comunicaciones entre el agente y Amazon S3. El cifrado de datos de Amazon S3 se utiliza para cifrar y proteger los datos en reposo.
4. Los servidores de administración de datos AMI Cloud de BMC se ejecutan como contenedores Docker en instancias EC2. Las instancias se comunican con los agentes que se ejecutan en buckets de S3 y LPAR de mainframe.

5. Amazon EFS se monta en instancias EC2 activas y pasivas para compartir el almacenamiento del Network File System (NFS). Esto sirve para garantizar que los metadatos relacionados con una política creada en el servidor de administración no se pierdan en caso de una conmutación por error. En caso de una conmutación por error por parte del servidor activo, se puede acceder al servidor pasivo sin pérdida de datos. Si el servidor pasivo falla, se puede acceder al servidor activo sin pérdida de datos.

Herramientas

Servicios de AWS

- Amazon Elastic Compute Cloud (Amazon EC2) proporciona una capacidad informática escalable en el. Nube de AWS Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon Elastic File System (Amazon EFS) le ayuda a crear y configurar sistemas de archivos compartidos en Nube de AWS.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar prácticamente cualquier cantidad de datos.
- Amazon Virtual Private Cloud (Amazon VPC) le ayuda a lanzar AWS recursos en una red virtual que haya definido. Esa red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.
- AWS Direct Connectconecta su red interna a una AWS Direct Connect ubicación a través de un cable Ethernet de fibra óptica estándar. Con esta conexión, puede crear interfaces virtuales directamente con los AWS servicios públicos y, al mismo tiempo, omitir a los proveedores de servicios de Internet en su ruta de red.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.

Herramientas BMC

- El servidor de administración BMC AMI Cloud es una aplicación de interfaz gráfica de usuario que se ejecuta como un contenedor de Docker en una Amazon Machine Image (AMI) de Amazon Linux para Amazon EC2. El servidor de administración proporciona la funcionalidad para gestionar las actividades de AMI Cloud de BMC, como la elaboración de informes, la creación y la gestión

de políticas, la ejecución de archivos y la realización de copias de seguridad, recuperaciones y restauraciones.

- El agente AMI Cloud de BMC se ejecuta en un LPAR de mainframe local que lee y escribe archivos directamente en el almacenamiento de objetos mediante TCP/IP. Una tarea iniciada se ejecuta en un LPAR de mainframe y es responsable de leer y escribir los datos de respaldo y archivar en Amazon S3 y desde este.
- La interfaz de línea de comandos (M9CLI) de BMC AMI Cloud Mainframe le proporciona un conjunto de comandos para realizar acciones de BMC AMI Cloud directamente desde el TSO/E o en operaciones por lotes, sin depender del servidor de administración.

Epics

Creación de un bucket de S3 y una política de IAM

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3.	Cree un bucket de S3 para almacenar los archivos y volúmenes de los que desee realizar copias de seguridad y archivar desde su entorno de mainframe.	AWS general
Cree una política de IAM.	Todos los servidores y agentes de administración AMI Cloud de BMC requieren acceso al bucket de S3 que creó en el paso anterior. Para conceder el acceso necesario, cree la siguiente política de IAM: `{ "Version": "2012-10-17", "Statement": [`	AWS general

Tarea	Descripción	Habilidades requeridas
	<pre>{ "Sid": "Listfolder", "Action": ["s3:ListBucket", "s3:GetBucketLocation", "s3:ListBucketVersions"], "Effect": "Allow", "Resource": ["arn:aws:s3:::<BucketName>"] }, { "Sid": "Objectaccess", "Effect": "Allow", "Action": ["s3:PutObject", "s3:GetObjectAcl", "s3:GetObject", "s3:DeleteObjectVersion", "s3:DeleteObject", "s3:PutObjectAcl",</pre>	

Tarea	Descripción	Habilidades requeridas
	<pre>"s3:GetObjectVersion"], "Resource": ["arn:aws:s3:::<Bucket Name>/*"] }] }</pre>	

Obtenga la licencia del software BMC AMI Cloud y descargue el software

Tarea	Descripción	Habilidades requeridas
Obtenga una licencia de software BMC AMI Cloud.	Para obtener una clave de licencia de software, póngase en contacto con el equipo de AMI Cloud de BMC. El resultado del comando `D M=CPU` de z/OS es necesario para generar una licencia.	Responsable de compilación
Descargue el software BMC AMI Cloud y la clave de licencia.	Obtenga los archivos de instalación y la clave de licencia siguiendo las instrucciones de la documentación de BMC.	Administrador de infraestructuras de mainframe

Instale el agente de software BMC AMI Cloud en el mainframe

Tarea	Descripción	Habilidades requeridas
Instale el agente de software AMI Cloud de BMC.	1. Antes de iniciar el proceso de instalación, compruebe que se cumplen los requisitos mínimos de software y hardware para el agente. 2. Para instalar el agente, siga las instrucciones de la documentación de BMC. 3. Cuando el agente comience a ejecutarse en el LPAR del mainframe , compruebe si aparece el mensaje `ZM91000I MODEL9 BACKUP AGENT INITIALIZED` en la cola Compruebe que la conectividad entre el agente y el bucket de S3 se haya establecido correctamente. Para ello, busque el `Object store connectivity has been established successfully` mensaje en el STDOUT del agente.	Administrador de infraestructuras de mainframe

Configure un servidor de administración AMI Cloud de BMC en una instancia EC2

Tarea	Descripción	Habilidades requeridas
Cree instancias de Amazon EC2 Linux 2.	Lance dos instancias de Amazon EC2 Linux 2 en distintas zonas de disponibilidad siguiendo las instrucciones del paso 1: lanzar una instancia de la documentación de Amazon EC2. La instancia debe cumplir los siguientes requisitos de hardware y software recomendados: • CPU: 4 núcleos como mínimo • RAM: 8 GB como mínimo • Unidad: 40 GB • Instancia EC2 recomendada: C5.xlarge • Sistema operativo: Linux • Software: Docker, unzip, VI/vim • Ancho de banda de red: 1 GB como mínimo Para obtener más información, consulte la documentación de BMC.	Arquitecto de la nube, administrador de la nube
Crear un sistema de archivos de Amazon EFS.	Cree un sistema de archivos Amazon EFS siguiendo las instrucciones del Paso 1:	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	Cree su sistema de archivos Amazon EFS en la documentación de Amazon EFS. Al crear el sistema de archivos, haga lo siguiente: • Elija la clase de almacenamiento estándar. • Elija la misma VPC que utilizó para lanzar sus instancias EC2.	

Tarea	Descripción	Habilidades requeridas
Instale Docker y configure el servidor de administración.	Conéctese a sus instancias EC2: Conéctese a sus instancias EC2 siguiendo las instrucciones de Conectarse a su instancia Linux en la documentación de Amazon EC2. Configure sus instancias EC2: Para cada instancia de EC2, haga lo siguiente: 1. Para instalar Docker, ejecute el comando: `sudo yum install docker` 2. Para iniciar Docker, ejecute el comando: `sudo service docker start` 3. Para validar el estado de Docker, ejecute el comando: `sudo service docker status` 4. En la carpeta `/etc/selinux`, cambie el archivo `config` a `SELINUX=permissive`.	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	5. Cargue los `VerificationScripts.zip` archivos `model9-v2.x.y_build_build-id-server.zip` y (que descargó anteriormente) en una carpeta temporal de una de las instancias de EC2 (por ejemplo, en la `/var/tmp` carpeta de su instancia). 6. Para ir a la `tmp` carpeta, ejecute el comando: `cd/var/tmp` 7. Para descomprimir el script de verificación, ejecute el comando: `unzip VerificationScripts.zip` 8. Para cambiar el directorio, ejecute el comando: `cd /var/tmp/sysutils/PrereqsScripts` 9. Para ejecutar el script de verificación, ejecute el comando: `./M9VerifyPrereqs.sh`	

Tarea	Descripción	Habilidades requeridas
	10. Cuando el script de verificación solicite la entrada, introduzca la URL y el número de puerto de Amazon S3. A continuación, introduzca la IP/DNS y el número de puerto de z/OS. Nota: El script comprueba que la instancia EC2 se puede conectar con el bucket y el agente de S3 que se ejecutan en el mainframe. Si se establece una conexión, se muestra un mensaje de confirmación.	

Tarea	Descripción	Habilidades requeridas
Instale el software del servidor de administración.	1. Cree una carpeta y una subcarpeta en el directorio raíz (por ejemplo, `/data/model9`) de la instancia EC2 en la que planea convertir en servidor activo. 2. Para instalar el `amazon-efs-utils` paquete y montar el sistema de archivos Amazon EFS creado anteriormente, ejecute los siguientes comandos: `sudo yum install -y amazon-efs-utils` `sudo mount -t efs -o tls <File System ID>:/ /data/model9` 3. Para actualizar el `/etc/fstab` archivo de la instancia EC2 con una entrada para el sistema de archivos Amazon EFS (de modo que Amazon EFS se vuelva a montar automáticamente cuando Amazon EC2 se reinicie), ejecute el comando: `<Amazon-EFS-file-system-id>:/ /data/model9 efs defaults,_netdev 0 0`	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	4. Para definir la ruta a los archivos de instalación de AMI Cloud de BMC y la ubicación de instalación de destino, ejecute los siguientes comandos para exportar variables: `export MODEL9_HOME=/data/model9` `export M9INSTALL=/var/tmp` Nota: Le recomendamos que añada estos comandos de exportación a su script `.bashrc`. 5. Para cambiar el directorio, ejecute el comando `cd $MODEL9_HOME` y, a continuación, cree otro subdirectorio ejecutando el comando `mkdir diag`. 6. Para descomprimir el archivo de instalación, ejecute el comando: `unzip $M9INSTALL/model9-<v2.x.y>_build_<build-id>-server.zip` Nota: Sustituya `x.y` (la versión) y `build-id` por sus valores.	

Tarea	Descripción	Habilidades requeridas
	7. Para implementar la aplicación, ejecute los siguientes comandos: `docker load -i $MODEL9_HOME/model9-<v2.x.y>_build_<build-id>.docker` `docker load -i $MODEL9_HOME/postgres-12.10-x86.docker.gz` Nota: Sustituya `v2.x.y` (la versión) y `build-id` por sus valores. 8. En la carpeta `$MODEL9_HOME/conf` , actualice el archivo `model9-local.yml` . Nota: Algunos de los parámetros tienen valores predeterminados y otros se pueden actualizar según sea necesario. Para más información, consulte las instrucciones en el archivo `model9-local.yml` . 9. Cree un archivo llamado y **`$MODEL9_HOME/conf`** , a continuación, añada los siguientes parámetros al archivo: `TZ=America/New_York`	

Tarea	Descripción	Habilidades requeridas
	`EXTRA_JVM_ARGS=-Xmx2048m` 10. Para crear un puente de red Docker, ejecute el comando: `docker network create -d bridge model9network` 11. Para iniciar el contenedor de base de datos PostgreSQL para AMI Cloud de BMC, ejecute el siguiente comando: `docker run -p 127.0.0.1:5432:5432 \ -v $MODEL9_HOME/db/data:/var/lib/postgresql/data:z \ --name model9db --restart unless-stopped \ --network model9network \ -e POSTGRES_PASSWORD=model9 -e POSTGRES_DB=model9 -d postgres:12.10` 12. Una vez que se inicie la ejecución del contenedor de PostgreSQL, ejecute el siguiente comando para iniciar el servidor de aplicaciones:	

Tarea	Descripción	Habilidades requeridas
	`` docker run -d -p 0.0.0.0:443:443 -p 0.0.0.0:80:80 \ --sysctl net.ipv4. tcp_keepalive_time =600 \ --sysctl net.ipv4. tcp_keepalive_intv l=30 \ --sysctl net.ipv4. tcp_keepalive_prob es=10 \ -v $MODEL9_HOME:/mode l9:z -h $(hostname) --restart unless-st opped \ --env-file $MODEL9_H OME/conf/model9.env \ --network model9net work \ --name model9-v2.x.y model9:<v2.x.y>.<b uild-id> ``` Nota: Sustituya `v2.x.y` (la versión) y `build-id` por sus valores. 13. Para comprobar el estado de ambos contenedores, ejecute el comando: ``` docker ps -a ``` 14. Para instalar un servidor de administración en las instancias EC2 pasivas,	

Tarea	Descripción	Habilidades requeridas
	repita los pasos 1 a 4, 7 y 10 a 13. Nota: Para solucionar problemas, vaya a los registros almacenados en la carpeta `/data/model9/logs/` . Para obtener más información, consulte la documentación de BMC.	

Agregue un agente y defina una política de respaldo o archivado en el servidor de administración AMI Cloud de BMC

Tarea	Descripción	Habilidades requeridas
Añada un nuevo agente.	Antes de añadir un agente nuevo, confirme lo siguiente: • Un agente AMI Cloud de BMC se está ejecutando en el LPAR del mainframe y se ha inicializado por completo. Identifique al agente buscando el mensaje de `ZM91000I MODEL9 BACKUP AGENT INITIALIZED` inicializ ación en la bobina. • Un contenedor Docker para el servidor de administr ación está completamente inicializado y en ejecución.	Desarrollador o administr ador de almacenamiento de mainframe

Tarea	Descripción	Habilidades requeridas
	Debe crear un agente en el servidor de administración antes de definir cualquier política de respaldo y archivado. Para crear el agente, haga lo siguiente: 1. Utilice un navegador web para acceder al servidor de administración que está desplegado en su máquina Amazon EC2 y, a continuación, inicie sesión con sus credenciales de mainframe. 2. Elija la pestaña AGENTES y, a continuación, AGREGAR NUEVO AGENTE. 3. En Nombre, escriba el nombre del agente. 4. Para el nombre de host/dirección IP, introduzca el nombre de host o la dirección IP de su mainframe. 5. En Puerto, escriba su número de puerto. 6. Elija PROBAR CONEXIÓN. Si la conectividad se ha establecido correctamente, verá un mensaje de confirmación. 7. Elija CREAR.	

Tarea	Descripción	Habilidades requeridas
	Una vez creado el agente, verá el estado de conexión en comparación con el almacenamiento de objetos y el agente de mainframe en una nueva ventana que aparece en la tabla.	
Cree una política de copia de seguridad o archivado.	1. Elija POLÍTICAS. 2. Elija CREAR POLÍTICA. 3. En la página CREAR UNA NUEVA POLÍTICA, introduzca las especific aciones de su política. Nota: Para obtener más información sobre las especificaciones disponibl es, consulte Creación de una nueva política en la documentación de BMC. 4. Seleccione Finalizar. 5. La nueva política ahora aparece en forma de tabla. Para ver esta tabla, seleccione la pestaña POLÍTICAS.	Desarrollador o administr ador de almacenamiento de mainframe

Ejecute la política de copia de seguridad o archivado desde el servidor de administración

Tarea	Descripción	Habilidades requeridas
Ejecute la política de copia de seguridad o archivado.	Ejecute la política de copia de seguridad o archivado de datos que creó anteriormente desde el servidor de administración de forma manual o automática (según una programación). Para ejecutar la política manualmente: 1. En el menú de navegación, elija la pestaña POLÍTICAS. 2. En el lado derecho de la tabla correspondiente a la política que desee ejecutar, seleccione el menú de tres puntos. 3. Seleccione Ejecutar ahora. 4. En la ventana de confirmación emergente, elija SÍ, EJECUTAR LA POLÍTICA AHORA. 5. Una vez ejecutada la política, compruebe el estado de ejecución en la sección de actividad de la política. 6. Para la política que se ejecutó, selecciona el menú de tres puntos y, a continuación, selecciona	Desarrollador o administrador de almacenamiento de mainframe

Tarea	Descripción	Habilidades requeridas
	Ver registro de ejecución para ver los registros. 7. Para comprobar que se creó la copia de seguridad, compruebe el bucket de S3.	

Tarea	Descripción	Habilidades requeridas
Restaure la copia de seguridad o la política de archivos.	1. En el menú de navegación, seleccione la pestaña POLÍTICAS. 2. Elige la política en la que se ejecutará el proceso de restauración. Esto mostrará una lista de todas las actividades de copia de seguridad o archivado que se ejecutaron en el pasado para esa política específica. 3. Para seleccionar las copias de seguridad que desea restaurar, elija la columna Fecha y hora. El nombre del grupo `file/Volume/Storage` muestra los detalles de ejecución de la política. 4. En la parte derecha de la tabla, selecciona el menú de tres puntos y, a continuación, selecciona RESTAURAR. 5. En la ventana emergente, introduzca el nombre, el volumen y el grupo de almacenamiento de destino y, a continuación, elija RESTAURAR. 6. Introduzca las credenciales de su mainframe y,	Desarrollador o administrador de almacenamiento de mainframe

Tarea	Descripción	Habilidades requeridas
	a continuación, vuelva a seleccionar RESTAURAR. 7. Para comprobar que la restauración se ha realizado correctamente, compruebe los registros o el ordenador principal.	

Ejecute la política de copia de seguridad o archivado desde el mainframe

Tarea	Descripción	Habilidades requeridas
Ejecute la política de backup o archivado mediante M9CLI.	Utilice la M9CLI para realizar procesos de copia de seguridad y restauración desde TSO/E, REXX o mediante JCL sin configurar reglas en el servidor de administración AMI Cloud de BMC. Uso de TSO/E: Si utiliza TSO/E, asegúrese de que esté concatenado a. `M9CLI REXX TS0` Para hacer una copia de seguridad de un conjunto de datos mediante TSO/E, usa el comando. `TS0 M9CLI BACKDSN <DSNAME>` Nota: Para obtener más información sobre los comandos M9CLI, consulte	Desarrollador o administrador de almacenamiento de mainframe

Tarea	Descripción	Habilidades requeridas
	la referencia de CLI en la documentación de BMC. Uso de JCL: Para ejecutar la política de copia de seguridad y archivado mediante JCL, ejecute el comando `M9CLI`. Uso de operaciones por lotes: El siguiente ejemplo muestra cómo archivar un conjunto de datos mediante la ejecución del `M9CLI` comando por lotes: `//JOBNAME JOB …` `//M9CLI EXEC PGM=IKJEF T01` `//STEPLIB DD DISP=SHR, DSN=<MODEL9 LOADLIB>` `//SYSEXEC DD DISP=SHR, DSN=<MODEL9 EXEC LIB>` `//SYSTSPRT DD SYSOUT=*` `//SYSPRINT DD SYSOUT=*` `//SYSTSIN DD TSO M9CLI` ` ARCHIVE` ` M9CLI ARCHIVE <DSNNAME` ` OR DSN PATTERN>` `/`	

Tarea	Descripción	Habilidades requeridas
Ejecute la política de copia de seguridad o de archivo en el lote JCL.	BMC AMI Cloud proporcio na un ejemplo de rutina JCL denominada M9SAPIJ. Puede personalizar el M9SAPIJ para que ejecute una política específica creada en el servidor de administración con un JCL. Este trabajo también puede formar parte de un programador de lotes para ejecutar automáticamente los procesos de copia de seguridad y restauración. El trabajo por lotes espera los siguientes valores obligatorios: • Dirección IP/nombre de host del servidor de administr ación • Número de puerto • ID de política o nombre de política (que se crea en el servidor de administración) Nota: También puede cambiar otros valores siguiendo las instrucciones del trabajo de muestra.	Desarrollador o administr ador de almacenamiento de mainframe

Recursos relacionados

- Modernización del mainframe con AWS (documentación de AWS)

- How Cloud Backup for Mainframes Cuts Costs with Model9 and AWS (blog AWS Partner Network)
- How to Enable Mainframe Data Analytics on AWS Using Model9 (blog AWS Partner Network)
- Recomendaciones de resiliencia de AWS Direct Connect (documentación de AWS)
- Documentación sobre la nube AMI de BMC (sitio web de BMC)

Cree un visor de archivos de unidad central avanzada en la nube de AWS

Creado por Boopathy GOPALSAMY (AWS) y Jeremiah O'Connor (AWS)

Entorno: PoC o piloto	Tecnologías: unidad central; migración; sin servidor	Carga de trabajo: IBM
Servicios de AWS: Amazon Athena; AWS Lambda; OpenSearch Amazon Service; AWS Step Functions		

Resumen

Este patrón proporciona ejemplos de código y pasos para ayudarlo a crear una herramienta avanzada para buscar y revisar los archivos de formato fijo de su unidad central mediante los servicios sin servidor de AWS. El patrón proporciona un ejemplo de cómo convertir un archivo de entrada de mainframe en un documento de Amazon OpenSearch Service para navegar y buscar. La herramienta de visualización de archivos puede ayudarle a lograr lo siguiente:

- Conservar la misma estructura y diseño de archivos de unidad central para mantener la coherencia en su entorno de migración de AWS objetivo (por ejemplo, puede mantener el mismo diseño para los archivos en una aplicación por lotes que transmite archivos a terceros)
- Acelerar el desarrollo y las pruebas durante la migración de su unidad central
- Dar soporte a las actividades de mantenimiento después de la migración

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una nube privada virtual (VPC) con una subred a la que pueda acceder la plataforma antigua
- Un archivo de entrada y su correspondiente cuaderno de texto en lenguaje común orientado a los negocios (COBOL) (Nota: para ver ejemplos de archivos de entrada y cuadernos de texto COBOL,

consulte en el repositorio). gfs-mainframe-solutions GitHub Para obtener más información sobre los cuadernos de COBOL, consulte la Guía de programación de Enterprise COBOL for z/OS 6.3 en el sitio web de IBM.)

Limitaciones

- El análisis de los copybook está limitado a no más de dos niveles anidados (SE PRODUCE)

Arquitectura

Pila de tecnología de origen

- Archivos de entrada en formato FB (bloqueado fijo)
- Diseño de copybook de COBOL

Pila de tecnología de destino

- Amazon Athena
- OpenSearch Servicio Amazon
- Amazon Simple Storage Service (Amazon S3)
- AWS Lambda
- AWS Step Functions

Arquitectura de destino

El siguiente diagrama muestra el proceso de analizar y convertir un archivo de entrada del ordenador central en un documento de OpenSearch servicio para su navegación y búsqueda.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un usuario administrador o una aplicación envía los archivos de entrada a un bucket de S3 y los copybook de COBOL a otro bucket de S3.
2. El bucket de S3 con los archivos de entrada invoca una función de Lambda que inicia un flujo de trabajo de Step Functions sin servidor. Nota: el uso de un activador de eventos de S3 y una

función de Lambda para impulsar el flujo de trabajo de Step Functions en este patrón es opcional. Los ejemplos de GitHub código de este patrón no incluyen el uso de estos servicios, pero puede usarlos según sus necesidades.

3. El flujo de trabajo de Step Functions coordina todos los procesos por lotes de las siguientes funciones de Lambda:
   - La función `s3copybookparser.py` analiza el diseño del copybook y extrae los atributos de los campos, los tipos de datos y las compensaciones (necesarios para el procesamiento de los datos de entrada).
   - La función `s3toathena.py` crea un diseño de tabla de Athena. Athena analiza los datos de entrada que procesa la función `s3toathena.py` y los convierte en un archivo CSV.
   - La `s3toelasticsearch.py` función ingiere el archivo de resultados del bucket de S3 y lo envía a OpenSearch Service.
4. Los usuarios acceden a los OpenSearch paneles con OpenSearch Service para recuperar los datos en varios formatos de tablas y columnas y, a continuación, ejecutar consultas con los datos indexados.

Herramientas

Servicios de AWS

- Amazon Athena es un servicio interactivo de consultas que le permite analizar datos directamente en Amazon Simple Storage Service (Amazon S3) usando SQL estándar.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice. En este patrón, se utiliza Lambda para implementar la lógica principal, como analizar archivos, convertir datos y cargar datos en OpenSearch Service para un acceso interactivo a los archivos.
- Amazon OpenSearch Service es un servicio gestionado que le ayuda a implementar, operar y escalar clústeres de OpenSearch servicios en la nube de AWS. En este patrón, utiliza OpenSearch Service para indexar los archivos convertidos y proporcionar capacidades de búsqueda interactiva a los usuarios.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

- La Interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su shell de línea de comandos.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Step Functions es un servicio de orquestación sin servidor que le ayuda a combinar funciones de Lambda y otros servicios de AWS para crear aplicaciones esenciales desde el punto de vista empresarial. En este patrón, se utilizan Step Functions para orquestar las funciones de Lambda.

Otras herramientas

- GitHubes un servicio de alojamiento de código que proporciona herramientas de colaboración y control de versiones.
- Python es un lenguaje de programación de alto nivel.

Código

El código de este patrón está disponible en el GitHub gfs-mainframe-patternsrepositorio.

Epics

Prepare el entorno de destino

Tarea	Descripción	Habilidades requeridas
Cree el bucket de S3.	Cree un bucket de S3 para almacenar los copybooks , los archivos de entrada y los archivos de salida. Recomendamos la siguiente estructura de carpetas para su bucket de S3: • `copybook/` • `input/` • `output/`	AWS general

Tarea	Descripción	Habilidades requeridas
	• `query/` • `results/`	
Cree la función s3copybookparser.	1. Cree una función Lambda llamada `s3copybookparser` y cargue el código fuente (`s3copybookparser.py` y `ycopybook.py`) desde el GitHubrepositorio. 2. Adjunte la política de IAM `S3ReadOnly` a la función de Lambda.	AWS general
Cree la función s3toathena.	1. Cree una función Lambda llamada `s3toathena` y cargue el código fuente (`s3toathena.py`) desde el GitHubrepositorio. Configure el tiempo de espera de Lambda en > 60 segundos. 2. Para proporcionar acceso a los recursos necesarios, adjunte las políticas de IAM `AmazonAthenaFullAccess` y `S3FullAccess` a la función de Lambda.	AWS general

Tarea	Descripción	Habilidades requeridas
Cree la función s3toelasticsearch.	1. Añada una dependencia de Python a su entorno Lambda. Importante: para usar la función `s3toelasticsearch`, debe añadir la dependencia de Python, ya que la función de Lambda usa las dependencias de cliente de Python Elasticsearch (`Elasticsearch==7.9.0` y `requests_aws4auth`). 2. Cree una función Lambda llamada `s3toelasticsearch` y cargue el código fuente (`s3toelasticsearch.py`) desde el GitHubrepositorio. 3. Importe la dependencia de Python como una capa Lambda. 4. Adjunte las políticas de IAM `S3ReadOnly` y `AmazonOpenSearchServiceReadOnlyAccess` a la función de Lambda.	AWS general

Tarea	Descripción	Habilidades requeridas
Cree el clúster OpenSearch de servicios.	Cree el clúster 1. Cree un clúster OpenSearch de servicios. Al crear el clúster, haga lo siguiente: • Cree un usuario maestro y una contraseña para el clúster que pueda usar para iniciar sesión en OpenSearch Dashboards. Nota: este paso no es obligatorio si utiliza la autenticación a través de Amazon Cognito. • Seleccione control de acceso preciso. Esto le proporciona formas adicionales de controlar el acceso a sus datos en OpenSearch Service. 2. Copie la URL del dominio y pásela como variable de entorno 'HOST' a la función de Lambda `s3toelasticsearch` . Conceder acceso al rol de IAM Para proporcionar un acceso detallado al rol de IAM de la función de Lambda (`arn:aws:iam::**:role/service-role/s3`	AWS general

Tarea	Descripción	Habilidades requeridas
	`toelasticsearch-role-**`), haga lo siguiente: 1. Inicie sesión en OpenSearch Dashboards como usuario maestro. 2. Seleccione la pestaña Security (Seguridad) y, a continuación, elija Roles, all_access, Map user (Asignar usuari)o y Backend roles (Roles de backend). 3. Añada el nombre de recurso de Amazon (ARN) del rol de IAM de la función de Lambda y, a continuación, seleccione Save (Guardar). Para obtener más información, consulte Asignar funciones a los usuarios en la documentación del OpenSearch servicio.	

Tarea	Descripción	Habilidades requeridas
Cree Step Functions para la orquestación.	1. Cree un equipo de estado de Step Functions con el flujo estándar. La definició n se incluye en el GitHub repositorio. 2. En el script JSON, sustituya los ARN de la función de Lambda por los ARN de la función de Lambda de su entorno.	AWS general

Implemente y ejecute

Tarea	Descripción	Habilidades requeridas
Cargue los archivos de entrada y los copybooks en un bucket de S3;.	Descargue los archivos de ejemplo de la carpeta de ejemplos del GitHub repositor io y cárguelos en el bucket de S3 que creó anteriormente. 1. Cargue `Mockedcop y.cpy` y `acctix.cpy` en la carpeta `<S3_Bucke t>/copybook` . 2. Suba los archivos de entrada de muestra `Modedupdate.txt` y `acctindex.cpy` a la carpeta `<S3_Bucket>/ input`.	AWS general
Invoque los Step Functions.	1. Inicie sesión en la consola de administración de AWS	AWS general

Tarea	Descripción	Habilidades requeridas
	y abra la consola de Step Functions. 2. En el panel de navegación izquierdo, elija State machines (Equipos de estado). 3. Elija su equipo de estado y, a continuación, elija Start execution (Iniciar ejecución). 4. En el cuadro Input (Entrada), introduzca la siguiente ruta del copybook o archivo como variable JSON al bucket de S3 y, a continuación, seleccione Start execution (Iniciar ejecución). `{ "s3_copybook_bucket_name": "<BUCKET NAME>", "s3_copybook_bucket_key": "<COPYBOOK PATH>", "s3_source_bucket_name": "<BUCKET NAME", "s3_source_bucket_key": "INPUT FILE PATH" }` Por ejemplo: `{`	

Tarea	Descripción	Habilidades requeridas
	<pre>"s3_copybook_bucket_name": "fileaidtest", "s3_copybook_bucket_key": "copybook/acctix.cpy", "s3_source_bucket_name": "fileaidtest", "s3_source_bucket_key": "input/acctindex" }</pre>	

Tarea	Descripción	Habilidades requeridas
Valide la ejecución del flujo de trabajo en Step Functions.	En la consola de Step Functions, revise la ejecución del flujo de trabajo en el inspector de gráficos. Los estados de ejecución están codificados por colores para representar el estado de ejecución. Por ejemplo, el azul indica In progress (En curso), el verde indica Succeeded (Correcto) y el rojo indica Failed (Con error). También puede revisar la tabla de la sección Historial de eventos de ejecución para obtener información más detallada sobre los eventos de ejecución. Para ver un ejemplo de la ejecución de un flujo de trabajo gráfico, consulte el gráfico de Step Functions en la sección Información adicional de este patrón.	AWS general

Tarea	Descripción	Habilidades requeridas
Valida los registros de entrega en Amazon CloudWatch.	1. Inicie sesión en la consola de administración de AWS y abra la consola de CloudWatch . 2. En el panel de navegación, elija Logs (Registros) y, luego, Log groups (Grupos de registros). 3. En el cuadro de búsqueda, busque el grupo de registros de la función `s3toelasticsearch` . Para ver un ejemplo de registros de entregas correctos, consulta los registros de CloudWatch entrega en la sección de información adicional de este patrón.	AWS general

Tarea	Descripción	Habilidades requeridas
Valide el archivo formateado en los OpenSearch paneles de control y lleve a cabo las operaciones con los archivos.	1. Inicie sesión en la Consola de administración de AWS. En Analytics, seleccion a Amazon OpenSearch Service. 2. En el panel de navegación, elija Dominios. 3. En el cuadro de búsqueda, introduce la URL de tu dominio en los OpenSearch paneles. 4. Elija su panel de control y, a continuación, inicie sesión como usuario maestro. 5. Examine los datos indexados en formato de tabla. 6. Compare el archivo de entrada con el archivo de salida formateado (documento indexado) en los paneles. OpenSearch La vista del panel muestra los encabezados de columna añadidos a los archivos formateados. Confirme que los datos de origen de los archivos de entrada sin formato coincidan con los datos de destino de la vista de panel. 7. Realice acciones como la búsqueda (por ejemplo,	AWS general

Tarea	Descripción	Habilidades requeridas
	mediante nombres de campo, valores o expresiones), el filtrado y las operaciones de DQL (Dashboard Query Language, lenguaje de consulta de paneles) en el archivo indexado.	

Recursos relacionados

Referencias

- Ejemplo de copybook de COBOL (documentación de IBM)
- Ayuda de archivo BMC Compuware (documentación de BMC)

Tutoriales

- Tutorial: uso de un desencadenador de Amazon S3 para invocar una función de Lambda (documentación de AWS Lambda)
- ¿Cómo creo un flujo de trabajo sin servidor con AWS Step Functions y AWS Lambda? (documentación de AWS)
- Uso de OpenSearch paneles con Amazon OpenSearch Service (documentación de AWS)

Información adicional

Gráfico de Step Functions

En el siguiente ejemplo se muestra un gráfico de Step Functions. El gráfico muestra el estado de ejecución de las funciones de Lambda utilizadas en este patrón.

CloudWatch registros de entrega

El siguiente ejemplo muestra los registros de entrega correctos para la ejecución de la ejecución `s3toelasticsearch`.

2022-08-10T15:53:33.033-05:00	Número de documentos en trámite: 100	
	2022-08-10T15:53:33.171-05:00	[INFO] 2022-08-10T20:53:33.171Z a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 POST https://search-essearch-3h4uqclifeqaj2vg4mphe7ffle.us-east-2.es.amazonaws.com:443/_bulk [status:200 request:0.100s]
	2022-08-10T15:53:33.172-05:00	Escritura masiva correcta: 100 documentos

Almacenamiento en contenedores de las cargas de trabajo de mainframe que Blu Age ha modernizado

Creado por Richard Milner-Watts (AWS)

Repositorio de código: ejemplo de contenedor de aplicaciones Blu Age	Entorno: producción	Origen: Cargas de trabajo de mainframe
Destino: Contenedores	Tipo R: renovar arquitectura	Carga de trabajo: IBM; todas las demás cargas de trabajo
Tecnologías: mainframe; contenedores y microservicios; migración; modernización	Servicios de AWS: Amazon ECS; Amazon ECR	

Resumen

Este patrón proporciona un ejemplo de entorno de contenedores para ejecutar cargas de trabajo de mainframe que se han modernizado con la herramienta Blu Age. Blu Age convierte las cargas de trabajo de mainframe heredadas en código Java moderno. Este patrón proporciona un envoltorio alrededor de la aplicación de Java para que pueda ejecutarla mediante servicios de orquestación de contenedores como Amazon Elastic Container Service (Amazon ECS) o Amazon Elastic Kubernetes Service (Amazon EKS).

Para obtener más información sobre la modernización de sus cargas de trabajo mediante el uso de Blu Age y los servicios de AWS, consulte estas publicaciones en las recomendaciones de AWS:

- Ejecución de cargas de trabajo de mainframe modernizadas de Blu Age en una infraestructura de AWS sin servidor
- Implementar un entorno para aplicaciones de Blu Age en contenedores mediante Terraform

Si necesita ayuda para utilizar Blu Age para modernizar las cargas de trabajo de sus mainframes, póngase en contacto con el equipo de Blu Age seleccionando la opción Contactar con nuestros

expertos en el sitio web de Blu Age. Si necesita ayuda para migrar sus cargas de trabajo modernizadas a AWS, integrarlas con los servicios de AWS y pasarlas a producción, póngase en contacto con su administrador de cuentas de AWS o rellene el formulario de AWS Professional Services.

Requisitos previos y limitaciones

Requisitos previos

- Una aplicación Java modernizada creada por Blu Age. Para fines de prueba, este patrón proporciona un ejemplo de aplicación Java que puede utilizar como prueba de concepto.
- Un entorno de Docker que puede utilizar para crear el contenedor.

Limitaciones

Según la plataforma de orquestación de contenedores que utilice, es posible que los recursos que se puedan poner a disposición del contenedor (como la CPU, la RAM y el almacenamiento) estén limitados. Por ejemplo, si utiliza Amazon ECS con AWS Fargate, consulte la documentación de Amazon ECS para conocer los límites y las consideraciones.

Arquitectura

Pila de tecnología de origen

- Blu Age
- Java

Pila de tecnología de destino

- Docker

Arquitectura de destino

En el siguiente diagrama, se muestra la arquitectura de la aplicación Blu Age dentro de un contenedor de Docker.

1. El punto de entrada al contenedor es el script contenedor. Este script bash es responsable de preparar el entorno de tiempo de ejecución para la aplicación Blu Age y de procesar los resultados.
2. Las variables de entorno del contenedor se utilizan a fin de configurar variables en el script del contenedor, como los nombres de bucket de Amazon Simple Storage Service (Amazon S3) y las credenciales de la base de datos. Las variables de entorno las proporcionan AWS Secrets Manager o Parameter Store, una funcionalidad de AWS Systems Manager. Si utiliza Amazon ECS como servicio de orquestación de contenedores, también puede codificar las variables de entorno en la definición de tareas de Amazon ECS.
3. El script contenedor se encarga de introducir todos los archivos de entrada del bucket de S3 en el contenedor antes de ejecutar la aplicación Blu Age. La interfaz de la línea de comandos de AWS (AWS CLI) se instala en el contenedor. Esto proporciona un mecanismo de acceso a los objetos que se almacenan en Amazon S3 a través del punto de conexión de la nube privada virtual (VPC) de la puerta de enlace.
4. Es posible que el archivo Java Archive (JAR) de la aplicación Blu Age necesite comunicarse con otras orígenes de datos, como Amazon Aurora.
5. Una vez finalizado, el script contenedor entrega los archivos de salida resultantes a un bucket de S3 para su posterior procesamiento (por ejemplo, por parte de Amazon CloudWatch Logging Services). El patrón también permite enviar archivos de registro comprimidos a Amazon S3, si utiliza una alternativa al CloudWatch registro estándar.

Herramientas

Servicios de AWS

- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable.
- Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores escalable y rápido que ayuda a ejecutar, detener y administrar contenedores en un clúster.

Herramientas

- Docker es una plataforma de software para crear, probar e implementar aplicaciones. Docker agrupa el software en unidades estandarizadas denominadas contenedores, que contienen todo lo que el software necesita para ejecutarse, incluidas las bibliotecas, las herramientas del sistema, el

código y el tiempo de ejecución. Puede usar Docker a fin de implementar y escalar aplicaciones en cualquier entorno.

- Bash es una interfaz de lenguaje de comandos (shell) para el sistema operativo GNU.
- Java es el lenguaje de programación y el entorno de desarrollo utilizados en este patrón.
- Blu Age es una herramienta de AWS Mainframe Modernization que convierte las cargas de trabajo de mainframe heredadas, incluidos el código de las aplicaciones, las dependencias y la infraestructura, en cargas de trabajo modernas para la nube.

Repositorio de código

El código de este patrón está disponible en el repositorio de contenedores de muestras de GitHub Blu Age.

Prácticas recomendadas

- Externalice las variables para alterar el comportamiento de su aplicación mediante variables de entorno. Estas variables permiten que la solución de orquestación de contenedores modifique el entorno de tiempo de ejecución sin tener que volver a construir el contenedor. Este patrón incluye ejemplos de variables de entorno que pueden ser útiles para las aplicaciones de Blu Age.
- Valide cualquier dependencia de la aplicación antes de ejecutar la aplicación Blu Age. Por ejemplo, compruebe que la base de datos esté disponible y que las credenciales sean válidas. Escriba las pruebas en el script contenedor para comprobar las dependencias y, si no se cumplen, no las consiga antes de tiempo.
- Utilice el registro detallado dentro del script contenedor. Interactuar directamente con un contenedor en ejecución puede resultar difícil, dependiendo de la plataforma de orquestación y del tiempo que lleve el trabajo. Asegúrese de que los resultados útiles estén escritos para ayudar a `STDOUT` a diagnosticar cualquier problema. Por ejemplo, el resultado puede incluir el contenido del directorio de trabajo de la aplicación antes y después de ejecutarla.

Epics

Obtenga un archivo JAR de la aplicación Blu Age

Tarea	Descripción	Habilidades requeridas
Opción 1: trabajar con Blu Age a fin de obtener el archivo JAR de su aplicación.	El contenedor de este patrón requiere una aplicación Blu Age. Como alternativa, puede usar la aplicación Java de ejemplo que viene con este patrón para un prototipo. Trabaje con el equipo de Blu Age para obtener un archivo JAR para su aplicación que pueda incluir en el contenedor. Si el archivo JAR no está disponible, consulte la siguiente tarea para usar la aplicación de ejemplo en su lugar.	Arquitecto de la nube
Opción 2: Cree o utilice el archivo JAR de la aplicación de muestra suministrado.	Este patrón proporciona un archivo JAR de muestra prediseñado. Este archivo genera las variables de entorno de la aplicación a `STDOUT` antes de dormir durante 30 segundos y salir. Este archivo recibe un nombre `bluAgeSample.jar` y se encuentra en la carpeta docker del GitHub repositorio. Si desea modificar el código y crear su propia versión del	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	archivo JAR, utilice el código fuente que se encuentra en. / java_sample/src/sample_java_app.java en el GitHub repositorio. Puede usar el script de compilación en ./java_sample/build.sh para compilar el código fuente de Java y crear un nuevo archivo JAR.	

Construya el contenedor de Blue Age

Tarea	Descripción	Habilidades requeridas
Clona el GitHub repositorio.	Clone el repositorio de código de muestra mediante el comando: `git clone https://github.com/aws-samples/aws-blu-age-sample-container`	AWS DevOps
Utilice Docker para crear el contenedor.	Utilice Docker para crear el contenedor antes de enviarlo a un registro de Docker, como Amazon ECR: 1. Desde la terminal que elija, vaya a la `docker` carpeta del GitHub repositorio local. 2. Use este comando para construir el contenedor:	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`docker build -t <tag> .` donde `<tag>` e sel nombre del contenedor que quiere usar.	
Pruebe el contenedor Blu Age.	(Opcional) Si es necesario , pruebe el contenedor en las instalaciones mediante el comando: `docker run -it <tag> / bin/bash`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Autenticar en su repositorio de Docker.	Si planea usar Amazon ECR, siga las instrucciones de la documentación de Amazon ECR para instalar y configurar la AWS CLI y autenticar la CLI de Docker en su registro predeterminado. Le recomendamos que utilice el get-login-password comando para la autenticación. Nota: La consola Amazon ECR proporciona una versión rellenada previamente de este comando si utiliza el botón Ver comandos push. Para obtener más información, consulte la documentación de Amazon ECR. `aws ecr get-login -password --region <region> | docker login --username AWS --password-stdin <account>.dkr.ecr.<region>.amazonaws.com` Si no piensa utilizar Amazon ECR, siga las instrucciones que se proporcionan para su sistema de registro de contenedores.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Cree un repositorio de contenedores.	Cree un repositorio en Amazon ECR. Para obtener instrucciones, consulte el patrón Implementar un entorno para aplicaciones de Blu Age en contenedores mediante Terraform. Si utiliza otro sistema de registro de contenedores, siga las instrucciones que se proporcionan para ese sistema.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Etiquete su contenedor y colóquelo en el repositorio de destino.	Si utiliza Amazon ECR: 1. Etiquete la imagen de Docker en las instalaciones con el registro y el repositorio de Amazon ECR para poder enviarla a su repositorio remoto: `docker tag <tag>:latest <account>.dkr.ecr.<region>.amazonaws.com/<repository>:<versionNumber>` 2. Inserte la imagen en el repositorio remoto: `docker push <account>.dkr.ecr.<region>.amazonaws.com/<repository>:<versionNumber>` Para obtener más información, consulte Insertar una imagen de Docker en la Guía del usuario de Amazon ECR.	AWS DevOps

Recursos relacionados

Recursos de AWS

- Repositorio de contenedores de muestras de AWS Blu Age

- Ejecución de cargas de trabajo de mainframe modernizadas de Blu Age en una infraestructura de AWS sin servidor
- Implementar un entorno para aplicaciones de Blu Age en contenedores mediante Terraform
- Uso de Amazon ECR con la AWS CLI (Guía del usuario de Amazon ECR)
- Autenticación de registro privado (Guía del usuario de Amazon ECR)
- Documentación de Amazon ECS
- Documentación de Amazon EKS

Recursos adicionales

- Sitio web de Blu Age
- Sitio web de Docker

Convierta y desempaquete datos EBCDIC a ASCII en AWS mediante Python

Creado por Luis Gustavo Dantas (AWS)

Repositorio de código: Mainframe Data Utilities	Entorno: PoC o piloto	Origen: datos EBCDIC de mainframe
Destino: datos ASCII distribuidos o modernizados en la nube	Tipo R: redefinir la plataforma	Carga de trabajo: IBM
Tecnologías: mainframe; bases de datos; almacenamiento y respaldo; modernización	Servicios de AWS: Amazon EBS; Amazon EC2	

Resumen

Dado que los mainframe suelen alojar datos empresariales críticos, la modernización de estos datos es una de las tareas más importantes a la hora de migrar datos a la nube de Amazon Web Services (AWS) o a otro entorno de American Standard Code for Information Interchange (ASCII). En los mainframe, los datos suelen codificarse en un formato ampliado de código de intercambio decimal codificado en binario (EBCDIC). La exportación de bases de datos, los métodos de acceso al almacenamiento virtual (VSAM) o los archivos planos suelen producir archivos EBCDIC binarios empaquetados, que son más complejos de migrar. La solución de migración de bases de datos más usada es la captura de datos de cambios (CDC), que, en la mayoría de los casos, convierte automáticamente la codificación de los datos. Sin embargo, es posible que los mecanismos de CDC no estén disponibles para estas bases de datos, VSAM o archivos planos. En el caso de estos archivos, es necesario adoptar un enfoque alternativo para modernizar los datos.

Este patrón describe cómo modernizar los datos EBCDIC convirtiéndolos a formato ASCII. Tras la conversión, puede cargar los datos en bases de datos distribuidas o hacer que las aplicaciones en la nube procesen los datos directamente. El patrón utiliza el script de conversión y los archivos de muestra del mainframe-data-utilities GitHub repositorio.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Un archivo de entrada EBCDIC y su correspondiente cuaderno en lenguaje común orientado a negocios (COBOL). En el repositorio se incluyen un archivo EBCDIC de muestra y un cuaderno de notas COBOL. mainframe-data-utilities GitHub Para obtener más información sobre los cuadernos COBOL, consulte la Guía del programador de Enterprise COBOL para z/OS 6.4 en el sitio web de IBM.

Limitaciones

- No es compatible con diseños de archivo definidos en COBOL. Deben estar disponibles por separado.

Versiones de producto

- Python, versión 3.8 o posterior

Arquitectura

Pila de tecnología de origen

- Datos EBCDIC en un mainframe
- Cuaderno COBOL

Pila de tecnología de destino

- Una instancia de Amazon Elastic Compute Cloud (Amazon EC2) en una nube privada virtual (VPC)
- Amazon Elastic Block Store (Amazon EBS)
- Python y sus paquetes necesarios, JavaScript Object Notation (JSON), sys y datetime
- Archivo plano ASCII listo para ser leído por una aplicación moderna o cargado en una tabla de base de datos relacional

Arquitectura de destino

El diagrama de arquitectura muestra el proceso de conversión de un archivo EBCDIC a un archivo ASCII en una instancia de EC2:

1. Con el script parse_copybook_to_json.py, el cuaderno COBOL se convierte en un archivo JSON.
2. Con el archivo JSON y el script extract_ebcdic_to_ascii.py, los datos EBCDIC se convierten en un archivo ASCII.

Automatizar y escalar

Una vez que disponga de los recursos necesarios para las primeras conversiones manuales de archivos, puede automatizar la conversión de archivos. Este patrón no incluye instrucciones para la automatización. La conversión se puede automatizar de varias formas. A continuación, se muestra un posible enfoque:

1. Encapsular la interfaz de la línea de comandos de AWS (AWS CLI) y los comandos de script de Python en un script de intérprete de comandos.
2. Crear una función de Lambda de AWS que envíe de forma asíncrona el trabajo del script de intérprete de comandos a una instancia de EC2. Para obtener más información, consulte Programar trabajos de SSH con AWS Lambda.
3. Crear un desencadenante de Amazon Simple Storage Service (Amazon S3) que invoque la función de Lambda cada vez que se cargue un archivo heredado. Para obtener más información, consulte Utilizar un desencadenador de Amazon S3 para invocar una función de Lambda.

Herramientas

Servicios de AWS

- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon Elastic Block Store (Amazon EBS) proporciona volúmenes de almacenamiento por bloques para su uso con instancias de Amazon Elastic Compute Cloud (Amazon EC2).
- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.

- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.

Otras herramientas

- GitHubes un servicio de alojamiento de código que proporciona herramientas de colaboración y control de versiones.
- Python es un lenguaje de programación de alto nivel.

Repositorio de código

El código de este patrón está disponible en el mainframe-data-utilities GitHub repositorio.

Epics

Prepare la instancia de EC2

Tarea	Descripción	Habilidades requeridas
Lanzar una instancia EC2.	La instancia de EC2 debe tener acceso saliente a Internet. Esto permite que la instancia acceda al código fuente de Python disponibl e en GitHub. Para crear una instancia: 1. Abra la consola Amazon EC2 en https://console.aw s.amazon.com/ec2. 2. Lance una instancia de EC2 de Linux. Use una dirección IP pública y permita el acceso entrante a través del puerto 22. Asegúrese de que el tamaño de almacenamiento de la	AWS general

Tarea	Descripción	Habilidades requeridas
	instancia sea, al menos, el doble del tamaño del archivo de datos EBCDIC. Para obtener instrucciones, consulte la documentación de Amazon EC2.	
Instale Git	1. Con un cliente de secure shell (SSH), conéctese a la instancia de EC2 que acaba de lanzar. Para obtener más información, consulte Conexión con la instancia de Linux. 2. En la consola de Amazon EC2, ejecute el siguiente comando. Se instalará Git en la instancia de EC2. `sudo yum install git` 3. Ejecute el comando siguiente y confirme que Git ha sido instalado correctam ente. `git --version`	AWS general, Linux

Tarea	Descripción	Habilidades requeridas
Instalación de Python.	1. En la consola de Amazon EC2, ejecute el siguiente comando. Esto instala Python en la instancia de EC2. `sudo yum install python3` 2. En la consola de Amazon EC2, ejecute el siguiente comando. Esto instala Pip3 en la instancia de EC2. `sudo yum install python3-pip` 3. En la consola de Amazon EC2, ejecute el siguiente comando. Se instalará AWS SDK para Python (Boto3) en la instancia de EC2. `sudo pip3 install boto3` 4. En la consola de Amazon EC2, ejecute el siguiente comando, donde `<us-east-1>` es el código de su región de AWS. Para obtener una lista de códigos de región, consulte Regiones disponibles en la documentación de Amazon EC2.	AWS general, Linux

Tarea	Descripción	Habilidades requeridas
	`export AWS_DEFAU LT_REGION=<us-east -1>`	
Clone el GitHub repositorio.	1. En la consola de Amazon EC2, ejecute el siguiente comando. De este modo, se clona el mainframe-data-uti litiesrepositorio GitHub y se abre la ubicación de copia predeterminada, la home carpeta. `git clone https://g ithub.com/aws-samp les/mainframe-data- utilities.git` 2. En la carpeta home, confirme que existe la carpeta `mainframe- data-utilities` .	AWS general, GitHub

Cree el archivo ASCII a partir de los datos del EBCDIC

Tarea	Descripción	Habilidades requeridas
Convierta el cuaderno COBOL en el archivo de diseño JSON.	En la carpeta `mainframe -data-utilities` , ejecute el script parse_cop ybook_to_json.py. Este módulo de automatización lee el diseño del archivo de un cuaderno COBOL y crea un archivo JSON. Este archivo	AWS general, Linux

Tarea	Descripción	Habilidades requeridas
	JSON contiene la informaci ón necesaria para interpret ar y extraer los datos del archivo fuente. Se crearán los metadatos de JSON a partir del cuaderno COBOL. El siguiente comando convierte el cuaderno COBOL en un archivo JSON. `python3 parse_cop ybook_to_json.py \ -copybook LegacyRef erence/COBPACK2.cpy \ -output sample-data/ cobpack2-list.json \ -dict sample-data/ cobpack2-dict.json \ -ebcdic sample-data/ COBPACK.OUTFILE.txt \ -ascii sample-data/ COBPACK.ASCII.txt \ -print 10000` El script imprime los argumentos recibidos. `---------- ---------- ---------- ---------- Copybook file..... .....| LegacyRef erence/COBPACK2.cpy Parsed copybook (JSON List).| sample-data/ cobpack2-list.json`	

Tarea	Descripción	Habilidades requeridas
	`JSON Dict (document ation)...| sample-da ta/cobpack2-dict.json ASCII file..... .....| sample- data/COBPACK.ASCII.t xt EBCDIC file..... .....| sample- data/COBPACK.OUTFILE .txt Print each..... .....| 10000 ---------- ---------- ---------- ----------` Para obtener más informaci ón sobre los argumentos, consulte el archivo README del GitHub repositorio.	

Tarea	Descripción	Habilidades requeridas
Inspeccione el archivo de diseño JSON.	1. Acceda a la ruta de salida definida en el script parse_copybook_to_json.py. 2. Compruebe la hora de creación del archivo sample-data/cobpack2-list.json para confirmar que ha seleccionado el archivo de diseño JSON adecuado. 3. Examine el archivo JSON y confirme que el contenido es similar a este. `"input": "extract-ebcdic-to-ascii/COBPACK.OUTFILE.txt", "output": "extract-ebcdic-to-ascii/COBPACK.ASCII.txt", "max": 0, "skip": 0, "print": 10000, "lrecl": 150, "rem-low-values": true, "separator": "|", "transf": [ { "type": "ch", "bytes": 19, "name": "OUTFILE-TEXT" }`	AWS general, JSON

Tarea	Descripción	Habilidades requeridas
	Los atributos más importantes del archivo de diseño JSON son: • `input` – Contiene la ruta del archivo EBCDIC que se va a convertir • `output` – Define la ruta en la que se generará el archivo ASCII • `lrecl` – Especifica el tamaño en bytes de la longitud del registro lógico • `transf` – Muestra todos los campos y su tamaño en bytes Para obtener más informaci ón sobre el archivo de diseño JSON, consulta el archivo README del GitHub repositor io.	

Tarea	Descripción	Habilidades requeridas
Cree el archivo ASCII.	Ejecute el script extract_ebcdic_to_ascii.py, que se incluye en el repositorio clonado GitHub . Este script lee el archivo EBCDIC y escribe un archivo ASCII convertido y legible. `python3 extract_ebcdic_to_ascii.py -local-json sample-data/cobpack2-list.json` A medida que el script procesa los datos del EBCDIC, imprime un mensaje por cada lote de 10 000 registros. Consulte el siguiente ejemplo. `---------- 2023-05-15 21:21:46.322253 | Local Json file | -local-json | sample-data/cobpack2-list.json 2023-05-15 21:21:47.034556 | Records processed | 10000 2023-05-15 21:21:47.736434 | Records processed | 20000 2023-05-15 21:21:48.441696 | Records processed | 30000`	AWS general

Tarea	Descripción	Habilidades requeridas
	2023-05-15 21:21:49. 173781 | Records processed | 40000 2023-05-15 21:21:49. 874779 | Records processed | 50000 2023-05-15 21:21:50. 705873 | Records processed | 60000 2023-05-15 21:21:51. 609335 | Records processed | 70000 2023-05-15 21:21:52. 292989 | Records processed | 80000 2023-05-15 21:21:52. 938366 | Records processed | 89280 2023-05-15 21:21:52. 938448 Seconds 6.616232 Para obtener informaci ón sobre cómo cambiar la frecuencia de impresión, consulte el archivo README del GitHub repositorio.	

Tarea	Descripción	Habilidades requeridas
Examinar el archivo ASCII.	1. Compruebe la hora de creación del archivo extract-ebcdic-to-ascii/cobpack.ascii.txt para comprobar que se ha creado recientemente. 2. En la consola de Amazon EC2, ejecute el siguiente comando. Se abrirá el primer registro del archivo ASCII. `head sample-data/COBPACK.ASCII.txt -n 1| xxd` 3. Examine el contenido del primer registro. Ya que los archivos EBCDIC suelen ser binarios, no tienen caracteres especiales de retorno y alimentación de línea (CRLF). El script extract_ebcdic_to_ascii.py añade un carácter de barra vertical como separador de columnas, que se define en los parámetros del script. Si ha usado el archivo EBCDIC proporcionado como ejemplo, el primer registro del archivo ASCII será este.	AWS general, Linux

Tarea	Descripción	Habilidades requeridas
	00000000: 2d30 3030 3030 3030 3030 3130 3030 3030 -000000000100000 00000010: 3030 307c 3030 3030 3030 3030 3031 3030 000|00000 0000100 00000020: 3030 3030 3030 7c2d 3030 3030 3030 3030 000000|-0 0000000 00000030: 3031 3030 3030 3030 3030 7c30 7c30 7c31 0100000000| 0|0|1 00000040: 3030 3030 3030 3030 7c2d 3130 3030 3030 00000000| -100000 00000050: 3030 307c 3130 3030 3030 3030 307c 2d31 000|10000 0000|-1 00000060: 3030 3030 3030 3030 7c30 3030 3030 7c30 00000000| 00000|0 00000070: 3030 3030 7c31 3030 3030 3030 3030 7c2d 0000|1000 00000|- 00000080: 3130 3030 3030 3030 307c 3030 3030 3030 100000000| 000000 00000090: 3030 3030 3130 3030 3030 3030 307c 2d30 000010000 0000|-0 000000a0: 3030 3030 3030 3030 3031 3030	

Tarea	Descripción	Habilidades requeridas
	3030 3030 000000000 1000000 000000b0: 3030 7c41 7c41 7c0a 00|A|A|.	

Tarea	Descripción	Habilidades requeridas
Evalúe el archivo EBCDIC.	En la consola de Amazon EC2, ejecute el siguiente comando. Esto abre el primer registro del archivo EBCDIC. `head sample-data/COBPACK.OUTFILE.txt -c 150 | xxd` Si ha usado el archivo EBCDIC de ejemplo, el resultado es el siguiente. `00000000: 60f0 f0f0 f0f0 f0f0 f0f0 f0f0 f1f0 f0f0 f0f0 f0f0 `........ .... 00000010: f0f0 f0f0 f0f0 f0f0 f0f0 f0f0 f0f0 f0f0 f1f0 f0f0 .... 00000020: f0f0 f0f0 f0f0 f0f0 f0f0 f0f0 f0f0 f1f0 .... 00000030: f0f0 f0f0 f0f0 d000 0000 0005 f5e1 00fa .... 00000040: 0a1f 0000 0000 0005 f5e1 00ff ffff fffa .... 00000050: 0a1f 0000 000f 0000 0c10 0000 000f 1000 .... 00000060: 0000 0d00 0000 0000 1000 0000`	AWS general, Linux, EBCDIC

Tarea	Descripción	Habilidades requeridas
	0f00 0000 .... 00000070: 0000 1000 0000 0dc1 c100 0000 0000 0000 .... 00000080: 0000 0000 0000 0000 0000 0000 0000 0000 .... 00000090: 0000 0000 0000 ...... Para evaluar la equivalencia entre los archivos de origen y de destino, es necesario un conocimiento exhaustivo de EBCDIC. Por ejemplo, el primer carácter del archivo EBCDIC de muestra es un guion (-). En la notación hexadecimal del archivo EBCDIC, este carácter se representa mediante 60, y en la notación hexadecimal del archivo ASCII, este carácter se representa mediante 2D. Para obtener una tabla de conversión de EBCDIC a ASCII, consulte EBCDIC a ASCII en el sitio web de IBM.	

Recursos relacionados

Referencias

- El conjunto de caracteres EBCDIC (documentación de IBM)
- EBCDIC a ASCII (documentación de IBM)
- COBOL (documentación de IBM)
- Conceptos básicos de JCL (documentación de IBM)
- Conéctese con su instancia de Linux (documentación de Amazon EC2)

Tutoriales

- Programar trabajos de SSH con AWS Lambda (publicación del blog de AWS)
- Uso de un desencadenador de Amazon S3 para invocar una función de Lambda (documentación de AWS Lambda)

Convertir archivos de mainframe del formato EBCDIC al formato ASCII delimitado por caracteres en Amazon S3 con AWS Lambda

Creado por Luis Gustavo Dantas (AWS)

Repositorio de código: Mainframe Data Utilities	Entorno: PoC o piloto	Origen: archivos EBCDIC de IBM
Destino: archivos ASCII delimitados	Tipo R: redefinir la plataforma	Carga de trabajo: IBM
Tecnologías: unidad central	Servicios de AWS: AWS CloudShell; AWS Lambda; Amazon S3; Amazon CloudWatch	

Resumen

Este patrón le muestra cómo lanzar una función de AWS Lambda que convierte automáticamente los archivos EBCDIC (código de intercambio decimal codificado en binario extendido) del mainframe en archivos ASCII (Código estándar estadounidense para el intercambio de información) delimitados por caracteres. La función de Lambda se ejecuta después de cargar los archivos ASCII en un bucket de Amazon Simple Storage Service (Amazon S3). Tras la conversión de archivos, puede leer los archivos ASCII en cargas de trabajo basadas en x86 o cargarlos en bases de datos modernas.

El enfoque de conversión de archivos que se muestra en este patrón puede ayudarle a superar los desafíos que supone trabajar con archivos EBCDIC en entornos modernos. Los archivos codificados en EBCDIC suelen contener datos representados en formato binario o decimal empaquetado, y los campos tienen una longitud fija. Estas características crean obstáculos porque las cargas de trabajo modernas basadas en x86 o los entornos distribuidos suelen trabajar con datos codificados en ASCII y no pueden procesar archivos EBCDIC.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un bucket de S3
- Usuario de AWS Identity and Access Management (IAM) con permisos administrativos
- AWS CloudShell
- Python 3.8.0 o posterior
- Archivo plano codificado en EBCDIC y su estructura de datos correspondiente en un cuaderno de texto común en un lenguaje empresarial común (COBOL)

Nota: Este patrón utiliza un archivo EBCDIC de muestra (Client.EBCDIC.txt) y su cuaderno de texto COBOL correspondiente (COBKS05.cpy). Ambos archivos están disponibles en el GitHub mainframe-data-utilitiesrepositorio.

Limitaciones

- Los cuadernos de COBOL suelen contener múltiples definiciones de diseño. El mainframe-data-utilitiesproyecto puede analizar este tipo de cuaderno, pero no puede deducir qué diseño considerar en la conversión de datos. Esto se debe a que los cuadernos no tienen esta lógica (que permanece en los programas COBOL). Por lo tanto, debe configurar manualmente las reglas para seleccionar los diseños después de analizar el cuaderno.
- Este patrón está sujeto a las cuotas de Lambda.

Arquitectura

Pila de tecnología de origen

- IBM z/OS, IBM i y otros sistemas EBCDIC
- Archivos secuenciales con datos codificados en EBCDIC (como descargas de IBM Db2)
- Cuaderno COBOL

Pila de tecnología de destino

- Amazon S3
- Notificaciones de eventos de Amazon S3
- IAM
- Función de Lambda

- Python 3.8 o posterior
- Utilidades de datos de unidad central
- Metadatos JSON
- Archivos ASCII delimitados por caracteres

Arquitectura de destino

El siguiente diagrama muestra una arquitectura para convertir archivos EBCDIC de mainframe en archivos ASCII.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El usuario ejecuta el script del analizador del cuaderno para convertir el cuaderno COBOL en un archivo JSON.
2. El usuario carga los metadatos JSON en un bucket de &S3;. Esto hace que los metadatos sean legibles por la función de Lambda de conversión de datos.
3. El usuario o un proceso automatizado carga el archivo EBCDIC en el bucket de &S3;.
4. El evento de notificación de S3 activa la función de Lambda de conversión de datos.
5. AWS verifica los permisos de lectura y escritura del bucket de S3 para la función de Lambda.
6. Lambda lee el archivo del bucket de S3 y lo convierte localmente de EBCDIC a ASCII.
7. Lambda registra el estado del proceso en Amazon. CloudWatch
8. Lambda vuelve a escribir el archivo ASCII en Amazon S3.

Nota: El script del analizador digital se ejecuta solo una vez, después de convertir los metadatos a JSON y, a continuación, cargar esos datos en un bucket de S3. Tras la conversión inicial, cualquier archivo EBCDIC que utilice el mismo archivo JSON que se haya cargado en el bucket de S3 utilizará los mismos metadatos.

Herramientas

Herramientas de AWS

- Amazon le CloudWatch ayuda a monitorizar las métricas de sus recursos de AWS y las aplicaciones que ejecuta en AWS en tiempo real.

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS CloudShell es un shell basado en navegador que puede utilizar para administrar los servicios de AWS mediante la interfaz de línea de comandos de AWS (AWS CLI) y una gama de herramientas de desarrollo preinstaladas.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Lambda ejecuta el código solo cuando es necesario y escala la capacidad de manera automática, por lo que solo pagará por el tiempo informático que utilice.

Otras herramientas

- GitHubes un servicio de alojamiento de código que proporciona herramientas de colaboración y control de versiones.
- Python es un lenguaje de programación de alto nivel.

Código

El código de este patrón está disponible en el GitHub mainframe-data-utilitiesrepositorio.

Prácticas recomendadas

Tenga en cuenta las siguientes prácticas recomendadas:

- Establezca los permisos requeridos en el nivel de nombre de recurso de Amazon (ARN).
- Otorgue siempre permisos con privilegios mínimos para las políticas de IAM. Para obtener más información, consulte las prácticas recomendadas de seguridad en IAM en la documentación de IAM.

Epics

Cree variables de entorno y una carpeta de trabajo

Tarea	Descripción	Habilidades requeridas
Crear variables de entorno.	Copie las siguientes variables de entorno en un editor de texto y, a continuación, sustituya <placeholder>los valores del siguiente ejemplo por los valores de sus recursos: `bucket=<your_bucket_name>` `account=<your_account_number>` `region=<your_region_code>` Nota: Más adelante, creará referencias a su bucket de S3, a su cuenta de AWS y a su región de AWS. Para definir las variables de entorno, abra la CloudShell consola y, a continuación, copie y pegue las variables de entorno actualizadas en la línea de comandos. Nota: Debe repetir este paso cada vez que se reinicie la CloudShell sesión.	AWS general
Cree una carpeta de trabajo.	Para simplificar el proceso de limpieza de recursos más	AWS general

Tarea	Descripción	Habilidades requeridas
	adelante, cree una carpeta de trabajo CloudShell ejecutando el siguiente comando: `mkdir workdir; cd workdir` Nota: Debe cambiar el directorio al directorio de trabajo (`workdir`) cada vez que pierda la conexión con la CloudShell sesión.	

Definir una política y un rol de IAM

Tarea	Descripción	Habilidades requeridas
Cree una política de confianza para la función de Lambda.	El convertidor EBCDIC se ejecuta en una función de Lambda. La función debe tener un rol de IAM. Antes de crear el rol de IAM, debe definir un documento de política de confianza que permita a los recursos asumir esa política. Desde la carpeta de CloudShell trabajo, cree un documento de política ejecutando el siguiente comando: `E2ATrustPol=$(cat <<EOF` `{`	AWS general

Tarea	Descripción	Habilidades requeridas
	<pre> "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Principa l": { "Service": "lambda.a mazonaws.com" }, "Action": "sts:AssumeRole" }] } EOF) printf "$E2ATrustPol" > E2ATrustPol.json</pre>	
Crear el rol de IAM para la conversión de Lambda.	Para crear un rol de IAM, ejecute el siguiente comando de la AWS CLI desde la carpeta de CloudShell trabajo: <pre>aws iam create-role --role-name E2AConvLa mbdaRole --assume- role-policy-docume nt file://E2ATrustPol .json</pre>	AWS general

Tarea	Descripción	Habilidades requeridas
Cree el documento de política de IAM para la función de Lambda.	La función Lambda debe tener acceso de lectura y escritura al bucket de S3 y permisos de escritura para Amazon Logs. CloudWatch Para crear una política de IAM, ejecute el siguiente comando desde la carpeta de trabajo: CloudShell `E2APolicy=$(cat <<EOF` `{` `"Version": "2012-10-17",` `"Statement": [` `{` `"Sid": "Logs",` `"Effect": "Allow",` `"Action": [` `"logs:PutLogEvents",` `"logs:CreateLogStream",` `"logs:CreateLogGroup"` `],` `"Resource": [` `"arn:aws:logs:*:*:log-group:*",` `"arn:aws:logs:*:*:log-group:*:log-stream:*"` `]	AWS general

Tarea	Descripción	Habilidades requeridas
	<pre> }, { "Sid": "S3", "Effect": "Allow", "Action": ["s3:GetObject", "s3:PutObject", "s3:GetObjectVersion"], "Resource": ["arn:aws:s3:::%s/*", "arn:aws:s3:::%s"] }] } EOF) printf "$E2APolicy" "$bucket" "$bucket" > E2AConvLambdaPolic y.json</pre>	

Tarea	Descripción	Habilidades requeridas
Adjuntar los documentos sobre la política de IAM al rol de IAM.	Para adjuntar la política de IAM a la función de IAM, ejecute el siguiente comando desde la carpeta CloudShell de trabajo: `aws iam put-role-policy --role-name E2AConvLambdaRole --policy-name E2AConvLambdaPolicy --policy-document file://E2AConvLambdaPolicy.json`	AWS general

Crear la función de Lambda para la conversión de EBCDIC

Tarea	Descripción	Habilidades requeridas
Descargar el código fuente de conversión a EBCDIC.	Desde la carpeta de CloudShell trabajo, ejecute el siguiente comando para descargar el código mainframe-data-utilities fuente desde la que se encuentra: GitHub `git clone https://github.com/aws-samples/mainframe-data-utilities.git mdu`	AWS general
Crear el paquete ZIP.	Desde la carpeta de CloudShell trabajo, ejecute el siguiente comando para crear el paquete ZIP que crea	AWS general

Tarea	Descripción	Habilidades requeridas
	la función Lambda para la conversión a EBCDIC: `cd mdu; zip ../mdu.zip *.py; cd ..`	
Crear la función de Lambda.	Desde la carpeta de CloudShell trabajo, ejecute el siguiente comando para crear la función Lambda para la conversión a EBCDIC: `aws lambda create-function \ --function-name E2A \ --runtime python3.9 \ --zip-file fileb://mdu.zip \ --handler extract_ebcdic_to_ascii.lambda_handler \ --role arn:aws:iam::$account:role/E2AConvLambdaRole \ --timeout 10 \ --environment "Variables={layout=$bucket/layout/}"` Nota: El diseño de las variables de entorno indica a la función de Lambda dónde residen los metadatos de JSON.	AWS general

Tarea	Descripción	Habilidades requeridas
Crear la política basada en recursos para la función de Lambda.	Desde la carpeta de CloudShell trabajo, ejecute el siguiente comando para permitir que la notificación de eventos de Amazon S3 active la función Lambda para la conversión a EBCDIC: `aws lambda add-permi ssion \ --function-name E2A \ --action lambda:In vokeFunction \ --principal s3.amazon aws.com \ --source-arn arn:aws:s 3:::$bucket \ --source-account $account \ --statement-id 1`	AWS general

Notificaciones de eventos de Amazon S3

Tarea	Descripción	Habilidades requeridas
Cree el documento de configuración para la notificac ión de eventos de Amazon S3.	La notificación de eventos de Amazon S3 inicia la función de Lambda de conversión EBCDIC cuando los archivos se colocan en la carpeta de entrada. Desde la carpeta de CloudShell trabajo, ejecute el siguiente comando para crear el documento JSON para la	AWS general

Tarea	Descripción	Habilidades requeridas
	notificación de eventos de Amazon S3: { "LambdaFunctionC onfigurations": [{ "Id": "E2A", "LambdaFu nctionArn": "arn:aws: lambda:%s:%s:funct ion:E2A", "Events": ["s3:ObjectCreated: Put"], "Filter": { "Key": { "FilterRu les": [{ "Name": "prefix", "Value": "input/" }] } } }] } EOF) printf "$S3E2AEvent" "$region" "$account" > S3E2AEvent.json	

Tarea	Descripción	Habilidades requeridas
Crear notificaciones de eventos de Amazon S3.	Desde la carpeta de CloudShell trabajo, ejecute el siguiente comando para crear la notificación de eventos de Amazon S3: `aws s3api put-bucket-notification-configuration --bucket $bucket --notification-configuration file://S3E2AEvent.json`	AWS general

Crear y cargar los metadatos JSON

Tarea	Descripción	Habilidades requeridas
Analizar el cuaderno de COBOL.	Desde la carpeta de CloudShell trabajo, ejecute el siguiente comando para convertir un cuaderno de COBOL de muestra en un archivo JSON (que define cómo leer y dividir el archivo de datos correctamente): `python3 mdu/parse_copybook_to_json.py \ -copybook mdu/LegacyReference/COBKS05.cpy \ -output CLIENT.json \`	AWS general

Tarea	Descripción	Habilidades requeridas
	`-output-s3key CLIENT.ASCII.txt \` `-output-s3bkt $bucket \` `-output-type s3 \` `-print 25`	

Tarea	Descripción	Habilidades requeridas
Añada la regla de transform ación.	El archivo de datos de ejemplo y su cuaderno de notas COBOL correspondiente son archivos de varios diseños. Esto significa que la conversió n debe dividir los datos en función de determinadas reglas. En este caso, los bytes de las posiciones 3 y 4 de cada fila definen el diseño. Desde la carpeta de CloudShell trabajo, edite el `CLIENT.json` archivo y cambie el contenido de la siguiente `"transf-rule": [],` manera: `"transf-rule": [` `{` `"offset": 4,` `"size": 2,` `"hex": "0002",` `"transf": "transf1"` `},` `{` `"offset": 4,` `"size": 2,` `"hex": "0000",` `"transf": "transf2"` `}` `],`	Información general sobre AWS, lade IBM y Cobol

Tarea	Descripción	Habilidades requeridas
Cargue los metadatos JSON en el bucket de &S3;.	Desde la carpeta de CloudShell trabajo, ejecute el siguiente comando de la AWS CLI para cargar los metadatos de JSON en su bucket de S3: `aws s3 cp CLIENT.json s3://$bucket/layout/CLIENT.json`	AWS general

Convertir el archivo EBCDIC

Tarea	Descripción	Habilidades requeridas
Enviar el archivo EBCDIC al bucket de S3.	Desde la carpeta de CloudShell trabajo, ejecute el siguiente comando para enviar el archivo EBCDIC al bucket de S3: `aws s3 cp mdu/sample-data/CLIENT.EBCDIC.txt s3://$bucket/input/` Nota: Se recomienda configurar carpetas diferente s para los archivos de entrada (EBCDIC) y de salida (ASCII) para evitar volver a llamar a la función de conversión de Lambda cuando el archivo ASCII se cargue en el bucket de S3.	AWS general

Tarea	Descripción	Habilidades requeridas
Comprobar la salida.	Desde la carpeta de CloudShell trabajo, ejecute el siguiente comando para comprobar si el archivo ASCII se ha generado en el depósito de S3: `awss3 ls s3://$bucket/` Nota: La conversión de datos puede tardar varios segundos en realizarse. Le recomendamos que compruebe el archivo ASCII varias veces. Cuando el archivo ASCII esté disponible, ejecute el siguiente comando para descargar el archivo del bucket de S3 a la carpeta actual: `aws s3 cp s3://$bucket/ CLIENT.ASCII.txt .` Comprobar el contenido del archivo ASCII: `head CLIENT.ASCII.txt`	AWS general

Limpiar el entorno

Tarea	Descripción	Habilidades requeridas
(Opcional) Prepare las variables y la carpeta.	Si pierde la conexión con CloudShell, vuelva a conectarse y ejecute el siguiente comando para cambiar el directorio a la carpeta de trabajo: `cd workdir` Asegúrese de que las variables de entorno estén definidas: `bucket=<your_bucket_name>` `account=<your_account_number>` `region=<your_region_code>`	AWS general
Eliminar la configuración de notificación para el bucket.	Desde la carpeta de CloudShell trabajo, ejecute el siguiente comando para eliminar la configuración de notificaciones de eventos de Amazon S3: `aws s3api put-bucket-notification-configuration \` `--bucket=$bucket \` `--notification-configuration="{}"`	AWS general

Tarea	Descripción	Habilidades requeridas
Elimine la función de Lambda.	Desde la carpeta de CloudShell trabajo, ejecute el siguiente comando para eliminar la función Lambda del convertidor EBCDIC: `awslambdadelete-function--function-nameE2A`	AWS general
Eliminar el rol y la política de IAM.	Desde la carpeta de CloudShell trabajo, ejecute el siguiente comando para eliminar la función y la política del convertidor EBCDIC: `aws iam delete-role-policy --role-name E2AConvLambdaRole --policy-name E2AConvLambdaPolicy` `aws iam delete-role --role-name E2AConvLambdaRole`	AWS general

Tarea	Descripción	Habilidades requeridas
Elimine los archivos generados en el bucket de S3.	Desde la carpeta de CloudShell trabajo, ejecute el siguiente comando para eliminar los archivos generados en el bucket de S3: `aws s3 rm s3://$bucket/layout --recursive` `aws s3 rm s3://$bucket/input --recursive` `aws s3 rm s3://$bucket/CLIENT.ASCII.txt`	AWS general
Elimine la carpeta de trabajo.	Desde la carpeta de CloudShell trabajo, ejecute el siguiente comando para eliminarlos `workdir` y su contenido: `cd ..; rm -Rf workdir`	AWS general

Recursos relacionados

- Mainframe Data Utilities README () GitHub
- El conjunto de caracteres EBCDIC (documentación de IBM)
- EBCDIC a ASCII (documentación de IBM)
- COBOL (documentación de IBM)
- Uso de un desencadenador de Amazon S3 para invocar una función de Lambda (documentación de AWS Lambda)

Convertir archivos de datos de mainframe con diseños de registros complejos mediante Micro Focus

Creado por Peter West

Entorno: producción	Origen: archivos de datos EBCDIC de mainframe	Destino: archivos de datos ASCII de Micro Focus
Tipo R: volver a alojar	Carga de trabajo: todas las demás cargas de trabajo	Tecnologías: Mainframe; modernización
Servicios de AWS: AWS Mainframe Modernization		

Resumen

Este patrón le muestra cómo convertir archivos de datos de mainframe con datos no textuales y diseños de registros complejos, pasando de la codificación de caracteres EBCDIC (código de intercambio decimal con código binario extendido) a la codificación de caracteres ASCII (Código estándar estadounidense para el intercambio de información) mediante un archivo de estructura de Micro Focus. Para completar la conversión de archivos, siga estos pasos:

1. Prepare un único archivo fuente que describa todos los elementos de datos y los diseños de registros de su entorno de mainframe.
2. Cree un archivo de estructura que contenga el diseño de registro de los datos mediante el editor de archivos de datos de Micro Focus como parte de las herramientas clásicas de archivos de datos o herramientas de archivos de datos de Micro Focus. El archivo de estructura identifica los datos no textuales para que pueda convertir correctamente los archivos del mainframe de EBCDIC a ASCII.
3. Pruebe el archivo de estructura mediante las herramientas clásicas de archivos de datos o las herramientas de archivos de datos.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Micro Focus Enterprise Developer para Windows, disponible a través de AWS Mainframe Modernization

Versiones de producto

- Micro Focus Enterprise Server 7.0 y versiones posteriores

Herramientas

- Micro Focus Enterprise Developer proporciona el entorno de ejecución para las aplicaciones creadas con cualquier variante del entorno de desarrollo integrado (IDE) de Enterprise Developer.
- Las herramientas de archivos de datos clásicas de Micro Focus le ayudan a convertir, navegar, editar y crear archivos de datos. Las herramientas clásicas para archivos de datos incluyen el convertidor de archivos de datos, el editor de diseño de registros y el editor de archivos de datos.
- Las herramientas de archivos de datos de Micro Focus le ayudan a crear, editar y mover archivos de datos. Las herramientas de archivos de datos incluyen el editor de archivos de datos, las utilidades de conversión de archivos y la utilidad de línea de comandos de estructura de archivos de datos.

Epics

Preparar el archivo de origen

Tarea	Descripción	Habilidades requeridas
Identificar los componentes de origen.	Identificar todos los diseños de registro posibles para el archivo, incluidas las redefinic iones que contengan datos no textuales. Si tiene diseños que contienen redefiniciones, debe reducir estos diseños a diseños únicos que describan cada	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	posible permutación de la estructura de datos. Por lo general, los diseños de registros de un archivo de datos se pueden describir mediante los siguientes arquetipos: • Diseño de registro con sólo datos de texto • Diseño de registro con datos no textuales • Diseño de registros con datos no textuales subordinados a una cláusula REDEFINES Para obtener más informaci ón sobre cómo crear diseños de registros aplanados para archivos que contienen diseños de registros complejos, consulte Realojar aplicaciones EBCDIC en entornos ASCII para migracion es de mainframe.	

Tarea	Descripción	Habilidades requeridas
Identificar las condiciones de diseño de los registros.	En el caso de los archivos con varios diseños de registro o los archivos que contienen diseños complejos con una cláusula REDEFINES, identifiq ue los datos y las condicion es de un registro que puede usar para definir qué diseño usar durante la conversión. Le recomendamos que analice esta tarea con un experto en la materia (SME) que conozca los programas que procesan estos archivos. Por ejemplo, un archivo puede contener dos tipos de registros que contienen datos no textuales. Puede inspeccionar el código fuente y encontrar código similar al siguiente: `MOVE "M" TO PART-TYPE` `MOVE "MAIN ASSEMBLY" TO` `PART-NAME` `MOVE "S" TO PART-TYPE` `MOVE "SUB ASSEMBLY 1"` `TO PART-NAME` El código ayuda a identificar lo siguiente: • El campo «TIPO DE PIEZA» se utiliza para determinar el tipo de registro	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	• El valor «M» se utiliza para el «M-PART-RECORD» • El valor «S» se utiliza para el «S-PART-RECORD» Puede documentar los valores que utiliza este campo para asociar los diseños de registros con los registros de datos correctos del archivo.	
Cree el archivo de origen.	Si el archivo se describe en varios archivos fuente o si el diseño de registros contiene datos no textuales que están subordinados a una cláusula REDEFINES, cree un nuevo archivo fuente que contenga los diseños de registros. No es necesario que el nuevo programa describa el archivo mediante las instrucciones SELECT y FD. El programa simplemente puede contener las descripciones de los registros en 10 niveles dentro de Working-Storage. Nota: puede crear un archivo de origen para cada archivo de datos o crear un archivo fuente maestro que describa todos los archivos de datos.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Compilar el código fuente.	Compile el archivo fuente para crear el diccionario de datos. Se recomienda compilar el archivo fuente mediante el juego de caracteres EBCDIC. Si utiliza la directiva IBMCOMP o las directivas ODOSLIDE, también debe utilizar estas directivas en el archivo fuente. Nota: IBMCOMP afecta al almacenamiento de bytes de los campos COMP y ODOSLIDE afecta al relleno cuando se producen estructur as variables. Si estas directiva s están configuradas incorrect amente, la herramienta de conversión no leerá el registro de datos correctamente. Esto da como resultado datos incorrectos en el archivo convertido.	Desarrollador de aplicaciones

(Opción A) Cree el archivo de estructura con las herramientas clásicas de archivos de datos

Tarea	Descripción	Habilidades requeridas
Inicie la herramienta y cargue el diccionario.	1. Seleccione el icono del menú Inicio de Windows, busque y seleccione Micro Focus Enterprise Developer y, a continuación, seleccion	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	e Herramientas clásicas de archivos de datos. 2. Seleccione Archivo y, a continuación, Diseño de registro. 3. En el cuadro de diálogo Seleccione un archivo a partir del cual crear los diseños, en Nombre de archivo, seleccione el archivo IDY (`.idy`) que se creó al compilar el archivo fuente anteriormente. A continuación, seleccione Abrir. 4. Para confirmar que Herramientas clásicas de archivos de datos utiliza EBCDIC, en el cuadro de diálogo Herramientas de archivos de datos, elija SÍ si el archivo IDY está establecido en EBCDIC y Herramientas de datos en ANSI.	

Tarea	Descripción	Habilidades requeridas
Cree el diseño de registro predeterminado.	Utilice el diseño de registro predeterminado para todos los registros que no coincidan con ningún diseño condicional. 1. En la ventana de diseño, expanda la estructura de datos y, a continuación, busque el nivel 01 utilizado para el diseño predeterm inado. 2. Haga clic con el botón derecho en el elemento 01 y seleccione Diseño nuevo. 3. En el cuadro de diálogo del asistente de diseño de nuevos registros, seleccion e Diseño predeterminado y, a continuación, Siguiente. 4. Seleccione Finalizar. El diseño predeterminado aparece en el panel Diseños y se puede identificar mediante el icono rojo de la carpeta.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Cree un diseño de registro condicional.	Utilice el diseño de registro condicional cuando haya más de un diseño de registro en un archivo. 1. En el panel Diseños, expanda la estructura de datos y, a continuación, localice el nivel 01 utilizado para el diseño condicional. 2. Haga clic con el botón derecho en el elemento 01 y seleccione Diseño nuevo. 3. En el cuadro de diálogo del asistente de diseño de nuevos registros, seleccion e Diseño condicional y, a continuación, Siguiente. 4. Seleccione Finalizar. El diseño condicional aparece en el panel Diseños y se puede identificar mediante el icono de carpeta amarillo. 5. Amplíe el diseño condicion al, haga clic con el botón derecho en el campo en el que debe colocar una condición y, a continuación, seleccione Propiedades. 6. En el cuadro de diálogo Propiedades del campo, introduzca la condición. Confirme que el juego de caracteres esté establecido	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	en EBCDIC y, a continuación, pulse OK. Aparece una marca de verificación junto al campo que tiene una condición establecida. 7. Repita los pasos 5 y 6 para cualquier otro campo que requiera condiciones para este diseño. 8. Repita los pasos 1 a 6 para cualquier otro diseño condicional que deba añadirse. 9. Seleccione Archivo, luego, Guardar como y, a continuación, guarde el archivo de estructura en el disco.	

(Opción B) Cree el archivo de estructura mediante las herramientas de archivos de datos

Tarea	Descripción	Habilidades requeridas
Inicie la herramienta y cargue el diccionario.	1. Seleccione el icono del menú Inicio de Windows, busque y seleccione Micro Focus Enterprise Developer y, a continuación, seleccione Herramientas de archivos de datos. 2. Seleccione Archivo, Nuevo o Archivo de estructura.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	3. En el cuadro de diálogo Abrir, en Nombre de archivo, seleccione el archivo IDY (`.idy`) que se creó al compilar el archivo fuente anteriormente. A continuación, seleccione Abrir. 4. Para confirmar que las herramientas de archivos de datos utilizan EBCDIC, confirme que el menú desplegable de la sección Depurar archivos esté configurado en EBCDIC.	

Tarea	Descripción	Habilidades requeridas
Cree el diseño de registro predeterminado.	Utilice el diseño de registro predeterminado para todos los registros que no coincidan con ningún diseño condicional. 1. En la sección Diseños disponibles del panel izquierdo, expanda la estructura de datos y, a continuación, localice el nivel 01 utilizado para el diseño predeterminado. 2. Haga clic con el botón derecho en el elemento 01 y seleccione Crear diseño predeterminado. El diseño predeterminado aparece en el panel Diseños y se puede identificar mediante el icono azul en forma de «D».	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Cree un diseño de registro condicional.	Utilice el diseño de registro condicional cuando haya más de un diseño de registro en un archivo. 1. En la sección Diseños seleccionados del panel derecho, expanda la estructura de datos y, a continuación, localice el nivel 01 utilizado para el diseño condicional. 2. Haga clic con el botón derecho en el elemento 01 y elija Crear diseño condicional. El diseño condicional aparece en el panel de diseños, en el lado derecho, y se puede identificar mediante el icono verde en forma de «C». 3. Amplíe el diseño condicional, haga clic con el botón derecho en el campo en el que debe colocar una condición y, a continuación, seleccione Propiedades. 4. En el cuadro de diálogo Propiedades del campo, introduzca la condición. Confirme que el juego de caracteres esté establecido en EBCDIC y, a continuación, pulse OK. Aparece	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	un icono rojo «SI» junto al campo que tiene una condición establecida. 5. Repita los pasos 3 y 4 para cualquier otro campo que requiera condiciones para este diseño. 6. Repita los pasos 1 a 4 para cualquier otro diseño condicional que deba añadirse. 7. Seleccione Archivo, luego, Guardar como y, a continuación, guarde el archivo de estructura en el disco.	

(Opción A) Pruebe el archivo de estructura con las herramientas clásicas de archivos de datos

Tarea	Descripción	Habilidades requeridas
Probar un archivo de datos EBCDIC.	Confirme que puede usar el archivo de estructura para ver correctamente un archivo de datos de prueba del EBCDIC. 1. Seleccione el icono del menú Inicio de Windows, busque Micro Focus Enterprise Developer y, a continuación, Herramientas clásicas de datos. 2. Seleccione Archivo y, a continuación, Abrir.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	3. En el cuadro de diálogo Abrir, en Nombre de archivo, seleccione el conjunto de datos EBCDIC y, a continuación, Abrir. 4. Seleccione Archivo, Editor de archivos de datos y Cargue diseños de registros . 5. En el cuadro de diálogo Abrir, en Nombre de archivo, seleccione el archivo de estructura y, a continuación, Abrir. 6. Para confirmar que el modo de juego de caractere s está establecido en EBCDIC, confirme que el menú desplegable está configurado en EBCDIC. Puede ver los datos de registro sin procesar en el panel izquierdo y los datos formateados en el panel derecho. 7. Elija varios registros para asegurarse de que todos los formatos se renderizan con el diseño correcto.	

(Opción B) Pruebe el archivo de estructura con las herramientas de archivos de datos

Tarea	Descripción	Habilidades requeridas
Probar un archivo de datos EBCDIC.	Confirme que puede usar el archivo de estructura para ver correctamente un archivo de datos de prueba del EBCDIC. 1. Seleccione el icono del menú Inicio de Windows, busque Desarrollador de empresa Micro Focus y, a continuación, Herramientas de archivos de datos. 2. Seleccione Archivo, Abrir o Archivo de datos. 3. En el cuadro de diálogo Abrir archivo de datos, en la pestaña Local, en Nombre de archivo, seleccione Examinar para buscar la ubicación del archivo de prueba del EBCDIC. 4. En Archivo de estructur a (opcional), seleccione Examinar para buscar la ubicación del archivo de estructura. 5. En la sección Detalles del archivo, introduzca los detalles del archivo y confirme que la codificac ión esté establecida en EBCDIC.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	6. Elija el modo Abierto Compartido o Abierto Exclusivo en función de sus necesidades. 7. Confirme que el menú desplegable de la sección Apariencia de la barra de herramientas esté configurado como EBCDIC. Verá los datos de registro sin procesar en el panel izquierdo y los datos formateados en el panel derecho. 8. Elija varios registros para asegurarse de que todos los formatos se renderizan con el diseño correcto.	

Pruebe la conversión de archivos de datos

Tarea	Descripción	Habilidades requeridas
Probar la conversión de un archivo EBCDIC.	1. Elija el icono del menú Inicio de Windows, busque y seleccione Desarrollador de empresa Micro Focus y, a continuación, Herramien tas clásicas de datos. 2. Seleccione Herramientas y, a continuación, Consola. 3. En el cuadro de diálogo Convertir archivos de	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	datos, en la sección Archivo de entrada, en Nombre de archivo, seleccione Examinar para buscar y seleccionar el archivo de entrada EBCDIC. Confirme que el conjunto de caracteres esté establecido en EBCDIC. 4. En la sección Conversió n de juegos de caractere s, active las casillas de verificación Convertir juegos de caracteres y Registros que contengan elementos de datos que no sean texto. Elija Seleccionar diseño para la conversión y, a continuac ión, Examinar para buscar y seleccionar el archivo de estructura. 5. En la sección Nuevo archivo, en Nombre de archivo, introduzca la ruta y el nombre del archivo de salida ASCII que desee crear. De forma predeterm inada, la herramienta de conversión tiene el mismo formato que el archivo de entrada. Para realizar pruebas, deje las opciones	

Tarea	Descripción	Habilidades requeridas
	con sus valores predeterminados. 6. Seleccione Convertir. 7. Siga los pasos de la sección (opción A) Pruebe el archivo de estructura con las herramientas clásicas de archivos de datos u (opción B) Pruebe el archivo de estructura con las herramientas de archivos de dato, pero cargue el archivo de salida ASCII en lugar del archivo EBCDIC. 8. Cargue los archivos EBCDIC y ASCII en el editor de archivos de datos y, a continuación, compare los archivos uno al lado del otro para comprobar la precisión de la conversión.	

Recursos relacionados

- Micro Focus (documentación de Micro Focus)
- Unidades centrales y código heredado (Blog de AWS)
- AWS Prescriptive Guidance (documentación de AWS)
- Documentación de AWS (documentación de AWS)
- Referencia general de AWS (documentación de AWS)
- Glosario de AWS (documentación de AWS)

Implementar un entorno para aplicaciones de Blu Age en contenedores mediante Terraform

Creado por Richard Milner-Watts (AWS)

Repositorio de código: Blu Age Sample ECS Infrastructure (Terraform)	Entorno: producción	Origen: mainframe
Destino: Contenedores	Tipo R: redefinir la plataforma	Carga de trabajo: IBM, todas las demás cargas de trabajo
Tecnologías: mainframe; contenedores y microservicios	Servicios de AWS: Amazon ECS; AWS Step Functions; Amazon VPC; Amazon Aurora	

Resumen

La migración de las cargas de trabajo de mainframe heredadas a arquitecturas de nube modernas puede eliminar los costos de mantenimiento de un mainframe, costos que solo aumentan a medida que el entorno envejece. Sin embargo, la migración de los trabajos desde un mainframe puede plantear desafíos únicos. Es posible que los recursos internos no estén familiarizados con la lógica del trabajo, y el alto rendimiento de los mainframes en estas tareas especializadas puede resultar difícil de reproducir en comparación con las CPU generalizadas y convencionales. Reescribir estas tareas puede ser una tarea ardua y requerir un esfuerzo considerable.

Blu Age convierte las cargas de trabajo heredadas de los mainframes en código Java moderno, que luego puede ejecutar como un contenedor.

Este patrón proporciona una muestra de arquitectura sin servidor para ejecutar una aplicación en contenedores que se ha modernizado con la herramienta Blu Age. Los archivos de HashiCorp Terraform incluidos crearán una arquitectura segura para la organización de los contenedores de Blu Age, que admitirá tanto las tareas por lotes como los servicios en tiempo real.

Para obtener más información sobre la modernización de sus cargas de trabajo mediante el uso de Blu Age y los servicios de AWS, consulte estas publicaciones en las recomendaciones de AWS:

- Ejecución de cargas de trabajo de mainframe que se han modernizado con Blu Age en una infraestructura sin servidor de AWS
- Almacenamiento en contenedores de las cargas de trabajo de mainframe que Blu Age ha modernizado

Si necesita ayuda para utilizar Blu Age para modernizar las cargas de trabajo de sus mainframes, póngase en contacto con el equipo de Blu Age seleccionando la opción Contactar con nuestros expertos en el sitio web de Blu Age. Si necesita ayuda para migrar sus cargas de trabajo modernizadas a AWS, integrarlas con los servicios de AWS y pasarlas a producción, póngase en contacto con su administrador de cuentas de AWS o rellene el formulario de AWS Professional Services.

Requisitos previos y limitaciones

Requisitos previos

- La aplicación en contenedores de muestra de Blu Age que proporciona el patrón Almacenamiento en contenedores de las cargas de trabajo de mainframe que Blu Age ha modernizado. La aplicación de muestra proporciona la lógica necesaria para gestionar el procesamiento de las entradas y salidas de la aplicación modernizada y se puede integrar con esta arquitectura.
- Se requiere Terraform para implementar estos recursos.

Limitaciones

- Amazon Elastic Container Service (Amazon ECS) limita los recursos de tareas que se pueden poner a disposición del contenedor. Estos recursos incluyen la CPU, la RAM y el almacenamiento. Por ejemplo, cuando se utiliza Amazon ECS con AWS Fargate, se aplican los límites de recursos de la tarea.

Versiones de producto

Esta solución se probó con las siguientes versiones:

- Terraform 1.3.6
- Proveedor 4.46.0 de AWS para Terraform

Arquitectura

Pila de tecnología de origen

- Blu Age
- Terraform

Pila de tecnología de destino

- Amazon Aurora compatible con PostgreSQL
- AWS Backup
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon ECS
- Servicio AWS Identity and Access Management (IAM)
- AWS Key Management Server (AWS KMS)
- AWS Secrets Manager
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)
- AWS Step Functions
- AWS Systems Manager

Arquitectura de destino

En el siguiente diagrama se muestra la arquitectura de la solución.

1. La solución implementa los siguientes roles de IAM:
    - Rol de tarea por lotes
    - Rol de ejecución de tareas por lotes
    - Rol de tarea de servicio
    - Rol de ejecución de tareas del servicio
    - Rol de Step Functions
    - Rol de AWS Backup

- Rol de monitorización mejorada RDS.

Los roles se ajustan a los principios de acceso de privilegios mínimos.

2. Amazon ECR se utiliza para almacenar la imagen del contenedor que está orquestada por este patrón.
3. El Almacén de parámetros de AWS Systems Manager proporciona datos de configuración sobre cada entorno a la definición de tareas de Amazon ECS durante el tiempo de ejecución.
4. AWS Secrets Manager proporciona datos de configuración sobre cada entorno a la definición de tareas de Amazon ECS durante el tiempo de ejecución. AWS KMS cifró los datos.
5. Los módulos Terraform crean definiciones de tareas de Amazon ECS para todas las tareas en tiempo real y por lotes.
6. Amazon ECS ejecuta una tarea por lotes utilizando AWS Fargate como motor de computación. Se trata de una tarea de corta duración, iniciada según lo exigido por AWS Step Functions.
7. Amazon Aurora, compatible con PostgreSQL, proporciona una base de datos para admitir la aplicación modernizada. Esto reemplaza a las bases de datos de mainframe, como IBM Db2 o IBM IMS DB.
8. Amazon ECS ejecuta un servicio de larga duración para ofrecer una carga de trabajo modernizada en tiempo real. Estas aplicaciones sin estado se ejecutan de forma permanente con contenedores repartidos entre las zonas de disponibilidad.
9. Se utiliza un equilibrador de carga de red para conceder acceso a la carga de trabajo en tiempo real. El equilibrador de carga de red es compatible con protocolos anteriores, como IBM CICS. Como alternativa, puede utilizar el equilibrador de carga de aplicación con cargas de trabajo basadas en HTTP.
10. Amazon S3 proporciona almacenamiento de objetos para las entradas y salidas de los trabajos. El contenedor debe gestionar las operaciones de extracción y envío a Amazon S3 a fin de preparar el directorio de trabajo para la aplicación Blu Age.
11. El servicio AWS Step Functions se utiliza para orquestar la ejecución de las tareas de Amazon ECS para procesar las cargas de trabajo por lotes.
12. Los temas de SNS para cada carga de trabajo por lotes se utilizan para integrar la aplicación modernizada con otros sistemas, como el correo electrónico, o para iniciar acciones adicionales, como entregar los objetos de salida de Amazon S3 a FTP.

Nota: De forma predeterminada, la solución no tiene acceso a Internet. Este patrón supone que la nube privada virtual (VPC) se conectará a otras redes mediante un servicio como AWS Transit

Gateway. Por lo tanto, se implementan varios puntos de conexión de VPC de interfaz para permitir el acceso a los servicios de AWS que utiliza la solución. Para activar el acceso directo a Internet, puede utilizar el conmutador del módulo Terraform para reemplazar los puntos de conexión de VPC por una puerta de enlace de Internet y los recursos asociados.

Automatizar y escalar

El uso de recursos sin servidor en todo este patrón ayuda a garantizar que, al escalar horizontalmente, haya pocos límites en la escala de este diseño. Esto reduce los problemas de vecino ruidoso, como la competencia por los recursos de computación que podría surgir en el mainframe original. Las tareas por lotes se pueden programar para que se ejecuten simultáneamente según sea necesario.

Los contenedores individuales están limitados por los tamaños máximos admitidos por Fargate. Para obtener más información, consulte la sección CPU de tareas y memoria en la documentación de Amazon ECS.

Para escalar las cargas de trabajo en tiempo real de forma horizontal, puede añadir contenedores.

Herramientas

Servicios de AWS

- La edición de Amazon Aurora compatible con PostgreSQL es un motor de base de datos relacional compatible con ACID, completamente administrado que le permite configurar, utilizar y escalar implementaciones de PostgreSQL.
- AWS Backup es un servicio completamente administrado que le ayuda a centralizar y automatizar la protección de datos en todos los servicios de AWS, en la nube y en las instalaciones.
- Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado que es seguro, escalable y fiable.
- Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores escalable y rápido que ayuda a ejecutar, detener y administrar contenedores en un clúster.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Key Management Service (AWS KMS) facilita poder crear y controlar claves criptográficas para proteger los datos.

- AWS Secrets Manager le permite reemplazar las credenciales codificadas en el código, incluidas las contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Step Functions es un servicio de orquestación sin servidor que le permite combinar funciones de Lambda AWS y otros servicios de AWS para crear aplicaciones esenciales desde el punto de vista empresarial.
- El Almacén de parámetros de AWS Systems Manager proporciona un almacenamiento seguro y jerárquico para administrar los datos de configuración y los secretos.

Otros servicios

- HashiCorp Terraform es una herramienta de código abierto de infraestructura como código (IaC) que le ayuda a usar el código para aprovisionar y administrar la infraestructura y los recursos de la nube. Este patrón usa Terraform para crear la arquitectura de muestra.

Repositorio de código

El código fuente de este patrón está disponible en el repositorio GitHub Blu Age Sample ECS Infrastructure (Terraform).

Prácticas recomendadas

- Para los entornos de prueba, use características como la opción `forceDate` para configurar la aplicación modernizada para generar resultados de prueba consistentes ejecutándola siempre durante un período de tiempo conocido.
- Ajuste cada tarea de forma individual para consumir la cantidad óptima de recursos. Puede utilizar Amazon CloudWatch Container Insights para obtener orientación sobre posibles cuellos de botella.

Epics

Preparación del entorno para la implementación

Tarea	Descripción	Habilidades requeridas
Clone el código fuente de la solución.	Clone el código de la solución del proyecto. GitHub	DevOps ingeniero
Impulse el entorno mediante la implementación de recursos para almacenar el estado de Terraform.	1. Abra una ventana de terminal y confirme que Terraform esté instalado y que las credenciales de AWS estén disponibles. 2. Vaya a la carpeta `bootstrap-terraform` . 3. Edite el archivo `main.tf` si desea cambiar los nombres del bucket de S3 (`<accountId>-terraform-backend`) y de la tabla de Amazon DynamoDB (`terraform-lock`). 4. Ejecute el comando `terraform apply` para implementar los recursos. Anote los nombres del bucket de S3 y de las tablas de DynamoDB.	DevOps ingeniero

Implementar la infraestructura de soluciones

Tarea	Descripción	Habilidades requeridas
Revise y actualice la configuración de Terraform.	En el directorio raíz, abra el archivo `main.tf,`, revise el contenido y considere la posibilidad de realizar las siguientes actualizaciones: 1. Actualice la región de AWS buscando y sustituyendo la cadena `eu-west-1` por la región que desee usar. 2. Actualice el nombre del bucket en el bloque `Terraform Backend` si el valor predeterminado se modificó en la épica anterior. 3. Actualice el valor `dynamodb_table` si el valor predeterminado se modificó en la épica anterior. 4. Actualice el valor de la variable `stack_prefix` a la cadena que desee. Esta cadena se antepondrá a los nombres de todos los recursos creados por este patrón. 5. Actualice el valor de `vpc_cidr` . Debe ser al menos un rango de `/24` direcciones.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	6. Revise la sección `Locals`. Esto se usa para definir las tareas de Blu Age que van a implementarse. La solución recorrerá el objeto de la lista `bluage_batch_modules` , creando los recursos asociados (máquina de estado de Step Functions, definición de tareas y tema de SNS) para cada elemento de la lista. En algunos casos, es posible que desee ajustar las variables para diferentes entornos. Por ejemplo, para forzar el tiempo de ejecución en los entornos de prueba, puede cambiar el valor de la variable `force_execution_time` . 7. Para activar el acceso a Internet, cambie el valor de `direct_internet_access_required` de `false` a `true`. Esto implementará una puerta de enlace de Internet, junto con las puertas de enlace NAT y las tablas de enrutamiento que activan el acceso público a Internet en la infraestructura. De	

Tarea	Descripción	Habilidades requeridas
	forma predeterminada, la solución implementará los puntos de conexión de VPC de interfaz en una VPC sin acceso directo a Internet. 8. Para conceder acceso a cualquier carga de trabajo cliente-servidor que se sirva a través de Elastic Load Balancing, actualice los valores de `additiona l_nlb_igress_cidrs` con las redes CIDR que deberían permitirse.	
Implemente el archivo Terraform.	Desde su terminal, ejecute el comando `terraform apply` para implementar todos los recursos. Revise los cambios generados por Terraform e introduzca sí para iniciar la compilación. Tenga en cuenta que la implementación de esta infraestructura puede tardar más de 15 minutos.	DevOps ingeniero

(Opcional) Implementar una aplicación de Blu Age en contenedores válida

Tarea	Descripción	Habilidades requeridas
Envíe la imagen del contenedor Blu Age a Amazon ECR.	Introduzca el contenedor en el repositorio de Amazon ECR que creó en la épica anterior.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Para obtener instrucciones, consulte la documentación de Amazon ECR. Anote el URI de la imagen del contenedor.	
Actualice Terraform para que haga referencia a la imagen del contenedor de Blu Age.	Actualice el archivo `main.tf` para que haga referencia a la imagen del contenedor que usted subió.	DevOps ingeniero
Volver a implementar el archivo Terraform.	Desde su terminal, ejecute `terraform apply` para implementar todos los recursos. Revise las actualizaciones sugeridas por Terraform y, a continuación, introduzca sí para continuar con la implementación.	DevOps ingeniero

Recursos relacionados

- Blu Age
- Ejecución de cargas de trabajo de mainframe que se han modernizado con Blu Age en una infraestructura sin servidor de AWS
- Almacenamiento en contenedores de las cargas de trabajo de mainframe que Blu Age ha modernizado

Genere información de datos mediante AWS Mainframe Modernization y Amazon Q en QuickSight

Entorno: PoC o piloto	Tecnologías: mainframe; análisis; migración; modernización; aprendizaje automático e inteligencia artificial	Carga de trabajo: IBM
Servicios de AWS: AWS Lambda; modernización del mainframe de AWS; Amazon; Amazon S3 QuickSight		

Resumen

Si su organización aloja datos fundamentales para la empresa en un entorno de mainframe, obtener información a partir de esos datos es fundamental para impulsar el crecimiento y la innovación. Al desbloquear los datos del mainframe, puede crear inteligencia empresarial más rápida, segura y escalable para acelerar la toma de decisiones, el crecimiento y la innovación basados en los datos en la nube de Amazon Web Services ()AWS.

Este patrón presenta una solución para generar información empresarial y crear narrativas compartibles a partir de datos de mainframe mediante la transferencia de AWS Mainframe Modernization archivos con BMC y Amazon Q in. QuickSight Los conjuntos de datos de mainframe se transfieren a Amazon Simple Storage Service (Amazon S3) mediante AWS Mainframe Modernization File Transfer con BMC. Una AWS Lambda función formatea y prepara el archivo de datos del mainframe para cargarlo en Amazon QuickSight.

Una vez que los datos estén disponibles en Amazon QuickSight, puede utilizar instrucciones en lenguaje natural con Amazon Q QuickSight para crear resúmenes de los datos, formular preguntas y generar historias de datos. No tiene que escribir consultas SQL ni aprender una herramienta de inteligencia empresarial (BI).

Contexto empresarial

Este patrón presenta una solución para los casos de uso del análisis de datos de mainframe y el conocimiento de los datos. Con el patrón, se crea un panel visual para los datos de su empresa. Para demostrar la solución, este patrón utiliza una empresa de atención médica que ofrece planes médicos, dentales y oftalmológicos a sus miembros en los EE. UU. En este ejemplo, la información demográfica y del plan de los miembros se almacenan en los conjuntos de datos del mainframe. El panel visual muestra lo siguiente:

- Distribución de miembros por región
- Distribución de miembros por género
- Distribución de miembros por edad
- Distribución de miembros por tipo de plan
- Miembros que no han completado la inmunización preventiva

Después de crear el panel, se genera una historia de datos que explica los conocimientos del análisis anterior. La historia de datos proporciona recomendaciones para aumentar el número de miembros que se han vacunado preventivamente.

Requisitos previos y limitaciones

Requisitos previos

- ¿Un activo Cuenta de AWS
- Conjuntos de datos de mainframe con datos empresariales
- Acceso para instalar un agente de transferencia de archivos en el mainframe

Limitaciones

- El archivo de datos del mainframe debe estar en uno de los formatos de archivo compatibles con Amazon QuickSight. Para ver una lista de los formatos de archivo admitidos, consulta la QuickSight documentación de Amazon.

  Este patrón utiliza una función Lambda para convertir el archivo de mainframe a un formato compatible con Amazon. QuickSight

Arquitectura

El siguiente diagrama muestra una arquitectura para generar información empresarial a partir de datos de mainframe mediante AWS Mainframe Modernization File Transfer with BMC y Amazon Q in. QuickSight

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un conjunto de datos de mainframe que contiene datos empresariales se transfiere a Amazon S3 mediante AWS Mainframe Modernization File Transfer with BMC.
2. La función Lambda convierte el archivo que se encuentra en el bucket S3 de destino de la transferencia de archivos en formato de valores separados por comas (CSV).
3. La función Lambda envía el archivo convertido al bucket S3 del conjunto de datos de origen.
4. Amazon QuickSight ingiere los datos del archivo.
5. Los usuarios acceden a los datos en Amazon QuickSight. Puede usar Amazon Q QuickSight para interactuar con los datos mediante instrucciones en lenguaje natural.

Herramientas

Servicios de AWS

- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Mainframe Modernization File Transfer with BMC convierte y transfiere conjuntos de datos de mainframe a Amazon S3 para casos de uso de modernización, migración y aumento de mainframes.
- Amazon QuickSight es un servicio de BI a escala de nube que le ayuda a visualizar, analizar y elaborar informes de sus datos en un único panel. Este patrón utiliza las capacidades de BI generativa de Amazon Q en QuickSight.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Prácticas recomendadas

- Al crear las funciones AWS Identity and Access Management (IAM) para la transferencia de AWS Mainframe Modernization archivos con BMC y la función Lambda, siga el principio del privilegio mínimo.
- Asegúrese de que su conjunto de datos de origen tenga tipos de datos compatibles con Amazon QuickSight. Si el conjunto de datos de origen contiene tipos de datos no compatibles, conviértalos en tipos de datos compatibles. Para obtener información sobre los tipos de datos de mainframe no compatibles y cómo convertirlos en tipos de datos compatibles con Amazon Q QuickSight, consulte la sección Recursos relacionados.

Epics

Configure la transferencia de AWS Mainframe Modernization archivos con BMC

Tarea	Descripción	Habilidades requeridas
Instale el agente de transferencia de archivos.	Para instalar AWS Mainframe Modernization el Agente de transferencia de archivos en su ordenador central, siga las instrucciones de la AWS documentación.	Administrador del sistema mainframe
Cree un depósito S3 para la transferencia de archivos del mainframe.	Cree un depósito de S3 para almacenar el archivo de salida de AWS Mainframe Modernization File Transfer with BMC. En el diagrama de arquitectura, este es el depósito de destino de la transferencia de archivos.	Ingeniero de migraciones
Cree el punto final de transferencia de datos.	1. Cree un depósito S3 para organizar el archivo de entrada del mainframe para la transferencia de AWS	Especialista en modernización de mainframes de AWS

Tarea	Descripción	Habilidades requeridas
	Mainframe Modernization archivos con BMC. 2. Para crear el punto final de transferencia de datos del mainframe, siga las instrucciones de la documentación.AWS	

Convierte la extensión del nombre del archivo de mainframe para la integración con Amazon QuickSight

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3.	Cree un depósito de S3 para que la función Lambda copie el archivo de mainframe convertido del depósito de origen al depósito de destino final.	Ingeniero de migraciones
Creación de una función de Lambda.	Para crear una función Lambda que cambie la extensión del archivo y copie el archivo de mainframe en el depósito de destino, haga lo siguiente: 1. Inicie sesión en la consola AWS Management Console y navegue hasta ella. AWS Lambda 2. Seleccione la función Crear y, a continuación, elija Autor desde cero.	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	3. En Nombre de función, introduzca un nombre para la función. 4. En la lista desplegab le Runtime, selecciona Python.3.X. 5. Amplíe Cambiar función de ejecución predeterminada y, a continuación, elija Crear una nueva función con permisos básicos de Lambda. 6. Elija Crear función. 7. Selecciona la pestaña Código y, a continuación, pega el código `S3CopyLam bda.py` Python que se proporciona en la sección Información adicional. El código Python se generó mediante Amazon Q Developer en el entorno de desarrollo integrado (IDE) de Microsoft Visual Studio. 8. Edite `destinati on_bucket_name` el nombre del bucket de S3 que creó anteriormente y `change destinati on_file_key` el nombre del archivo del mainframe.	

Tarea	Descripción	Habilidades requeridas
	9. Implemente la función de Lambda.	

Tarea	Descripción	Habilidades requeridas
Cree un activador de Amazon S3 para invocar la función Lambda.	Para configurar un disparador que invoque la función Lambda, haga lo siguiente: 1. Abra la página Funciones en la consola de Lambda. 2. Elija la función de Lambda. 3. En la descripción general de la función, seleccione Añadir disparador. 4. En la lista desplegable de configuración del disparador, elija S3. 5. En el campo Bucket, introduce el nombre del bucket de origen. 6. En la lista desplegable Tipo de evento, seleccione Todos los eventos de creación de objetos. 7. Active la casilla de verificación Acepto que no se recomienda usar el mismo depósito de S3 para la entrada y la salida y, a continuación, elija Agregar. Para obtener más información, consulte Tutorial: utilizar un desencadenador de Amazon S3 para invocar una función de Lambda.	Líder de migración

Tarea	Descripción	Habilidades requeridas
Proporcione permisos de IAM para la función Lambda.	Se requieren permisos de IAM para que la función Lambda acceda a los depósitos S3 del conjunto de datos de origen y destino de la transferencia de archivos. Actualice la política asociada a la función de ejecución de la función Lambda mediante la concesión de `s3:DeleteObject` permisos `s3:GetObject` y permisos para el bucket S3 de destino de la transferencia de archivos y el `s3:PutObject` acceso al bucket S3 del conjunto de datos de origen. Para obtener más información, consulte la sección Creación de una política de permisos en el tutorial: Uso de un disparador de Amazon S3 para invocar una función Lambda.	Líder de migración

Defina una tarea de transferencia de datos de mainframe

Tarea	Descripción	Habilidades requeridas
Cree una tarea de transferencia para copiar el archivo del mainframe al bucket de S3.	Para crear una tarea de transferencia de archivos de mainframe, siga las instrucci	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	ones de la AWS Mainframe Modernization documentación. Nota: Especifique la codificación de la página de códigos fuente como IBM1047 y la codificación de la página de códigos de destino como UTF-8.	
Compruebe la tarea de transferencia.	Para comprobar que la transferencia de datos se ha realizado correctamente, siga las instrucciones de la AWS Mainframe Modernization documentación. Confirme que el archivo de la unidad central esté en el bucket S3 de destino de la transferencia de archivos.	Líder de migración
Compruebe la función de copia Lambda.	Compruebe que se haya iniciado la función Lambda y que el archivo se haya copiado con la extensión.csv en el bucket S3 del conjunto de datos de origen. El archivo.csv creado por la función Lambda es el archivo de datos de entrada de Amazon. QuickSight Para ver datos de ejemplo, consulte el `Sample-data-member-healthcare-APG` archivo en la sección de adjuntos.	Líder de migración

Connect Amazon QuickSight a los datos del mainframe

Tarea	Descripción	Habilidades requeridas
Configura Amazon QuickSight.	Para configurar Amazon QuickSight, sigue las instrucciones de la AWS documentación.	Líder de migración
Crea un conjunto de datos para Amazon QuickSight.	Para crear un conjunto de datos para Amazon QuickSight, sigue las instrucciones de la AWS documentación. El archivo de datos de entrada es el archivo de mainframe convertido que se creó al definir la tarea de transferencia de datos de mainframe.	Líder de migración

Obtenga información empresarial a partir de los datos del mainframe mediante Amazon Q en QuickSight

Tarea	Descripción	Habilidades requeridas
Configura Amazon Q en QuickSight.	Esta capacidad requiere la edición Enterprise. Para configurar Amazon Q in QuickSight, haga lo siguiente: 1. Para obtener el complemento Amazon Q, sigue las instrucciones del paso 1: Obtén el complemento Q de la AWS documentación. 2. Para utilizar las capacidades de BI generativa de Amazon Q, actualice las	Líder de migración

Tarea	Descripción	Habilidades requeridas
	cuentas de sus usuarios. Siga las instrucciones de la AWS documentación. 3. Crea un tema de Amazon Q con el conjunto de datos que creaste anteriormente. Siga las instrucciones de la AWS documentación. 4. Para configurar los metadatos del tema de manera que sean compatibles con el lenguaje natural, siga las instrucciones de la documentación.AWS	

Tarea	Descripción	Habilidades requeridas
Analice los datos del mainframe y cree un panel visual.	Para analizar y visualizar los datos en Amazon QuickSight, haga lo siguiente: 1. Para crear el análisis de datos del mainframe, siga las instrucciones de la AWS documentación. Para el conjunto de datos, elija el conjunto de datos creado en el paso anterior. 2. En la página de análisis, selecciona Build visual. 3. En la ventana Crear tema para el análisis, elija Actualizar tema existente. 4. En la lista desplegable Seleccione un tema, elija el tema que creó anteriorm ente. 5. Selecciona Enlazar temas. 6. Después de vincular el tema, elija Build visual para abrir la ventana Build a Visual de Amazon Q. 7. En la barra de indicaciones, escriba sus preguntas de análisis. Los ejemplos de preguntas que se utilizan para este patrón son los siguientes: • Mostrar la distribución de miembros por región	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	• Mostrar la distribución de miembros por edad • Mostrar la distribución de miembros por género • Mostrar la distribución de miembros por tipo de plan • Mostrar el afiliado que no ha completado la inmunización preventiva Después de introducir las preguntas, elija Construir . Amazon Q in QuickSight crea las imágenes. 8. Para añadir las imágenes a su panel de control visual, elija AÑADIR AL ANÁLISIS. Cuando haya terminado , puede publicar su panel para compartirlo con otros miembros de su organización. Para ver ejemplos, consulte el panel visual de Mainframe en la sección de información adicional.	

Cree una historia de datos con Amazon Q a QuickSight partir de los datos del mainframe

Tarea	Descripción	Habilidades requeridas
Cree una historia de datos.	Cree una historia con datos para explicar las ideas del análisis anterior y genere una recomendación para aumentar la inmunización preventiva de los miembros: 1. Para crear la historia de datos, siga las instrucciones de la AWS documentación. 2. Para el mensaje de la historia de datos, utilice lo siguiente: `Build a data story about Region with most numbers of members. Also show the member distribution by medical plan, vision plan, dental plan. Recommend how to motivate members to complete immunizat ion. Include 4 points of supportin g data for this pattern.` También puede crear su propio mensaje para generar historias de	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	datos para obtener otros conocimientos empresariales. 3. Elija Añadir imágenes y añada las imágenes que sean relevantes para la historia de datos. Para este patrón, utilice las imágenes que creó anteriormente. 4. Elija Compilar. 5. Para ver un ejemplo de salida de una historia de datos, consulte la salida de una historia de datos en la sección de información adicional.	
Vea la historia de datos generada.	Para ver la historia de datos generada, siga las instrucciones de la AWS documentación.	Líder de migración
Edite una historia de datos generada.	Para cambiar el formato, el diseño o las imágenes de una historia de datos, siga las instrucciones de la AWS documentación.	Líder de migración
Comparta una historia de datos.	Para compartir una historia de datos, siga las instrucciones de la AWS documentación.	Ingeniero de migraciones

Resolución de problemas

Problema	Solución
No se han podido encontrar los archivos o conjuntos de datos del mainframe introducidos en los criterios de búsqueda de conjuntos de datos para Crear una tarea de transferencia en AWS Mainframe Modernization File Transfer with BMC.	1. En primer lugar, compruebe la conexión seleccionando los puntos finales de transferencia de datos en la consola AWS Mainframe Modernization Transferir con BMC. Si el tiempo del último latido es superior a dos minutos, significa que no se ha establecido la conexión para la transferencia de archivos. Si el tiempo del último latido es inferior a 2 minutos para el agente que se ejecuta en el ordenador central, la conexión con el agente se ha realizado correctamente. Continúe con el paso 2. 2. Compruebe la AWS Secrets Manager configuración. Se debe configurar una clave secreta en Secrets Manager con una clave de `userId` (I mayúscula) con un valor del ID de usuario del mainframe y una clave de `password` con el valor de la contraseña del mainframe. La clave `password` secreta `userId` y la clave distinguen mayúsculas de minúsculas y se deben introducir tal cual.

Recursos relacionados

Para convertir tipos de datos de mainframe como PACKED-DECIMAL (COMP-3) o BINARY (COMP o COMP-4) a un tipo de datos compatible con Amazon, consulta los siguientes patrones: QuickSight

- Convierta y descomprima datos EBCDIC a ASCII mediante Python AWS
- Convierta archivos de mainframe del formato EBCDIC al formato ASCII delimitado por caracteres en Amazon S3 mediante AWS Lambda

Información adicional

S3 .py CopyLambda

El siguiente código de Python se generó mediante un mensaje con Amazon Q Developer en un IDE:

```
#Create a lambda function triggered by S3. display the S3 bucket name and key
import boto3
s3 = boto3.client('s3')
def lambda_handler(event, context):
print(event)
bucket = event['Records'][0]['s3']['bucket']['name']
key = event['Records'][0]['s3']['object']['key']
print(bucket, key)
#If key starts with object_created, skip copy, print "copy skipped". Return lambda with
 key value.
if key.startswith('object_created'):
print("copy skipped")
return {
'statusCode': 200,
'body': key
}
# Copy the file from the source bucket to the destination bucket.
 Destination_bucket_name = 'm2-filetransfer-final-opt-bkt'. Destination_file_key =
 'healthdata.csv'
copy_source = {'Bucket': bucket, 'Key': key}
s3.copy_object(Bucket='m2-filetransfer-final-opt-bkt', Key='healthdata.csv',
 CopySource=copy_source)
print("file copied")
#Delete the file from the source bucket.
s3.delete_object(Bucket=bucket, Key=key)
return {
'statusCode': 200,
'body': 'Copy Successful'
}
```

Panel visual de mainframe

Amazon Q creó la siguiente imagen visual de datos QuickSight para la pregunta de análisis `show member distribution by region`.

Amazon Q creó la siguiente imagen visual de datos QuickSight para la pregunta`show member distribution by Region who have not completed preventive immunization, in pie chart`.

Resultado de una historia de datos

En las siguientes capturas de pantalla se muestran secciones de la historia de datos creada por Amazon Q QuickSight para el mensaje `Build a data story about Region with most numbers of members. Also show the member distribution by medical plan, vision plan, dental plan. Recommend how to motivate members to complete immunization. Include 4 points of supporting data.`

En la introducción, la historia de datos recomienda elegir la región con más miembros para obtener el mayor impacto de las iniciativas de inmunización.

La historia con datos proporciona un análisis del número de miembros de las tres regiones principales y menciona al sudoeste como la región que más se centra en las iniciativas de inmunización.

Nota: Cada una de las regiones del sudoeste y del noreste tiene ocho miembros. Sin embargo, el suroeste tiene más miembros que no están completamente vacunados, por lo que tiene más posibilidades de beneficiarse de las iniciativas para aumentar las tasas de inmunización.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Integrar el controlador universal Stonebranch con AWS Mainframe Modernization

Repositorio de código: aws-mainframe-modernization-stonebranch-integration	Entorno: PoC o piloto	Tecnologías: Mainframe ; Modernización DevOps; Operaciones; SaaS
Carga de trabajo: código abierto; Microsoft	Servicios de AWS: AWS Mainframe Modernization; Amazon RDS; Amazon S3	

Resumen

Este patrón explica cómo integrar la orquestación de cargas de trabajo de Stonebranch Universal Automation Center (UAC) con el servicio de AWS Mainframe Modernization de Amazon Web Services (AWS). El servicio de AWS Mainframe Modernization migra y moderniza las aplicaciones de mainframe a la nube de AWS. Ofrece dos patrones: la redefinici[on de la plataforma de AWS Mainframe Modernization con la tecnología empresarial de Micro Focus y la refactorización automatizada de la AWS Mainframe Modernization con AWS Blu Age.

Stonebranch UAC es una plataforma de automatización y organización de TI en tiempo real. El UAC está diseñado para automatizar y organizar los trabajos, las actividades y los flujos de trabajo en los sistemas de TI híbridos, desde los entornos locales hasta los de AWS. Los clientes empresariales que utilizan sistemas de mainframe están realizando la transición a infraestructuras y aplicaciones modernizadas centradas en la nube. Las herramientas y los servicios profesionales de Stonebranch facilitan la migración de los programadores y las capacidades de automatización existentes a la nube de AWS.

Al migrar o modernizar sus programas de mainframe a la nube de AWS mediante el servicio AWS Mainframe Modernization, puede utilizar esta integración para automatizar la programación por lotes, aumentar la agilidad, mejorar el mantenimiento y reducir los costos.

Este patrón proporciona instrucciones para integrar el programador Stonebranch con las aplicaciones de mainframe migradas al entorno de ejecución Micro Focus Enterprise del servicio de AWS Mainframe Modernization. Este patrón es para arquitectos de soluciones, desarrolladores,

consultores, especialistas en migración y otras personas que trabajan en migraciones, modernizaciones, operaciones o. DevOps

Resultados específicos

Este patrón se centra en proporcionar los siguientes resultados objetivo:

- La capacidad de programar, automatizar y ejecutar trabajos por lotes de mainframe que se ejecutan en el servicio AWS Mainframe Modernization (tiempo de ejecución de Microfocus) de Stonebranch Universal Controller.
- Supervise los procesos por lotes de la aplicación desde el controlador universal Stonebranch.
- Inicie, reinicie, vuelva a ejecutar o detenga los procesos por lotes de forma automática o manual desde el controlador universal Stonebranch.
- Recupere los resultados de los procesos por lotes de AWS Mainframe Modernization.
- Capture los CloudWatch registros de AWS de los trabajos por lotes en Stonebranch Universal Controller.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una aplicación de demostración de Micro Focus Bankdemo con archivos de Job Control Language (JCL) y un proceso por lotes implementado en un entorno de servicios de AWS Mainframe Modernization (tiempo de ejecución de Micro Focus)
- Conocimientos básicos sobre cómo crear e implementar una aplicación de mainframe que se ejecute en Micro Focus Enterprise Server
- Conocimientos básicos del controlador universal Stonebranch
- Licencia de prueba de Stonebranch (póngase en contacto con Stonebranch)
- Instancias de Amazon Elastic Compute Cloud (Amazon EC2) para Windows o Linux (por ejemplo, xlarge) con un mínimo de cuatro núcleos, 8 GB de memoria y 2 GB de espacio en disco
- Apache Tomcat, versión 8.5.x o 9.0.x
- Entorno de ejecución de Java (JRE) o OpenJDK versión 8 u 11
- Edición de Amazon Aurora compatible con MySQL
- Bucket de Amazon Simple Storage Service (Amazon S3) para repositorio de exportación

- Amazon Elastic File System (Amazon EFS) para las conexiones del agente Stonebranch Universal Message Service (OMS) para una alta disponibilidad (HA)
- Archivos de instalación de Universal Agent 7.2 de Stonebranch Universal Controller 7.2
- AWS Mainframe Modernization plantilla de programación de tareas (última versión publicada del archivo .zip)

Limitaciones

- El producto y la solución se han probado y se ha validado su compatibilidad solo con OpenJDK 8 y 11.
- La plantilla de programación de tareas aws-mainframe-modernization-stonebranch-integration sólo funcionará con el servicio AWS Mainframe Modernization.
- Esta plantilla de programación de tareas solo funcionará en las ediciones para Unix, Linux o Windows de los agentes de Stonebranch.

Arquitectura

Arquitectura de estado objetivo

En el siguiente diagrama se muestra el entorno de AWS de ejemplo que se requiere para este piloto.

1. El Universal Automation Center (UAC) de Stonebranch incluye dos componentes principales: Universal Controller y Universal Agents. Stonebranch OMS se utiliza como un bus de mensajes entre el controlador y los agentes individuales.
2. Universal Controller utiliza la base de datos UAC de Stonebranch. La base de datos puede ser compatible con MySQL, Microsoft SQL Server, Oracle o Aurora MySQL.
3. Servicio de modernización de mainframe de AWS: entorno de ejecución de Micro Focus con la BankDemo aplicación implementada. Los archivos de la BankDemo aplicación se almacenarán en un bucket de S3. Este bucket también contiene los archivos JCL de la unidad central.
4. Stonebranch UAC puede ejecutar las siguientes funciones para la ejecución por lotes:
   a. Inicie un trabajo por lotes con el nombre del archivo JCL que existe en el bucket de S3 vinculado al servicio de AWS Mainframe Modernization.
   b. Obtenga el estado de la ejecución del trabajo por lotes.
   c. Espere hasta que se complete la ejecución del trabajo por lotes.

   d. Obtenga los registros de la ejecución del trabajo por lotes.
   e. Vuelva a ejecutar los trabajos por lotes fallidos.
   f. Cancele el trabajo por lotes mientras se está ejecutando.
5. Stonebranch UAC puede ejecutar las siguientes funciones para la aplicación:
   a. Iniciar la aplicación
   b. Obtener el estado de la aplicación
   c. Espere hasta que la aplicación se inicie o se detenga
   d. Detener la aplicación
   e. Obtener los registros del funcionamiento de la aplicación

Conversión de trabajos en Stonebranch

El siguiente diagrama representa el proceso de conversión de puestos de trabajo de Stonebranch durante el proceso de modernización. Describe cómo los cronogramas de trabajo y las definiciones de tareas se convierten a un formato compatible que puede ejecutar tareas por lotes de AWS Mainframe Modernization.

1. Para el proceso de conversión, las definiciones de los trabajos se exportan desde el sistema de mainframe existente.
2. Los archivos JCL se pueden cargar en el depósito S3 de la aplicación Mainframe Modernization para que el servicio AWS Mainframe Modernization pueda implementarlos.
3. La herramienta de conversión convierte las definiciones de trabajo exportadas en tareas de UAC.
4. Una vez creadas todas las definiciones de tareas y los cronogramas de trabajos, estos objetos se importarán al controlador universal. A continuación, las tareas convertidas ejecutan los procesos en el servicio de AWS Mainframe Modernization en lugar de ejecutarlos en el mainframe.

Arquitectura UAC de Stonebranch

El siguiente diagrama de arquitectura representa un active-active-passive modelo de controlador universal de alta disponibilidad (HA). El UAC de Stonebranch se implementa en varias zonas de disponibilidad para proporcionar una alta disponibilidad y respaldar la recuperación de desastres (DR).

Controlador universal

Se aprovisionan dos servidores Linux como controladores universales. Ambos se conectan al mismo punto de conexión de la base de datos. Cada servidor alberga una aplicación Universal Controller y un OMS. La versión más reciente de Universal Controller se utiliza en el momento del aprovisionamiento.

Los controladores universales se implementan en la aplicación web de Tomcat como el documento ROOT y se distribuyen en el puerto 80. Esta implementación facilita la configuración del equilibrador de cargas de la interfaz.

El HTTP a través de TLS o HTTPS se habilita mediante el certificado comodín de Stonebranch (por ejemplo, `https://customer.stonebranch.cloud`). Esto asegura la comunicación entre el navegador y la aplicación.

OMS

Un agente universal y un OMS (servicio de mensajes de Opswise) residen en cada servidor de Universal Controller. Todos los agentes universales desplegados por el cliente están configurados para conectarse a ambos servicios de OMS. OMS actúa como un servicio de mensajería común entre los agentes universales y el controlador universal.

Amazon EFS monta un directorio de bobinas en cada servidor. OMS utiliza este directorio compartido para mantener la información de conexión y tareas de los controladores y los agentes. OMS funciona en un modo de alta disponibilidad. Si el OMS activo deja de funcionar, el OMS pasivo tiene acceso a todos los datos y reanuda las operaciones activas automáticamente. Los agentes universales detectan este cambio y se conectan automáticamente al nuevo OMS activo.

Base de datos

Amazon Relational Database Service (Amazon RDS) aloja la base de datos de UAC y su motor es compatible con Amazon Aurora MySQL. Amazon RDS ayuda a gestionar y ofrecer copias de seguridad programadas a intervalos regulares. Ambas instancias de Universal Controller se conectan al mismo punto de conexión de la base de datos.

Equilibrador de carga

Se configura un equilibrador de carga de aplicación para cada instancia. El equilibrador de carga dirige el tráfico al controlador activo en cualquier momento dado. Los nombres de dominio de su instancia apuntan a los puntos finales del equilibrador de carga respectivos.

Direcciones URL

Cada una de sus instancias tiene una URL, como se muestra en el siguiente ejemplo.

Entorno	Instancia
Producción	customer.stonebranch.cloud
Desarrollo (no producción)	customerdev.stonebranch.cloud
Pruebas (fuera de producción)	customertest.stonebranch.cloud

Nota: Los nombres de las instancias que no son de producción se pueden configurar en función de sus necesidades.

Alta disponibilidad

La alta disponibilidad (HA) es la capacidad de un sistema de funcionar de forma continua y sin fallos durante un período de tiempo designado. Estos fallos incluyen, entre otros, el almacenamiento, las demoras en la respuesta de las comunicaciones del servidor causadas por problemas de la CPU o la memoria y la conectividad de red.

Para cumplir con los requisitos de alta disponibilidad:

- Todas las instancias, bases de datos y demás configuraciones de EC2 se reflejan en dos zonas de disponibilidad independientes dentro de la misma región de AWS.
- El controlador se aprovisiona a través de una imagen de máquina de Amazon (AMI) en dos servidores Linux en las dos zonas de disponibilidad. Por ejemplo, si está aprovisionado en la región de Europa eu-west-1, tiene un controlador universal en la zona de disponibilidad eu-west-1a y en la zona de disponibilidad eu-west-1c.
- No se permite que ningún trabajo se ejecute directamente en los servidores de aplicaciones ni que se almacene ningún dato en estos servidores.
- El equilibrador de carga de aplicación realiza comprobaciones de estado en cada controlador universal para identificar el controlador activo y dirigir el tráfico hacia él. En caso de que se produzcan problemas con un servidor, el equilibrador de carga pasa automáticamente al estado activo del controlador universal pasivo. A continuación, el equilibrador de cargas identifica la nueva instancia activa de Universal Controller a partir de las comprobaciones de estado y comienza a dirigir el tráfico. La conmutación por error se produce en un plazo de cuatro minutos sin pérdida de trabajo, y la URL de la interfaz sigue siendo la misma.

- El servicio de base de datos Aurora compatible con MySQL almacena los datos de Universal Controller. Para los entornos de producción, un clúster de base de datos se crea con dos instancias de base de datos en dos zonas de disponibilidad diferentes dentro de una sola región de AWS. Ambos controladores universales utilizan una interfaz de conectividad de bases de datos Java (JDBC) que apunta a un único punto de conexión del clúster de base de datos. En caso de que una instancia de base de datos tenga problemas, el punto de conexión del clúster de base de datos apunta dinámicamente a la instancia en buen estado. No se requiere intervención manual alguna.

Backup y purga

El controlador universal Stonebranch está configurado para realizar copias de seguridad y purgar los datos antiguos siguiendo el programa que se muestra en la tabla.

Tipo	Programación
Actividad	7 días
Auditoría	90 días
Historial	60 días

Los datos de backup anteriores a las fechas mostradas se exportan al formato.xml y se almacenan en el sistema de archivos. Una vez finalizado el proceso de copia de seguridad, los datos más antiguos se purgan de la base de datos y se archivan en un depósito de S3 durante un máximo de un año en el caso de las instancias de producción.

Puede ajustar este programa en la interfaz de la controladora universal. Sin embargo, el aumento de estos plazos puede provocar un tiempo de inactividad más prolongado durante el mantenimiento.

Herramientas

Servicios de AWS

- AWS Mainframe Modernization es un servicio que le ayuda a modernizar sus aplicaciones de unidad central para convertirlas en entornos de tiempo de ejecución administrados nativos en la nube de AWS. Ofrece herramientas y recursos para ayudarle a planificar e implementar la migración y modernización.

- Amazon Elastic Block Store (Amazon EBS) proporciona volúmenes de almacenamiento de nivel de bloque para su uso con instancias de Amazon EC2.
- Amazon Elastic File System (Amazon EFS) le ayuda a crear y configurar sistemas de archivos compartidos en la nube de AWS.
- Amazon Relational Database Service (Amazon RDS) le ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS. Este patrón utiliza la edición de Amazon Aurora compatible con MySQL.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Elastic Load Balancing (ELB) distribuye el tráfico entrante de aplicaciones o redes entre varios destinos. Así, por ejemplo, puede distribuir el tráfico entre instancias de Amazon EC2, contenedores y direcciones IP de una o varias zonas de disponibilidad. Este patrón utiliza un Equilibrador de carga de aplicación.

Stonebranch

- Universal Automation Center (UAC) es un sistema de productos de automatización de cargas de trabajo empresariales. Este patrón utiliza los siguientes componentes del UAC:
  - Universal Controller, una aplicación web Java que se ejecuta en un contenedor web de Tomcat, es la solución empresarial de programación de tareas y agente de automatización de cargas de trabajo de Universal Automation Center. El controlador presenta una interfaz de usuario para crear, monitorizar y configurar la información del controlador; gestiona la lógica de programación; procesa todos los mensajes enviados y enviados por Universal Agents; y sincroniza gran parte del funcionamiento de alta disponibilidad de Universal Automation Center.
  - Universal Agent es un agente de programación independiente del proveedor que colabora con el programador de tareas existente en las principales plataformas informáticas, tanto antiguas como distribuidas. Se admiten todos los programadores que se ejecutan en z/Series, i/Series, Unix, Linux o Windows.
- Universal Agent es un agente de programación independiente del proveedor que colabora con el programador de tareas existente en las principales plataformas informáticas, tanto antiguas como distribuidas. Se admiten todos los programadores que se ejecutan en z/Series, i/Series, Unix, Linux o Windows.
- Integración con Stonebranch La extensión universal de aws-mainframe-modernization-stonebranch AWS Mainframe Modernization es la plantilla de integración para ejecutar, monitorear y volver a ejecutar trabajos por lotes en la plataforma AWS Mainframe Modernization.

Código

El código de este patrón está disponible en el repositorio aws-mainframe-modernization-stonebranch-integration. GitHub

Epics

Instalación de Universal Controller y Universal Agent en Amazon EC2

Tarea	Descripción	Habilidades requeridas
Descargue los archivos de instalación.	Descargue la instalación desde los servidores de Stonebranch. Para obtener los archivos de instalación, póngase en contacto con Stonebranch.	Arquitecto de la nube
Lanzar la instancia EC2.	Necesitará unos 3 GB de espacio adicional para las instalaciones de Universal Controller y Universal Agent. Por lo tanto, proporciona al menos 30 GB de espacio en disco para la instancia. Agrega el puerto 8080 al grupo de seguridad para que sea accesible.	Arquitecto de la nube
Compruebe los requisitos previos.	Antes de la instalación, haga lo siguiente: 1. Instale Java como se describe en Descarga del entorno de ejecución de Java. `$ sudo yum -y update`	Administrador de la nube, administrador de Linux

Tarea	Descripción	Habilidades requeridas
	`` $ sudo yum install java-11-amazon-cor retto ``` Asegúrese de utilizar una de las versiones de JAVA compatibles. El comando anterior debería instalar java-11. Compruebe la versión de Java y asegúrese de que está utilizando la versión 11 antes de continuar. 2. Como se describe en el documento Instalación de Apache Tomcat, ejecute los siguientes comandos. ``` $ sudo yum install tomcat tomcat-admin- webapps $ sudo systemctl enable tomcat $ sudo systemctl start tomcat ``` 3. Cree una base de datos de Amazon Aurora como se describe en Creación de un clúster de base de datos de Aurora MySQL y cómo conectarse a él. Edición de Amazon Aurora compatible con MySQL. Elija un nombre de usuario maestro y una contraseñ	

Tarea	Descripción	Habilidades requeridas
	a maestra. Mantenga los valores predeterminados para el resto de los ajustes.	

Tarea	Descripción	Habilidades requeridas
Instale Universal Controller.	1. Cargue el archivo de instalación `universal-controller-7.2.0.0.tar` en la instancia EC2. 2. Desarchive los archivos de instalación en una carpeta `temp`. `$ tar -xvf universal-controller-7.2.0.0.tar` 3. Conceda permiso de ejecución al script de instalación. `$ chmod a+x install-controller.sh` 4. Instale el controlador. En este ejemplo, se utiliza el siguiente comando para instalar Universal Controller en `/usr/share/tomcat`. Utilice el nombre de la base de datos de Amazon Aurora que creó en los pasos anteriores. `$ sudo ./install-controller.sh --tomcat-dir /usr/share/tomcat/ --controller-file universal-controller-7.2.0.0-build.145.war --`	Arquitecto de la nube, administrador de Linux

Tarea	Descripción	Habilidades requeridas
	dbuser admin --dbpass “****” --dbname uc --rdbms mysql --dburl jdbc:mysql://database-2-instance-1.cih63miincgy.us-east-1.rds.amazonaws.com:3306/ La última línea del resultado del script debe ser «Instalación completa». 5. Navegue hasta la siguiente URL en la instancia de EC2. http://<public_ip>:8080/uc 6. En la pantalla de inicio de sesión, introduzca ops.admin en la sección Nombre de usuario y deje vacío el campo Contraseña. 7. Establezca una contraseña para el usuario de `ops.admin` .	

Tarea	Descripción	Habilidades requeridas
Instale Universal Agent.	1. Cargue el archivo de instalación `sb-7.2.0.1-linux-3.10-x86_64.tar.Z` en la instancia EC2. 2. Inicie sesión en la instancia EC2. 3. Desarchive el paquete de instalación de Universal Agent. `$ zcat sb-7.2.0.1-linux-3.10-x86_64.tar.Z | tar xvf -` 4. Ejecute el siguiente comando de la . `$ sudo ./unvinst --oms_servers 7878@localhost --oms_autostart yes --python yes` 5. Cree un archivo PAM. `$ cp /etc/pam.d/login /etc/pam.d/ucmd` 6. Habilite el inicio automático para Universal Agent. `$ /sbin/restorecon -v /etc/rc.d/init.d/ubrokerd`	Administrador de la nube, administrador de Linux

Tarea	Descripción	Habilidades requeridas
Agregue OMS a Universal Controller.	1. Inicie sesión en Universal Controller con el usuario de `ops.admin` . 2. Elija el menú de Servicios en la esquina superior izquierda de la pantalla y, a continuación, elija el menú de Servidores OMS en el Sistema 3. En el campo Dirección del servidor OMS, escriba localhost y, a continuación, guarde. 4. Verá el estado del servidor OMS como Conectado y el Estado de la sesión como Operativo.	Administrador de Universal Controller

Importe la extensión universal de AWS Mainframe Modernization y cree una tarea

Tarea	Descripción	Habilidades requeridas
Plantilla de integración de importación.	Para este paso, necesita la extensión universal de AWS Mainframe Modernization. Asegúrese de descargar la última versión publicada del archivo .zip. 1. Inicie sesión en el Universal Controller con el `ops.admin` usuario.	Administrador de Universal Controller

Tarea	Descripción	Habilidades requeridas
	2. Vaya a Servicios, Importar la plantilla de integración. 3. Seleccione el archivo .zip de la plantilla de integración (`aws_mainframe_modernization_stonebranch_extension.zip`) y elija Importar. Una vez importada la plantilla de integración, verá las tareas de AWS Mainframe Modernization en la sección Servicios disponibles.	

Tarea	Descripción	Habilidades requeridas
Habilite las credenciales que se pueden resolver.	1. Navegue hasta Servicios, Tareas de AWS Mainframe Modernization. 2. En el panel derecho, rellene los campos obligatorios: • Nombre: nueva tarea de modernización de la unidad central • Agente: seleccione el único agente (AGNT0001). En los detalles de la AWS Mainframe Modernization: • Acción: enumerar los entornos • Credenciales de AWS: si se le ha agregado un rol de AWS Identity and Access Management IAM a la instancia EC2, puede dejar este campo en blanco. Si va a utilizar `AWSAccessKeyID` y`AWSSecretKey` , seleccione el icono () situado junto al campo. En la ventana de Detalles de la credencial que se abre, introduzca la siguiente información y, a continuac ión, guárdela.	Administrador de Universal Controller

Tarea	Descripción	Habilidades requeridas
	• Nombre: credenciales de modernización de mainframe de AWS • Usuario en tiempo de ejecución: escriba el ID de la clave de acceso de AWS en este campo. • Contraseña de tiempo de ejecución: escriba la clave secreta de AWS en este campo. • Punto de conexión: asegúrese de que el punto de conexión tenga la región de AWS correcta. El valor predeterminado es https://m2.us-east-1.amazonaws.com. • Región: introduzca la región del servicio de AWS Mainframe Modernization. El valor predeterminado es `us-east-1` . 3. Mantenga los valores predeterminados en el resto de los campos y guarde la tarea.	

Tarea	Descripción	Habilidades requeridas
Iniciar la tarea.	1. En la parte superior del panel derecho, seleccione Iniciar tarea. 2. En la ventana de Confirmación, seleccione Lanzar. Después de eso, la consola universal Controller mostrará un mensaje similar al siguiente. 2022-08-24 10:11:49 AM Se lanzó correctamente la tarea universal «Nueva tarea de modernización de la unidad central» con la instancia de tarea sys_id 1661291493634146313NC8E38DB8OZJY. 3. Navegue hasta las Instancias. Si no ve la pestaña Instancias, utilice la flecha derecha para desplazarse hacia la derecha. 4. Abra el menú contextual (haga clic con el botón derecho) de la instancia de la tarea de la lista, seleccione Recuperar salida y, a continuación, Enviar en la opción de Recuperar salida	Administrador de Universal Controller

Tarea	Descripción	Habilidades requeridas
	5. En la ventana Recuperar resultados, verá la lista de entornos de STDOUT.	

Probar el inicio de un trabajo por lotes

Tarea	Descripción	Habilidades requeridas
Crear una tarea para el trabajo por lotes.	1. Navegue hasta Servicios, Tareas de AWS Mainframe Modernization. 2. En el panel derecho, rellene los campos obligatorios: • Nombre: nueva tarea de modernización de la unidad central • Agente: seleccione el único agente (AGNT0001). En los detalles de la AWS Mainframe Modernization: • Acción: iniciar el lote (o iniciar el lote y esperar a que se ejecute el trabajo por lotes y esperar a que la tarea se complete en AWS) • Credenciales de AWS: si ha agregado un rol de IAM a la instancia EC2, puede dejar este campo vacío. Si va a utilizar `AWSAccess`	Administrador de Universal Controller

Tarea	Descripción	Habilidades requeridas
	`KeyID` `yAWSSecret Key` , seleccione el icono () situado junto al campo. • Punto de conexión: asegúrese de que el punto de conexión tenga la región de AWS correcta. El valor predeterminado es https://m2.us-east-1.amazonaws.com. • Región: introduzca la región del servicio de AWS Mainframe Modernization. El valor predeterminado es `us-east-1` . • Solicitud: seleccione el icono situado junto al campo () y luego, Enviar en las opciones de actualización de la solicitud . Esto se conectará al servicio de AWS Mainframe Modernization y devolverá la lista de aplicaciones. Ahora puede seleccionar la aplicación de la lista desplegable. Seleccione la aplicación en la que desea ejecutar el trabajo por lotes.	

Tarea	Descripción	Habilidades requeridas
	• Nombre del archivo JCL: `RUNHELLO.jcl` • Espere a que se complete correctamente o reciba un error: si se selecciona esta opción, la tarea esperará hasta que el estado del trabajo por lotes sea exitoso o fallido. • Intervalo de sondeo: es el tiempo que transcurre entre cada sondeo. • Obtener registros de ejecución: si se seleccion a, los registros se recuperarán automátic amente cuando se complete el trabajo por lotes. • Formato de registro: este es el formato de los registros que se van a imprimir. Puede ser en formato texto o JSON. 3. Mantenga los valores predeterminados en el resto de los campos y guarde la tarea.	

Tarea	Descripción	Habilidades requeridas
Iniciar la tarea.	1. En la parte superior del panel derecho, seleccione Iniciar tarea. 2. En la ventana de Confirmación, seleccione Lanzar. Después de eso, la consola universal Controller mostrará un mensaje similar al siguiente. 2022-08-24 11:11:59 AM Se lanzó correctamente la tarea universal «Mainframe Modernization Start Batch» con la instancia de tarea sys_id <sys id>. 3. Navegue hasta las Instancias. Si no ve la pestaña Instancias, utilice la flecha derecha para desplazarse hacia la derecha. 4. Abra el menú contextual (haga clic con el botón derecho) de la instancia de la tarea de la lista, seleccione Recuperar salida y, a continuación, Enviar en la opción de Recuperar salida 5. En la ventana Recuperar resultados, verá la lista de entornos de STDOUT.	Administrador de Universal Controller

Cree un flujo de trabajo para múltiples tareas

Tarea	Descripción	Habilidades requeridas
Copie las tareas.	1. Abra el menú contextual (haga clic con el botón derecho) de la tarea de la que quiera crear copias y elija Copiar. 2. En la ventana Copiar AWS Mainframe Modernization Task, introduzca el siguiente nombre nuevo para la nueva tarea: Mainframe Modernization Start Batch - RUNAWS2. 3. Vuelva a copiar la tarea con el siguiente nombre: Mainframe Modernization Start Batch - RUNAWS3. 4. Vuelva a copiar la tarea con el siguiente nombre: Mainframe Modernization Start Batch - RUNAWS4. 5. Copie la tarea por última vez con el siguiente nombre: Mainframe Modernization Start Batch - FOOBAR.	Administrador de Universal Controller
Tarea de actualizar.	1. Abra (haga doble clic) la tarea Start Batch - RUNAWS2 de Mainframe Modernization, cambie el campo Nombre de archivo	Administrador de Universal Controller

Tarea	Descripción	Habilidades requeridas
	JCL a `RUNAWS2.jcl` y guárdela. 2. Abra (haga doble clic) la tarea Start Batch - RUNAWS3 de Mainframe Modernization, cambie el campo Nombre de archivo JCL a `RUNAWS3.jcl` , y guárdela. 3. Abra (haga doble clic) la tarea Start Batch - RUNAWS4 de Mainframe Modernization, cambie el campo Nombre de archivo JCL a `RUNAWS4.jcl` , y guárdela. 4. Abra (haga doble clic) la tarea Start Batch - FOOBAR de Mainframe Modernization, cambie el campo Nombre de archivo JCL a `MISSING.jcl` , y guárdela. Esta tarea fallará porque el valor del nombre de archivo JCL es incorrecto.	

Tarea	Descripción	Habilidades requeridas
Cree un flujo de trabajo.	1. Navegue hasta Servicios, Flujos de trabajo. 2. En el panel derecho, introduzca Mainframe Modernization Workflow en el campo Nombre y guarde. 3. En el panel de la derecha, seleccione Editar flujo de trabajo. 4. En la Pestaña del editor de flujos de trabajo, el botón Añadir tarea (+). 5. En la ventana de Búsqueda de tareas, seleccione Buscar para ver todas las tareas de Universal Controller. 6. Haga clic en el icono situado junto a Mainframe Modernization Start Batch Task y arrastre el icono a un lugar vacío del Editor de flujos de trabajo. 7. Repita la misma acción para las demás tareas de modernización de la unidad central y colóquelas como se muestra en la sección de Información adicional. 8. Pulse el botón Conectar () y conecte las tareas entre sí. Para conectar una tarea con otra, haga clic en el	Administrador de Universal Controller

Tarea	Descripción	Habilidades requeridas
	centro de la tarea y arrástrel a hasta la tarea de destino. 9. Conecta las tareas como se muestra en la sección Información adicional y guarda el flujo de trabajo. 10. Haga clic con el botón derecho en un lugar vacío del editor de flujos de trabajo, seleccione Iniciar flujo de trabajo y, a continuación, Aceptar.	

Tarea	Descripción	Habilidades requeridas
Compruebe el estado del flujo de trabajo.	1. En el menú de la izquierda, seleccione la Actividad 2. En el centro de la ventana, seleccione Iniciar. Verá la lista de instancias de tareas en la lista. 3. Abra el flujo de trabajo de modernización de mainframe (haga doble clic en él) en la lista o abra el menú contextual (haga clic con el botón derecho) y seleccione Comandos de tareas del flujo de trabajo y Ver flujo de trabajo. Verá las tareas tal y como se muestra en la sección de información adicional. Se esperaba que la segunda tarea fallara porque utilizast e un archivo JCL que faltaba.	Administrador de universal Controller

Solucione los problemas de los trabajos por lotes fallidos y vuelva a ejecutarlos

Tarea	Descripción	Habilidades requeridas
Corrija la tarea fallida y vuelva a ejecutarla.	1. Abra (haga doble clic en) la tarea fallida para ver el error de la tarea. 2. Tiene dos opciones al corregir la tarea fallida.	Administrador de Universal Controller

Tarea	Descripción	Habilidades requeridas
	• Corrija el nombre del archivo JCL y configúrelo en `F00BAR.jcl` . • Añada el nombre de archivo JCL correcto al nombre de archivo JCL (Temp). Este campo sobrescribirá el campo Nombre del archivo JCL. Para este piloto, seleccione la segunda opción y guarde la instancia de la tarea. 3. En el Supervisor de flujo de trabajo, abra el menú contextual (haga clic con el botón derecho) de la tarea fallida y seleccione Comandos y Volver a ejecutar. 4. Después de eso, todas las tareas se completarán correctamente.	

Cree las tareas de inicio y detención de la aplicación

Tarea	Descripción	Habilidades requeridas
Cree la acción Iniciar aplicación.	1. Navegue hasta Servicios, Tareas de AWS Mainframe Modernization. 2. En el panel derecho, rellene los campos obligatorios.	Administrador de Universal Controller

Tarea	Descripción	Habilidades requeridas
	• Nombre: aplicación de inicio de modernización de mainframe • Agente: seleccione el único agente (AGNT0001) En los detalles de la AWS Mainframe Modernization: • Acción: iniciar la aplicació n • Credenciales de AWS: si ha agregado un rol de IAM a la instancia EC2, puede dejar este campo vacío. Si va a utilizar `AWSAccessKeyID` y `AWSSecretKey` , seleccione la credencial que creó anteriormente. • Punto de conexión: asegúrese de que el punto de conexión tenga la región correcta. El valor predeterminado es https://m2.us-eas t-1.amazonaws.com. • Región: introduzca la región del servicio de AWS Mainframe Modernization. El valor predeterminado es `us-east-1` .	

Tarea	Descripción	Habilidades requeridas
	• Solicitud: seleccione el icono situado junto al campo () y luego, Enviar en las opciones de actualización de la solicitud. Esto se conectará al servicio de AWS Mainframe Modernization y devolverá la lista de aplicaciones. Ahora puede seleccionar la aplicación de la lista desplegable. Seleccione la aplicación en la que desea ejecutar el trabajo por lotes. • Espere a que se complete correctamente o reciba un error: si se selecciona esta opción, la tarea esperará hasta que el estado del trabajo por lotes sea exitoso o fallido. • Intervalo de sondeo: es el tiempo que transcurre entre cada sondeo. • Obtener registros de ejecución: si se selecciona, los registros se recuperarán automáticamente cuando se complete el trabajo por lotes.	

Tarea	Descripción	Habilidades requeridas
	• Formato de registro: este es el formato de los registros que se van a imprimir. Puede ser en formato texto o JSON. 3. Mantenga los valores predeterminados en el resto de los campos y guarde la tarea. 4. Ahora copie esta tarea y cree una tarea para Stop Application. Cambie el nombre a Mainframe Moderinization Stop Application y cambie la acción a Detener aplicació n.	

Crear una tarea de cancelación de ejecución por lotes

Tarea	Descripción	Habilidades requeridas
Cree la acción Cancelar Batch.	1. Navegue hasta Servicios, Tareas de AWS Mainframe Modernization. 2. En el panel derecho, rellene los campos obligatorios. • Nombre: Mainframe Modernization Cancel Batch Execution • Agente: seleccione el único agente (AGNT0001)	

Tarea	Descripción	Habilidades requeridas
	En los detalles de la AWS Mainframe Modernization: • Acción: cancelar la ejecución por lotes • Credenciales de AWS: si ha agregado un rol de IAM a la instancia EC2, puede dejar este campo vacío. Si va a utilizar `AWSAccessKeyID` y `AWSSecretKey` , seleccione la credencial que creó anteriormente. • Punto de conexión: asegúrese de que el punto de conexión tenga la región correcta. El valor predeterminado es https://m2.us-east-1.amazonaws.com. • Región: introduzca la región del servicio de AWS Mainframe Modernization. El valor predeterminado es `us-east-1` . • Solicitud: seleccione el icono situado junto al campo () y luego, Enviar en las opciones de actualización de la solicitud . Esto se conectará	

Tarea	Descripción	Habilidades requeridas
	al servicio de AWS Mainframe Moderniza tion y devolverá la lista de aplicaciones. Ahora puede seleccionar la aplicación de la lista desplegable. Seleccion e la aplicación en la que desea ejecutar el trabajo por lotes. • Espere a que se complete correctamente o reciba un error: si se selecciona esta opción, la tarea esperará hasta que el estado del trabajo por lotes sea exitoso o fallido. • Intervalo de sondeo: es el tiempo que transcurre entre cada sondeo. • Obtener registros de ejecución: si se seleccion a, los registros se recuperarán automátic amente cuando se complete el trabajo por lotes. • Formato de registro: este es el formato de los registros que se van a imprimir. Puede ser en formato texto o JSON. 3. Mantenga los valores predeterminados en el resto	

Tarea	Descripción	Habilidades requeridas
	de los campos y guarde la tarea.	

Recursos relacionados

- Controlador universal
- Agente universal
- Configuración de LDAP
- Configuración de inicio de sesión único
- Alta disponibilidad
- Herramienta de conversión Xpress

Información adicional

Iconos en el editor de flujos de trabajo

Todas las tareas están conectadas

Estado del flujo de trabajo

Migre y replique archivos VSAM a Amazon RDS o Amazon MSK mediante Connect de Precisely

Creado por Prachi Khanna (AWS) y Boopathy GOPALSAMY (AWS)

Entorno: PoC o piloto	Origen: VSAM	Destino: bases de datos
Tipo R: renovar arquitectura	Carga de trabajo: IBM	Tecnologías: Mainframe; modernización
Servicios de AWS: Amazon MSK; Amazon RDS; AWS Mainframe Modernization		

Resumen

Este patrón le muestra cómo migrar y replicar archivos del Método de Acceso a Almacenamiento Virtual (VSAM) de un mainframe a un entorno de destino en la nube de AWS mediante Connect de Precisely. Los entornos de destino indicados en este patrón incluyen Amazon Relational Database Service (Amazon RDS) y Amazon Managed Streaming para Apache Kafka (Amazon MSK). Connect emplea registro de datos de cambios (CDC) para supervisar continuamente las actualizaciones de sus archivos VSAM de origen y, a continuación, transferir estas actualizaciones a uno o más de sus entornos de destino de AWS. Puede usar este patrón para lograr sus objetivos de modernización de aplicaciones o análisis de datos. Por ejemplo, puede usar Connect para migrar los archivos de aplicaciones de VSAM a la nube de AWS con baja latencia, o migrar sus datos de VSAM a un almacenamiento de datos o lago de datos de AWS para realizar análisis que puedan tolerar latencias de sincronización superiores a las requeridas para la modernización de las aplicaciones.

Requisitos previos y limitaciones

Requisitos previos

- IBM z/OS V2R1 o posterior
- CICS Transaction Server for z/OS (CICS TS) V5.1 o posterior (registro de datos de CICS/VSAM)
- IBM MQ 8.0 o posterior

- Cumplimiento de los requisitos de seguridad de z/OS (por ejemplo, autorización de APF para las bibliotecas de carga de SQData)
- Registros de recuperación de VSAM activados
- (Opcional) Versión de recuperación de CICS VSAM (CICS VR) para capturar automáticamente los registros de CDC
- Una cuenta de AWS activa
- Una nube privada virtual (VPC) de Amazon con una subred a la que pueda acceder la plataforma antigua
- Una licencia de VSAM Connect de Precisely

Limitaciones

- Connect no admite la creación automática de tablas de destino basadas en cuadernos o esquemas VSAM de origen. Debe definir la estructura de la tabla de destino por primera vez.
- En el caso de destinos que no son de transmisión, como Amazon RDS, debe especificar el mapeo entre el origen de la conversión y el destino en el script de configuración de Apply Engine.
- Las funciones de registro, monitoreo y alerta se implementan a través de API y requieren componentes externos (como Amazon CloudWatch) para estar completamente operativos.

Versiones de producto

- SQData 40134 para z/OS
- SQData 4.0.43 para Imagen de máquina de Amazon (AMI) de Amazon Linux en Amazon Elastic Compute Cloud (Amazon EC2)

Arquitectura

Pila de tecnología de origen

- Lenguaje de control de tareas (JCL)
- Shell z/OS Unix e Instalación de Sistema Interactivo de Productividad (ISPF)
- Utilidades VSAM (IDCAMS)

Pila de tecnología de destino

- Amazon EC2
- Amazon MSK
- Amazon RDS
- Amazon VPC

Arquitectura de destino

Migración de archivos VSAM a Amazon RDS

El siguiente diagrama muestra cómo migrar archivos VSAM a una base de datos relacional, como Amazon RDS, en tiempo real o casi en tiempo real mediante el agente/publicador de CDC en el entorno de origen (mainframe en las instalaciones) y el Apply Engine en el entorno de destino (nube de AWS).

El diagrama muestra el siguiente flujo de trabajo por lotes:

1. Connect registra los cambios en un archivo comparando los archivos VSAM de los archivos de respaldo para identificar los cambios y, a continuación, los envía al flujo de registro.
2. El publicador consume los datos del flujo de registro del sistema.
3. El publicador comunica los cambios registrados en los datos a un motor de destino a través de TCP/IP. El controlador Daemon autentica la comunicación entre los entornos de origen y destino.
4. El Apply Engine del entorno de destino recibe los cambios del agente publicador y los aplica a una base de datos relacional o no relacional.

En el diagrama, se muestra el siguiente flujo on line:

1. Connect registra los cambios en el archivo online mediante una réplica de registro y, a continuación, transmite los cambios registrados a un flujo de registro.
2. El publicador consume los datos del flujo de registro del sistema.
3. El publicador comunica los cambios en los datos registrados al motor de destino a través de TCP/IP. El controlador Daemon autentica la comunicación entre los entornos de origen y destino.
4. El motor de implementación del entorno de destino recibe los cambios del agente publicador y los aplica a una base de datos relacional o no relacional.

Migración de archivos VSAM a Amazon MSK

El siguiente diagrama muestra cómo transmitir estructuras de datos de VSAM desde un mainframe a Amazon MSK en modo de alto rendimiento, y cómo generar automáticamente conversiones de esquemas JSON o AVRO que se integran con Amazon MSK.

El diagrama muestra el siguiente flujo de trabajo por lotes:

1. Connect registra los cambios en un archivo mediante CICS VR o comparando los archivos VSAM de los archivos de respaldo para identificar los cambios. Los cambios registrados se envían al flujo de registro.
2. El publicador consume los datos del flujo de registro del sistema.
3. El publicador comunica los cambios en los datos registrados al motor de destino a través de TCP/IP. El controlador Daemon autentica la comunicación entre los entornos de origen y destino.
4. El motor replicador, que funciona en modo de procesamiento paralelo, divide los datos en una unidad de caché de trabajo.
5. Los subprocesos de trabajo registran los datos de la caché.
6. Los datos se publican en los temas de Amazon MSK desde los hilos de trabajo.
7. Los usuarios aplican los cambios de Amazon MSK a destinos como Amazon DynamoDB, Amazon Simple Storage Service (Amazon S3) OpenSearch o Amazon Service mediante conectores.

En el diagrama, se muestra el siguiente flujo on line:

1. Los cambios en el archivo online se registran mediante una réplica de registro. Los cambios registrados se envían al flujo de registro.
2. El publicador consume los datos del flujo de registro del sistema.
3. El publicador comunica los cambios en los datos registrados al motor de destino a través de TCP/IP. El controlador Daemon autentica la comunicación entre los entornos de origen y destino.
4. El motor replicador, que funciona en modo de procesamiento paralelo, divide los datos en una unidad de caché de trabajo.
5. Los subprocesos de trabajo registran los datos de la caché.
6. Los datos se publican en los temas de Amazon MSK desde los hilos de trabajo.
7. Los usuarios aplican los cambios de Amazon MSK a destinos como DynamoDB, Amazon S3 o Service mediante OpenSearch conectores.

Herramientas

- Amazon Managed Streaming para Apache Kafka (Amazon MSK) es un servicio completamente administrado que le permite crear y ejecutar aplicaciones que utilizan Apache Kafka para procesar datos de streaming.
- Amazon Relational Database Service (Amazon RDS) le ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS.

Epics

Prepare el entorno de origen (mainframe)

Tarea	Descripción	Habilidades requeridas
Instale Connect CDC 4.1.	1. Póngase en contacto con el equipo de soporte de Precisely para obtener una licencia y paquetes de instalación. 2. Use JCL de ejemplo para instalar Connect CDC 4.1. Para obtener más instrucciones, consulte Instalar Connect CDC (SQData) mediante JCL en la documentación de Precisely. 3. Ejecute el comando `SETPROG APF` para autorizar las bibliotec as de carga de Connect SQDATA.V4nnn.LOADLIB.	Desarrollador/administrador de IBM Mainframe
Configure el directorio zFS.	Para configurar un directori o zFS, siga las instrucciones de Directorios de variables	Desarrollador/administrador de IBM Mainframe

Tarea	Descripción	Habilidades requeridas
	zFS en la documentación de Precisely. Nota: las configuraciones del controlador Daemon y del agente registrador/publicador se almacenan en el sistema de archivos de z/OS UNIX Systems Services (denominado zFS). Los agentes de controlador Daemon, registrador, almacenamiento y publicador requieren una estructura de directorios zFS predefinida para almacenar un número reducido de archivos.	
Configure los puertos TCP/IP.	Para configurar los puertos TCP/IP, siga las instrucciones de Puertos TCP/IP de la documentación de Precisely. Nota: El controlador Daemon requiere puertos TCP/IP en los sistemas de origen. Los puertos son referenciados por los motores en los sistemas de destino (donde se procesan los datos de cambios registrados).	Desarrollador/administrador de IBM Mainframe

Tarea	Descripción	Habilidades requeridas
Cree un flujo de registro de z/OS.	Para crear un flujo de registro de z/OS, siga las instrucciones de la sección Crear flujos de registro en el sistema z/OS en la documentación de Precisely . Nota: Connect emplea el flujo de registro para registrar y transmitir datos entre el entorno de origen y el entorno de destino durante la migración. Para ver un ejemplo de JCL que crea un z/OS LogStream , consulte Crear flujos de registro del sistema z/OS en la documentación de Precily.	Desarrollador de Mainframe de IBM
Identifique y autorice las ID de los usuarios de zFS y las tareas iniciadas.	Use RACF para conceder acceso al sistema de archivos OMVS zFS. Para ver un ejemplo de JCL, consulte Identificar y autorizar ID de usuario y tarea iniciada en zFS en la documentación de Precisely.	Desarrollador/administrador de IBM Mainframe

Tarea	Descripción	Habilidades requeridas
Genere las claves públicas/privadas de z/OS y el archivo de claves autorizadas.	Ejecute JCL para generar el par de claves. Para ver un ejemplo, consulte Ejemplo de par de claves en la sección de Información adicional de este patrón. Para obtener instrucciones, consulte Generar claves públicas y privadas de z/OS y archivo de claves autorizadas en la documentación de Precisely.	Desarrollador/administrador de IBM Mainframe
Active el registro replicado de CICS VSAM y adjúntelo al flujo de registro.	Ejecute el siguiente script de JCL. ``` //STEP1 EXEC PGM=IDCAMS //SYSPRINT DD SYSOUT=* //SYSIN DD * ALTER SQDATA.CICS.FILEA - LOGSTREAMID(SQDATA.VSAMCDC.LOG1) - LOGREPLICATE ```	Desarrollador/administrador de IBM Mainframe

Tarea	Descripción	Habilidades requeridas
Active el registro de recuperación de archivos de VSAM mediante FCT.	Modifique la tabla de control de archivos (FCT) para que refleje los siguientes cambios en los parámetros: `Configure FCT Parms CEDA ALT FILE(name) GROUP(groupname) DSNAME(data set name) RECOVERY(NONE|BACKOUTONLY|ALL) FWDRECOVLOG(NO|1-99) BACKUPTYPE(STATIC|DYNAMIC) RECOVERY PARAMETERS RECOVery : None | Backoutonly | All Fwdrecovlog : No | 1-99 BAckuptype : Static | Dynamic`	Desarrollador/administrador de IBM Mainframe
Configure el CD para el agente publicador. CzLog	1. Cree el archivo CAB de CD CzLog Publisher. 2. Cifre los datos publicados. 3. Prepare el CD CzLog Publisher Runtime JCL.	Desarrollador/administrador de IBM Mainframe

Tarea	Descripción	Habilidades requeridas
Active el controlador Daemon.	1. Abra el panel de ISPF y ejecute el siguiente comando para abrir el menú de Precisely: `EXEC 'SQDATA.V4nnnnn.ISPFLIB(SQDC$STA)' 'SQDATA.V4nnnnn'` 2. Para configurar el controlador Daemon, seleccione la opción 2 del menú.	Desarrollador/administrador de IBM Mainframe
Active el publicador.	1. Abra el panel de ISPF y ejecute el siguiente comando para abrir el menú de Precisely: `EXEC 'SQDATA.V4nnnnn.ISPFLIB(SQDC$STA)' 'SQDATA.V4nnnnn'` 2. Para configurar el publicador, seleccione la opción 3 del menú e I para insertar.	Desarrollador/administrador de IBM Mainframe

Tarea	Descripción	Habilidades requeridas
Active el flujo de registro.	1. Abra el panel de ISPF y ejecute el siguiente comando para abrir el menú de Precisely: `EXEC 'SQDATA.V4nnnnn.ISPFLIB(SQDC$STA)' 'SQDATA.V4nnnnn'` 2. Para configurar el flujo de registro, elija la opción 4 del menú e I para insertar. A continuación, introduzca el nombre del flujo de registro creado en los pasos anteriores.	Desarrollador/administrador de IBM Mainframe

Prepare el entorno de destino (AWS)

Tarea	Descripción	Habilidades requeridas
Instale Precisely en una instancia de EC2.	Para instalar Connect de Precisely en la AMI de Amazon Linux para Amazon EC2, siga las instrucciones de Instalar Connect CDC (SQData) en UNIX en la documentación de Precisely.	AWS general
Abra los puertos TCP/IP.	Para modificar el grupo de seguridad e incluir los puertos del controlador Daemon para el acceso entrante y saliente, siga las instrucciones de TCP/IP en la documentación de Precisely.	AWS general

Tarea	Descripción	Habilidades requeridas
Cree directorios de archivos.	Para crear directorios de archivos, siga las instrucciones de Preparar el entorno de aplicación de destino en la documentación de Precisely.	AWS general
Cree el archivo de configuración de Apply Engine.	Cree el archivo de configuración de Apply Engine en el directorio de trabajo de Apply Engine. El siguiente ejemplo de archivo de configuración muestra Apache Kafka como destino: `builtin.features=SASL_SCRAM` `security.protocol=SASL_SSL` `sasl.mechanism=SCRAM-SHA-512` `sasl.username=` `sasl.password=` `metadata.broker.list=` Nota: para más información, consulte Seguridad de la documentación de Apache Kafka.	AWS general

Tarea	Descripción	Habilidades requeridas
Cree scripts para el procesamiento de Apply Engine.	Cree scripts para que Apply Engine procese los datos de origen y los replique en el destino. Para obtener más información, consulte Crear un script de Apply Engine en la documentación de Precisely.	AWS general
Ejecute los scripts.	Para iniciar el script, ejecute los comandos `SQDPARSE` y `SQDENG`. Para obtener más información, consulte Analizar un script para zOS en la documentación de Precisely.	AWS general

Validar el entorno

Tarea	Descripción	Habilidades requeridas
Valide la lista de archivos VSAM y las tablas de destino para su procesamiento en CDC.	1. Valide los archivos VSAM, incluidos los registros de replicación, los registros de recuperación, los parámetros de FCT y el flujo de registro. 2. Valide las tablas de la base de datos de destino, indicando si las tablas se han creado según la según la definición de esquema requerida, el acceso a las tablas y otros criterios.	AWS general, Mainframe

Tarea	Descripción	Habilidades requeridas
Compruebe que el producto Connect CDC SQData esté vinculado.	Ejecute un trabajo de prueba y compruebe que el código de retorno de este trabajo es 0 (correcto). Nota: los mensajes de estado de Apply Engine de Connect CDC SQData deben mostrar mensajes de conexión activa.	AWS general, Mainframe

Ejecute y valide casos de prueba (lote)

Tarea	Descripción	Habilidades requeridas
Ejecute el trabajo por lotes en el mainframe.	Ejecute el trabajo de aplicación por lotes con un JCL modificado. Incluya pasos en el JCL modificado para hacer lo siguiente: 1. Realizar una copia de seguridad de los archivos de datos. 2. Comparar el archivo de respaldo con los archivos de datos modificados, generar el archivo delta y, a continuación, anotar el recuento de registros de delta de los mensajes. 3. Enviar el archivo delta al flujo de registro de z/OS. 4. Ejecutar JCL. Para ver un JCL de ejemplo, consulte	AWS general, Mainframe

Tarea	Descripción	Habilidades requeridas
	Preparar JCL de comparación y captura de archivos en la documentación de Precisely.	
Comprobar el flujo de registros.	Compruebe el flujo de registro para confirmar que puede ver los datos de cambios del trabajo por lotes completado en el mainframe.	AWS general, Mainframe
Valide los recuentos de la tabla de cambios delta de origen y de destino.	Para confirmar que se han contabilizado los registros, haga lo siguiente: 1. Recopile el recuento delta de origen a partir de los mensajes de lotes de JCL. 2. Supervise Apply Engine para ver los recuentos a nivel de registro del número de registros insertados, actualizados o eliminados en el archivo VSAM. 3. Consulte los recuentos de registros en la tabla de destino. 4. Compare y contabilice los distintos recuentos de registros.	AWS general, Mainframe

Ejecute y valide casos de prueba (On line)

Tarea	Descripción	Habilidades requeridas
Ejecute la transacción online en una región CICS.	1. Ejecute la transacción online para validar el caso de prueba. 2. Valide el código de ejecución de la transacción (RC=0: correcta).	Desarrollador de Mainframe de IBM
Comprobar el flujo de registros .	Confirme que el flujo de registro incluye los cambios específicos a nivel de registro.	Desarrollador de AWS Mainframe
Valide el recuento en la base de datos de destino.	Supervise Apply Engine para comprobar el recuento a nivel de registro.	Precisely, Linux
Valide los recuentos de registros y los registros de datos en la base de datos de destino.	Consulte la base de datos de destino para validar los recuentos de registros y los registros de datos.	AWS general

Recursos relacionados

- VSAM z/OS (documentación de Precisely)
- Apply engine (documentación de Precisely)
- Motor de replicador (documentación de Precisely)
- Flujo de registro (documentación de IBM)

Información adicional

Archivo de configuración de ejemplo

Este es un archivo de configuración de ejemplo para un flujo de registro en el que el entorno de origen es un mainframe y el entorno de destino es Amazon MSK:

```
 -- JOBNAME -- PASS THE SUBSCRIBER NAME
 -- REPORT  progress report will be produced after "n" (number) of Source records
processed.

 JOBNAME VSMTOKFK;
 --REPORT EVERY 100;
 -- Change Op has been ‘I’ for insert, ‘D’ for delete , and ‘R’ for Replace. For RDS
it is 'U' for update
 -- Character Encoding on z/OS is Code Page 1047, on Linux and UNIX it is Code Page
819 and on Windows, Code Page 1252
 OPTIONS
 CDCOP('I', 'U', 'D'),
 PSEUDO NULL = NO,
 USE AVRO COMPATIBLE NAMES,
 APPLICATION ENCODING SCHEME = 1208;

 --       SOURCE DESCRIPTIONS

 BEGIN GROUP VSAM_SRC;
 DESCRIPTION COBOL ../copybk/ACCOUNT AS account_file;
 END GROUP;

 --       TARGET DESCRIPTIONS

 BEGIN GROUP VSAM_TGT;
 DESCRIPTION COBOL ../copybk/ACCOUNT AS account_file;
 END GROUP;

 --       SOURCE DATASTORE (IP & Publisher name)

 DATASTORE cdc://10.81.148.4:2626/vsmcdct/VSMTOKFK
 OF VSAMCDC
 AS CDCIN
 DESCRIBED BY GROUP VSAM_SRC ACCEPT ALL;

 --       TARGET DATASTORE(s) - Kafka and topic name

 DATASTORE 'kafka:///MSKTutorialTopic/key'
 OF JSON
```

```
  AS CDCOUT
  DESCRIBED BY GROUP VSAM_TGT FOR INSERT;

  --       MAIN SECTION

  PROCESS INTO
  CDCOUT
  SELECT
  {
  SETURL(CDCOUT, 'kafka:///MSKTutorialTopic/key')
  REMAP(CDCIN, account_file, GET_RAW_RECORD(CDCIN, AFTER), GET_RAW_RECORD(CDCIN,
 BEFORE))
  REPLICATE(CDCOUT, account_file)
  }
  FROM CDCIN;
```

Ejemplo de par de claves

Este es un ejemplo de cómo ejecutar JCL para generar el par de claves:

```
//SQDUTIL EXEC PGM=SQDUTIL //SQDPUBL DD DSN=&USER..NACL.PUBLIC, //
 DCB=(RECFM=FB,LRECL=80,BLKSIZE=21200), // DISP=(,CATLG,DELETE),UNIT=SYSDA, //
 SPACE=(TRK,(1,1)) //SQDPKEY DD DSN=&USER..NACL.PRIVATE, //
 DCB=(RECFM=FB,LRECL=80,BLKSIZE=21200), // DISP=(,CATLG,DELETE),UNIT=SYSDA, //
 SPACE=(TRK,(1,1)) //SQDPARMS DD  keygen //SYSPRINT DD SYSOUT= //SYSOUT DD SYSOUT=* //
SQDLOG DD SYSOUT=* //*SQDLOG8 DD DUMMY
```

Modernice la administración de la producción de mainframe en AWS mediante OpenText Micro Focus Enterprise Server y LRS X PageCenter

Documento creado por Shubham Roy (AWS), Abraham Rondon (Micro Focus) y Guy Tucker (Levi, Ray and Shoup Inc)

Entorno: PoC o piloto	Origen: Mainframe de IBM	Destino: AWS
Tipo R: redefinir la plataforma	Carga de trabajo: IBM	Tecnologías: mainframe; migración; modernización
Servicios de AWS: AWS Managed Microsoft AD; Amazon EC2; Amazon FSx para Windows File Server; Amazon RDS; AWS Mainframe Modernization		

Resumen

Al modernizar la administración de la producción de su mainframe, puede ahorrar costos, mitigar la deuda técnica que implica el mantenimiento de los sistemas heredados y mejorar la resiliencia y la agilidad mediante las tecnologías nativas de la DevOps nube de Amazon Web Services (AWS). Este patrón muestra cómo modernizar las cargas de trabajo de administración de la producción de mainframe críticas para la empresa en la nube de AWS. El patrón utiliza OpenText Micro Focus Enterprise Server como entorno de ejecución para una aplicación de mainframe modernizada, con Levi, Ray & Shoup, Inc. (LRS) VPSX/MFI (Micro Focus Interface) como servidor de impresión y LRS PageCenter X como servidor de archivos. El LRS PageCenter X ofrece soluciones de administración de resultados para ver, indexar, buscar, archivar y proteger el acceso a los resultados empresariales.

El patrón se basa en el enfoque de modernización del mainframe a través de redefinir la plataforma. Las aplicaciones de mainframe se migran mediante AWS Mainframe Modernization a Amazon Elastic Compute Cloud (Amazon EC2). Las cargas de trabajo de administración de la producción de mainframe se migran a Amazon EC2, y una base de datos de mainframe, como IBM Db2 for z/

OS, se migra a Amazon Relational Database Service (Amazon RDS). El servidor dLRS Directory Integration Server (LRS/DIS) funciona con AWS Directory Service para Microsoft Active Directory con el fin de autenticar y autorizar el flujo de trabajo de administración de la producción.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una carga de trabajo de administración de la producción de mainframe.
- Conocimientos básicos sobre cómo reconstruir y entregar una aplicación de mainframe que se ejecute en Micro Focus Enterprise Server. OpenText Para obtener más información, consulte la hoja de datos de Enterprise Server en la documentación de OpenText Micro Focus.
- Conocimientos básicos de las soluciones y los conceptos de impresión en la nube de LRS. Para obtener más información, consulte Output Modernization (Modernización de la producción) en la documentación del LRS.
- Software y licencia de Micro Focus Enterprise Server. Para obtener más información, póngase en contacto con el departamento de ventas de OpenText Micro Focus.
- Software y licencias de LRS VPSX/MFI, LRS PageCenter X, LRS/Queue y LRS/DIS. Para obtener más información, póngase en contacto con LRS. Debe proporcionar los nombres de host de las instancias de EC2 en las que se instalarán los productos LRS.

Nota: Para obtener más información sobre las consideraciones de configuración de las cargas de trabajo de administración de la producción de mainframe, consulte Considerations en la sección Additional information de este patrón.

Versiones de producto

- OpenText Micro Focus Enterprise Server 8.0 o posterior
- LRS VPSX/MFI
- LRS PageCenter X V1R3 o posterior

Arquitectura

Pila de tecnología de origen

- Sistema operativo: IBM z/OS
- Lenguaje de programación: Common Business-Oriented Language (COBOL), Job Control Language (JCL) y Customer Information Control System (CICS)
- Base de datos: IBM Db2 para z/OS, base de datos del Sistema de Gestión de la Información de IBM (IMS) y Método de acceso al almacenamiento virtual (VSAM)
- Seguridad: Resource Access Control Facility (RACF), CA Top Secret para z/OS y Access Control Facility 2 (ACF2)
- Soluciones de impresión y archivado: productos de producción e impresión z/OS para mainframe de IBM (IBM Infoprint Server for z/OS, LRS y CA Deliver) y soluciones de archivado (CA Deliver, ASG Mobius o CA Bundle)

Arquitectura de origen

El diagrama siguiente muestra una arquitectura de estado actual tipo para una carga de trabajo de administración de la producción de mainframe.

El diagrama muestra el siguiente flujo de trabajo:

1. Los usuarios llevan a cabo transacciones comerciales en un sistema de participación (SoE) que se basa en una aplicación CICS de IBM escrita en COBOL.
2. El SoE invoca el servicio de mainframe, que registra los datos de las transacciones comerciales en una base de datos system-of-records (SoR), como IBM Db2 for z/OS.
3. El SoR conserva los datos comerciales del SoE.
4. El programador de trabajos por lotes inicia un trabajo por lotes para generar resultados de impresión.
5. El trabajo por lotes extrae los datos de la base de datos. Formatea los datos de acuerdo con los requisitos comerciales y, a continuación, genera producción empresarial, como extractos de facturación, tarjetas de identidad o extractos de préstamos. Por último, el trabajo por lotes dirige la producción a la administración de la producción para formatear, publicar y almacenar los resultados en función de los requisitos empresariales.
6. La administración de la producción recibe los resultados del trabajo por lotes. La gestión de salida indexa, organiza y publica la salida en un destino específico del sistema de gestión de salida, como las soluciones LRS PageCenter X (como se demuestra en este patrón) o CA View.

7. Los usuarios pueden ver, buscar y recuperar los resultados.

Pila de tecnología de destino

- Sistema operativo: Windows Server que se ejecuta en Amazon EC2
- Procesamiento: Amazon EC2
- Almacenamiento: Amazon Elastic Block Store (Amazon EBS) y Amazon FSx para Windows File Server
- Lenguaje de programación: COBOL, JCL y CICS
- Bases de datos: Amazon RDS
- Seguridad: AWS Managed Microsoft AD
- Impresión y archivado: solución de impresión LRS (VPSX) y archivado (PageCenterX) en AWS
- Entorno de ejecución de mainframe: Micro Focus Enterprise Server OpenText

Arquitectura de destino

El diagrama siguiente muestra una arquitectura para una carga de trabajo de administración de la producción de mainframe que se implementa en la nube de AWS.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El programador de trabajos por lotes inicia un trabajo por lotes para generar la producción, como extractos de facturación, tarjetas de identificación o extractos de préstamos.
2. El trabajo por lotes del mainframe (rediseñado a Amazon EC2) utiliza el tiempo de ejecución de OpenText Micro Focus Enterprise Server para extraer datos de la base de datos de la aplicación, aplicar lógica empresarial a los datos y formatear los datos. A continuación, envía los datos a un destino de salida mediante el módulo de salida de la impresora OpenText Micro Focus (documentación de OpenText Micro Focus).
3. La base de datos de la aplicación (un SoR que se ejecuta en Amazon RDS) conserva los datos para su impresión.
4. La solución de impresión LRS VPSX/MFI se implementa en Amazon EC2 y sus datos operativos se almacenan en Amazon EBS. El LRS VPSX/MFI utiliza el agente de transmisión LRS/Queue basado en TCP/IP para recopilar los datos de salida a través de la API JES Print Exit de Micro Focus. OpenText

LRS VPSX/MFI realiza el preprocesamiento de datos, como la traducción de EBCDIC a ASCII. También realiza tareas más complejas, como la conversión de flujos de datos exclusivos de ordenadores centrales, como IBM Advanced Function Presentation (AFP) y Xerox Line Conditioned Data Stream (LCDS), en flujos de datos más comunes de visualización e impresión, como el lenguaje de comandos de impresora (PCL) y el PDF.

Durante el período de mantenimiento del LRS PageCenter X, el LRS VPSX/MFI conserva la cola de salida y sirve de respaldo para la cola de salida. El LRS VPSX/MFI conecta y envía la salida al LRS X mediante el protocolo LRS/Queue. PageCenter LRS/Queue realiza un intercambio de la preparación y la finalización de los trabajos para garantizar que la transferencia de datos se lleve a cabo.

Notas:

Para obtener más información sobre los datos de impresión que se pasan de OpenText Micro Focus Print Exit a LRS/Queue y a los mecanismos de procesamiento por lotes de mainframe compatibles con LRS VPSX/MFI, consulte la captura de datos de impresión en la sección de información adicional.

El LRS VPSX/MFI puede realizar comprobaciones de estado en el nivel de la flota de impresora s. Para obtener más información, consulte Printer-fleet health checks (Comprobaciones de estado de la flota de impresoras) en la sección Additional information (Información adicional) de este patrón.

5. La solución de administración de salida LRS PageCenter X se implementa en Amazon EC2 y sus datos operativos se almacenan en Amazon FSx for Windows File Server. LRS PageCenter X proporciona un sistema central de administración de informes de todos los archivos importados a LRS PageCenter X, además de que todos los usuarios pueden acceder a los archivos. Los usuarios pueden ver el contenido de un archivo específico o realizar búsquedas de criterios coincidentes en varios archivos.

   El componente LRS/NetX es un servidor de aplicaciones web multiproceso que proporciona un entorno de ejecución común para la aplicación LRS X y otras aplicaciones PageCenter LRS. El componente LRS/Web Connect está instalado en el servidor web y proporciona un conector desde el servidor web al servidor de aplicaciones web LRS/NetX.
6. El LRS X proporciona almacenamiento para los objetos del sistema de archivos. PageCenter Los datos operativos del LRS PageCenter X se almacenan en Amazon FSx for Windows File Server.

7. AWS Managed Microsoft AD lleva a cabo la autenticación y la autorización de la administración de la producción con LRS/DIS.

Nota: La solución de destino no suele requerir cambios en la aplicación para adaptarse a los lenguajes de formato de mainframe, como IBM AFP o Xerox LCDS.

Arquitectura de infraestructura de AWS

El diagrama siguiente muestra una arquitectura de infraestructura de AWS segura y de alta disponibilidad para una carga de trabajo de administración de la producción de mainframe.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El programador de lotes inicia el proceso por lotes y se implementa en Amazon EC2 en varias zonas de disponibilidad para alta disponibilidad (HA).

   Nota: Este patrón no incluye la implementación del programador de lotes. Para obtener más información acerca de la implementación, consulte la documentación del proveedor de software del programador.

2. El trabajo por lotes del ordenador central (escrito en un lenguajes de programación como JCL o COBOL) utiliza la lógica empresarial básica para procesar y generar la producción de impresión, como extractos de facturación, tarjetas de identificación y extractos de préstamos. El trabajo por lotes se implementa en Amazon EC2 en dos zonas de disponibilidad, para alta disponibilidad. Utiliza la API Print Exit de OpenText Micro Focus para enrutar la salida de impresión al LRS VPSX/MFI para el preprocesamiento de los datos.
3. El servidor de impresión LRS VPSX/MFI se implementa en Amazon EC2 en dos zonas de disponibilidad, para alta disponibilidad (par redundante activo-en espera). Utiliza Amazon EBS como almacén de datos operativos. El Equilibrador de carga de red comprueba el estado de las instancias EC2 de LRS VPSX/MFI. Si una instancia activa está en mal estado, el equilibrador de carga dirige el tráfico a las instancias activas en espera de la otra zona de disponibilidad. Las solicitudes de impresión se mantienen en la cola de trabajos del LRS de forma local en cada una de las instancias de EC2. En caso de producirse un error, se debe reiniciar la instancia errónea antes de que los servicios de LRS puedan reanudar el procesamiento de la solicitud de impresión.

Nota: LRS VPSX/MFI puede realizar comprobaciones de estado en el nivel de la flota de impresoras. Para obtener más información, consulte Printer-fleet health checks (Comproba ciones de estado de la flota de impresoras) en la sección Additional information (Información adicional) de este patrón.

4. La administración de salida de LRS PageCenter X se implementa en Amazon EC2 en dos zonas de disponibilidad para HA (par redundante activo-en espera). Utiliza Amazon FSx para Windows File Server como almacén de datos operativos. Si una instancia activa está en mal estado, el balanceador de cargas realiza una comprobación del estado de las instancias EC2 de LRS PageCenter X y dirige el tráfico a las instancias en espera de la otra zona de disponibilidad.
5. Un Network Load Balancer proporciona un nombre DNS para integrar el servidor VPSX/MFI de LRS con el LRS X. PageCenter

   Nota: El LRS PageCenter X admite un balanceador de carga de capa 4.

6. LRS PageCenter X utiliza Amazon FSx for Windows File Server como almacén de datos operativo desplegado en dos zonas de disponibilidad para alta disponibilidad. LRS PageCenter X solo entiende los archivos que se encuentran en el recurso compartido de archivos, no en una base de datos externa.
7. AWS Managed Microsoft AD se utiliza con LRS/DIS para llevar a cabo la autenticación y la autorización del flujo de trabajo de administración de la producción. Para obtener más información, consulte Print output authentication and authorization (Autenticación y autorización de la producción de impresión) en la sección Additional information (Información adicional).

Herramientas

Servicios de AWS

- AWS Directory Service para Microsoft Active Directory permite que las cargas de trabajo compatibles con un directorio y los recursos de AWS utilicen Active Directory administrado en la nube de AWS.
- Amazon Elastic Block Store (Amazon EBS) proporciona volúmenes de almacenamiento por bloques para su uso con instancias de Amazon Elastic Compute Cloud (Amazon EC2).

- Amazon Elastic Compute Cloud (Amazon EC2) brinda capacidad de computación escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Elastic Load Balancing (ELB) distribuye el tráfico entrante de aplicaciones o redes entre varios destinos. Así, por ejemplo, puede distribuir el tráfico entre instancias de Amazon EC2, contenedores y direcciones IP de una o varias zonas de disponibilidad. Este patrón utiliza un equilibrador de carga de red.
- Amazon FSx proporciona sistemas de archivos que admiten los protocolos de conectividad estándares del sector y ofrecen alta disponibilidad y replicación en todas las regiones de AWS. Este patrón utiliza Amazon FSx para Windows File Server.
- Amazon Relational Database Service (Amazon RDS) ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS.

Otras herramientas

- El software LRS PageCenter X proporciona una solución escalable de administración de contenido de documentos e informes que ayuda a los usuarios a obtener el máximo valor de la información mediante funciones automatizadas de indexación, cifrado y búsqueda avanzada.
- La interfaz VPSX/MFI (Micro Focus Interface) de LRS, desarrollada conjuntamente por LRS y OpenText Micro Focus, captura la salida de una bobina JES de Micro Focus Enterprise Server y la OpenText envía de forma fiable a un destino de impresión específico.
- LRS/Queue es un agente de transmisión basado en TCP/IP. El LRS VPSX/MFI utiliza LRS/Queue para recopilar o capturar datos de impresión a través de la interfaz de programación JES Print Exit de Micro Focus. OpenText
- LRS Directory Integration Server (LRS/DIS) es un directorio de integración que se utiliza para la autenticación y la autorización durante el flujo de trabajo de impresión.
- OpenText Micro Focus Enterprise Server es un entorno de implementación de aplicaciones para aplicaciones de mainframe. Proporciona el entorno de ejecución para las aplicaciones de mainframe que se migran o crean con cualquier versión de Micro Focus Enterprise Developer. OpenText

Epics

Configure el tiempo de ejecución de OpenText Micro Focus e implemente una aplicación por lotes para mainframe

Tarea	Descripción	Habilidades requeridas
Configure el tiempo de ejecución e implemente una aplicación de demostración.	Para configurar OpenText Micro Focus Enterprise Server en Amazon EC2 e implementar la aplicación de BankDemo demostración de OpenText Micro Focus, siga las instrucciones de la guía del usuario de AWS Mainframe Modernization. La BankDemo aplicación es una aplicación por lotes para mainframe que crea y, a continuación, inicia la impresión.	Arquitecto de la nube

Configurar un servidor de impresión LRS en Amazon EC2

Tarea	Descripción	Habilidades requeridas
Cree una instancia de Amazon EC2 para Windows.	Para lanzar una instancia de Amazon EC2 para Windows, siga las instrucciones del Step 1: Launch an instance (Paso 1: lanzamiento de una instancia) de la documentación de Amazon EC2. Utilice el mismo nombre de host que utilizó para la licencia de producto de LRS.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	La instancia debe cumplir los siguientes requisitos de hardware y software para LRS VPSX/MFI: • CPU: doble núcleo • RAM: 16 GB • Unidad: 500 GB • Instancia EC2 mínima: `m5.xlarge` • Sistema operativo Windows • Software: Internet Information Services (IIS) o Apache Nota: Los requisitos de hardware y software anteriores están pensados para una flota de impresoras pequeña (entre 500 y 1000). Para conocer todos los requisitos, consulte a sus personas de contacto en LRS y AWS. 1. Al crear la instancia de Windows, confirme que el nombre de host de EC2 es el mismo que se utilizó para la licencia de producto de LRS. 2. Conéctese a la instancia EC2 siguiendo las instrucciones del Paso 2: Conéctese a su instancia de la	

Tarea	Descripción	Habilidades requeridas
	documentación de Amazon EC2. 3. En el menú de Windows Start (Inicio), busque y abra Server Manager (Administ rador de servidores). 4. En Server Manager, seleccione Dashboard (Panel de control), Quick Start (Inicio rápido), Add roles and features(Agregar funciones y características) y, a continuación, Server roles (Roles de nivel de servidor). 5. En Funciones de servidor, elija WebServer (IIS) y, a continuación, elija Desarroll o de aplicaciones. 6. En Desarrollo de aplicacio nes, seleccione la casilla de verificación CGI. 7. Para instalar CGI, siga las instrucciones del asistente en Add roles and features (Agregar roles y caracterí sticas) de Windows Server Manager. 8. Abra el puerto 5500 en el firewall de Windows de la instancia EC2 para la comunicación entre LRS/ Queue.	

Tarea	Descripción	Habilidades requeridas
Instale LRS VPSX/MFI en la instancia EC2.	1. Conéctese a la instancia EC2. 2. Abra el enlace a la página de descarga del producto que se muestra en el mensaje de correo electrónico de LRS que habrá recibido. Nota: Los productos de LRS se distribuyen mediante transferencia de archivos electrónica (EFT). 3. Descargue LRS VPSX/MFI y descomprima el archivo (carpeta predeterminada:). `c:\LRS` 4. Para instalar LRS VPSX/MFI, inicie el instalador de producto de LRS desde la carpeta descomprimida. 5. En el menú Select Feature (Seleccionar característica), seleccione VPSX® Server y, a continuación, Next (Siguiente) para iniciar el proceso de instalación. Cuando se complete la instalación, recibirá un mensaje de confirmación.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Instale LRS/Queue.	1. Conéctese a su instancia EC2 de OpenText Micro Focus Enterprise Server. 2. Abra el enlace a la página de descarga del producto LRS que se incluye en el mensaje de correo electrónico de LRS que habrá recibido, descargue LRS/Queue y, a continuación, descomprima el archivo. 3. Vaya a la ubicación en la que descargó los archivos y, a continuación, inicie el instalador de producto de LRS para instalar LRS/Queue. 4. Siga las instrucciones del instalador de producto de LRS para completar el proceso de instalación.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Instale LRS/DIS.	El producto LRS/DIS suele incluirse en la instalación de LRS VPSX. Sin embargo, si LRS/DIS no se instaló junto con LRS VPSX, siga los pasos indicados a continuación para instalarlo: 1. Conéctese a la instancia EC2 de LRS VPSX/MFI. 2. Abra el enlace a la página de descarga del producto LRS que se incluye en el mensaje de correo electrónico de LRS que habrá recibido, descargue LRS/DIS y, a continuación, descomprima el archivo. 3. Vaya a la ubicación en la que descargó los archivos y, a continuación, inicie el instalador de producto de LRS. 4. En el instalador de producto de LRS, amplíe LRS Misc Tools, seleccione LRS DIS y, a continuación, Next (Siguiente). 5. Siga el resto de las instrucciones del instalador del producto de LRS para completar el proceso de instalación.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Crear un grupo de destino.	Cree un grupo de destino siguiendo las instrucciones de Create a target group for your Network Load Balancer (Crear un grupo de destino para el equilibrador de carga de red). Al crear el grupo de destino, registre la instancia EC2 de LRS VPSX/MFI como destino: 1. En la página Specify group details (Especificar detalles del grupo), busque Choose a Target Type (Elegir un tipo de destino) y seleccione Instances (Instancias). 2. En Protocol, seleccione TCP. 3. En Puerto, seleccione 5500. 4. En la página Register targets (Registrar destinos), busque la sección Available instances (Instancias disponibles) y seleccione la instancia EC2 de LRS VPSX/MFI.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Crear un equilibrador de carga de red.	Para crear el equilibrador de carga de red, siga las instrucciones de la documentación de Elastic Load Balancing (Equilibrio de carga elástico). Su Network Load Balancer dirige el tráfico desde OpenText Micro Focus Enterprise Server a la instancia EC2 de LRS VPSX/MFI. Al crear el equilibrador de carga de red, elija los valores siguientes en la página Listeners and Routing (Oyentes y enrutamiento): 1. En Protocol, seleccione TCP. 2. En Puerto, seleccione 5500. 3. En Default action (Acción predeterminada), seleccione Forward to (Reenviar a) para el grupo de destino que ha creado.	Arquitecto de la nube

Integre OpenText Micro Focus Enterprise Server con LRS/Queue y LRS VPSX/MFI

Tarea	Descripción	Habilidades requeridas
Configure Micro Focus Enterprise Server para la integración de LRS/Queue.	1. Conéctese a su instancia EC2 de OpenText Micro Focus Enterprise Server	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	siguiendo las instrucciones de la documentación de Amazon EC2. 2. En el menú Inicio de Windows, abra la interfaz de usuario de administración de OpenText Micro Focus Enterprise Server. 3. En la barra de menús, seleccione NATIVE. 4. En el panel de navegación, seleccione Directory Server y, a continuación, BANKDEMO para su región de Enterprise Server. 5. En General, busque el panel de navegación izquierdo, despláce hacia abajo hasta la sección Additional para configurar las variables del entorno (`LRSQ_ADDRESS`, `LRSQ_PORT`, `LRSQ_COMMAND`) de modo que dirijan hacia LRSQ. • Para LRSQ_ADDRESS, escriba la dirección IP o el nombre DNS del equilibrador de carga de red que creó anteriormente. • Para LRSQ_PORT, especifique VPSX LRSQ Listener Port (5500).	

Tarea	Descripción	Habilidades requeridas
	• Para LRSQ_COMMAND, especifique la ubicación de la ruta del ejecutable de LRSQ. Nota: Actualmente, LRS admite un límite máximo de 50 caracteres para los nombres DNS. Si el nombre DNS tiene más de 50 caracteres, puede utilizar la dirección IP del equilibrador de carga de red como alternativa.	

Tarea	Descripción	Habilidades requeridas
Configure OpenText Micro Focus Enterprise Server para la integración de LRS VPSX/MFI.	1. Copie la carpeta `VPSX_MFI_R2` del instalador de LRS VPSX/MFI a la ubicación del servidor Micro Focus Enterprise en `C\BANKDEMO\print` . 2. Conéctese a la instancia EC2 de Micro Focus Enterprise Server siguiendo las instrucciones de la documentación de Amazon EC2. 3. En el menú Start (Inicio) de Windows, abra la interfaz de usuario de administración de Micro Focus Enterprise Server. 4. En la barra de menús, seleccione NATIVE. 5. En el panel de navegación, seleccione Directory Server y, a continuación, BANKDEMO. 6. En BANKDEMO, seleccione JES. 7. En JES Program Path, agregue la ruta `DLL(VPSX_MFI_R2)` de `C\BANKDEMO\print` .	Arquitecto de la nube

Configurar la cola de impresión y los usuarios de impresión

Tarea	Descripción	Habilidades requeridas
Asocie el módulo OpenText Micro Focus Print Exit al proceso de ejecución del servidor de la impresora por lotes Micro Focus Enterprise Server.	1. Conéctese a su instancia EC2 de OpenText Micro Focus Enterprise Server siguiendo las instrucciones de la documentación de Amazon EC2. 2. En el menú Inicio de Windows, abra la interfaz de usuario de administr ación de OpenText Micro Focus Enterprise Server. 3. En la barra de menús, seleccione NATIVE. 4. En el panel de navegació n, seleccione Directory Server y, a continuación, BANKDEMO. 5. En BANKDEMO, seleccion e JES y desplácese hacia abajo hasta Printers (Impresoras). 6. En Impresoras, asocie el módulo OpenText Micro Focus Print Exit (LRSPRTE6 para Batch) al proceso de ejecución del servidor (SEP) de la impresora por lotes OpenText Micro Focus Enterprise Server. Esto permite enrutar la salida	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	de impresión a LRS VPSX/MFI. Para obtener más información sobre la configuración, consulte Uso de la salida en la documentación de OpenText Micro Focus.	

Tarea	Descripción	Habilidades requeridas
Cree una cola de salida de impresión en el LRS VPSX/MFI e intégrela con el LRS X. PageCenter	1. Conéctese a la instancia EC2 de LRS VPSX/MFI. 2. En el menú Start (Inicio) de Windows, abra VPSX Web Interface. 3. En el panel de navegación, seleccione Printers (Impresoras). 4. Seleccione Add (Agregar) y, después, Add Printer (Agregar impresora). 5. En la página Printer Configuration (Configuración de la impresora), busque Printer Name (Nombre de impresora) y especifique Local. 6. Para VPSX ID, introduzca VPS1. 7. Para CommType, seleccione TCPIP/LRSQ. 8. En Host/Dirección IP, introduzca la dirección IP del Network Load Balancer que se encuentra frente a las instancias LRS X EC2. PageCenter 9. Para Remote port (Puerto remoto), especifique 5800. 10. En Remote Queue, introduzca el nombre de la carpeta de documentos del LRS PageCenter X	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	en la que se almacenará la salida. 11. Seleccione Add (Agregar).	

Tarea	Descripción	Habilidades requeridas
Cree un usuario de impresión en LRS VPSX/MFI.	1. Conéctese a la instancia EC2 de LRS VPSX/MFI. 2. En el menú Start (Inicio) de Windows, abra VPSX Web Interface. 3. En el panel de navegación, seleccione Security y, a continuación, la opción Users (Usuarios). 4. En la columna Nombre de usuario, seleccione admin y, a continuación, seleccione Copiar. 5. En la ventana Mantenimiento del perfil de usuario, en Nombre de usuario, introduzca un nombre de usuario (por ejemplo, PrintUser). 6. En Descripción, escriba una descripción breve (por ejemplo, Usuario para impresión de prueba). 7. Seleccione Update (Actualizar). Esto crea un usuario de impresión (por ejemplo, PrintUser). 8. En el panel de navegación, busque User y seleccione el nuevo usuario que ha creado.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	9. En el menú Command (Comandos), seleccione Security (Seguridad). 10. En la página Reglas de seguridad, seleccione todas las opciones de seguridad de la impresora y seguridad laboral aplicables y, a continuación, seleccione Guardar. 11. Para agregar el nuevo usuario de impresión al grupo Administrator, acceda al panel de navegación, seleccione Security y, a continuación, Configure (Configurar). 12. En la ventana Configuración de seguridad, añada su nuevo usuario de impresión a la columna Administrador.	

Configuración de un servidor LRS PageCenter X en Amazon EC2

Tarea	Descripción	Habilidades requeridas
Cree una instancia de Amazon EC2 para Windows.	Para lanzar una instancia de Amazon EC2 para Windows, siga las instrucciones del Step 1: Launch an instance (Paso 1: lanzamiento de una instancia) de la documentación de Amazon EC2. Utilice	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	el mismo nombre de host que utilizó para la licencia de producto de LRS. La instancia debe cumplir los siguientes requisitos de hardware y software para PageCenter LRS X: • CPU: doble núcleo • RAM: 16 GB • Unidad: 500 GB • Instancia EC2 mínima: `m5.xlarge` • Sistema operativo Windows • Software: IIS o Apache Nota: los requisitos de hardware y software anteriores están pensados para una flota de impresoras pequeña (entre 500 y 1000). Para conocer todos los requisitos, consulte a sus personas de contacto en LRS y AWS. 1. Al crear la instancia de Windows, confirme que el nombre de host de EC2 es el mismo que se utilizó para la licencia de producto de LRS. 2. Conéctese a la instancia EC2 siguiendo las instrucci	

Tarea	Descripción	Habilidades requeridas
	ones de la documentación de Amazon EC2. 3. En el menú de Windows Start (Inicio), busque y abra Server Manager (Administ rador de servidores). 4. En Server Manager, seleccione Dashboard (Panel de control), Quick Start (Inicio rápido), Add roles and features(Agregar funciones y características) y, a continuación, Server roles (Roles de nivel de servidor). 5. En Funciones de servidor, elija WebServer (IIS) y, a continuación, Desarrollo de aplicaciones. 6. En Desarrollo de aplicacio nes, seleccione la casilla de verificación CGI. 7. Para instalar CGI, siga las instrucciones del asistente en Add roles and features (Agregar roles y caracterí sticas) de Windows Server Manager. 8. Abra el puerto 5800 para el tráfico TCP/IP entrante en el firewall de Windows de la instancia EC2. El LRS VPSX utiliza el protocolo TCPIP/LRSQ en el puerto	

Tarea	Descripción	Habilidades requeridas
	5800 para comunicarse con el LRS X. PageCenter	
Instale PageCenter LRS X en la instancia EC2.	1. Conéctese a la instancia EC2. 2. Abra el enlace a la página de descarga del producto que se muestra en el mensaje de correo electrónico de LRS que habrá recibido. Nota: Los productos de LRS se distribuyen mediante transferencia de archivos electrónica (EFT). 3. Descargue LRS PageCenter X y descomprima el archivo (carpeta predeterminada:). `c:\LRS` 4. Para instalar LRS PageCenter X, inicie el instalador de productos LRS desde la carpeta descomprimida. 5. En el menú Seleccionar funciones, seleccione PageCenterX y, a continuación, elija Siguiente para iniciar el proceso de instalación. Cuando se complete la instalación, recibirá un mensaje de confirmación.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Instale LRS/DIS.	El producto LRS/DIS suele incluirse en la instalación de LRS VPSX. Sin embargo, si LRS/DIS no se instaló junto con LRS VPSX, siga los pasos indicados a continuación para instalarlo: 1. Conéctese a su instancia LRS PageCenter X EC2. 2. Abra el enlace a la página de descarga del producto LRS que se incluye en el correo electrónico de LRS que habrá reqcibido , descargue LRS/DIS y, a continuación, descomprima el archivo. 3. Vaya a la ubicación en la que descargó los archivos y, a continuación, inicie el instalador de producto de LRS. 4. En el instalador de producto de LRS, amplíe LRS Misc Tools, seleccione LRS DIS y, a continuación, Next (Siguiente). 5. Siga el resto de las instrucci ones del instalador del producto de LRS para completar el proceso de instalación.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Crear un grupo de destino.	Cree un grupo de destino siguiendo las instrucciones de Create a target group for your Network Load Balancer (Crear un grupo de destino para el equilibrador de carga de red). Al crear el grupo de destino, registre la instancia LRS PageCenter X EC2 como destino: 1. En la página Specify group details (Especificar detalles del grupo), busque Choose a Target Type (Elegir un tipo de destino) y seleccione Instances (Instancias). 2. En Protocol, seleccione TCP. 3. En Puerto, seleccione 5800. 4. En la página Registrar destinos, en la sección Instancias disponibles, seleccione la instancia LRS PageCenter X EC2.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Crear un equilibrador de carga de red.	Para crear el equilibrador de carga de red, siga las instrucciones de la documentación de Elastic Load Balancing (Equilibrio de carga elástico). Su Network Load Balancer enruta el tráfico desde LRS VPSX/MFI a la instancia EC2 de LRS X. PageCenter Al crear el equilibrador de carga de red, elija los valores siguientes en la página Listeners and Routing (Oyentes y enrutamiento): 1. En Protocol, seleccione TCP. 2. En Puerto, seleccione 5800. 3. En Default action (Acción predeterminada), seleccione Forward to (Reenviar a) para el grupo de destino que ha creado.	Arquitecto de la nube

Configure las funciones PageCenter de administración de salida en LRS X

Tarea	Descripción	Habilidades requeridas
Habilite la función de importación en LRS X. PageCenter	Puede utilizar la función de importación de LRS PageCenter X para reconocer las salidas que llegan al LRS PageCenter X mediante	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	criterios como el nombre del trabajo o el ID del formulari o. A continuación, puede enrutar los resultados a carpetas específicas del LRS X. PageCenter Para habilitar la importación, siga estos pasos: 1. Conéctese a su instancia LRS PageCenter X EC2 siguiendo las instrucciones de la documentación de Amazon EC2. 2. En el menú Start (Inicio) de Windows, abra PCX Web Interface. 3. En Folder Explorer (Explorador de carpetas), seleccione Admin. 4. En la página Configura tion, seleccione Advanced, Import parameter (Parámetr o de importación). 5. En la sección Import parameter, active la casilla Advanced Import (Importac ión avanzada). 6. Para confirmar los cambios, seleccione Update (Actualiz ar).	

Tarea	Descripción	Habilidades requeridas
Configure la política de conservación de documentos.	LRS PageCenter X utiliza una política de retención de documentos para decidir durante cuánto tiempo se debe conservar un documento en LRS X. PageCenter Para configurar la política de conservación de documentos, siga los pasos siguientes: 1. Conéctese a su instancia LRS PageCenter X EC2. 2. En el menú Start (Inicio) de Windows, abra PCX Web Interface. 3. En Folder Explorer (Explorador de carpetas), seleccione Admin. 4. En la página Admin, seleccione Archive Group List/General Admin y, a continuación, Retention policy (Política de conservación). 5. En la sección Retention policy, seleccione Add para crear una política de conservación. 6. En la página Retention Policy Information (Información de la política de conservación), especifique un Retention policy	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	name (nombre de política de conservación), una Description y el período de Document retention (Conservación de documentos). 7. Seleccione Ok (Aceptar) para guardar la nueva política.	

Tarea	Descripción	Habilidades requeridas
Cree una regla para enrutar el documento de salida a una carpeta específica de LRS X. PageCenter	En LRS PageCenter X, Destination determina la ruta de la carpeta a la que se enviará la salida cuando Report Definition invoque este destino. Para este ejemplo, cree una carpeta basada en la carpeta de Form ID en la definición del informe y guarde el resultado en esa carpeta. 1. Conéctese a su instancia LRS PageCenter X EC2. 2. En el menú Start (Inicio) de Windows, abra PCX Web Interface. 3. En Folder Explorer (Explorador de carpetas) , seleccione Admin, Advanced Import (Importación avanzada) y Destination (Destino). 4. En la sección Destination, seleccione Add (Agregar) para abrir el formulario Destination Maintenance (Mantenimiento del destino). 5. En el formulario de Destination Maintenance, especifique los valores siguientes: • Destination name: Form (Formulario)	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	• Description: Una descripción del destino, como Form-based folder structure (Estructura de carpeta basada en formularios) • Destination type: Folder (Carpeta) • Parámetros de carpeta: ruta de importación de la carpeta (la ruta de la carpeta que se creará en PageCenter X cuando llegue el documento; por ejemplo, la ruta **`/Test/&FORM/&IMPORTDATE/&IMPORTTIME`** creará una **`Test`** carpeta base, una subcarpeta basada en el nombre del ID del formulario, una subcarpeta basada en la fecha de importación y **`STD`**, por último, una subcarpeta en función de la hora de importación) • Document name (Nombre del documento): El nombre dinámico que se asigna a un documento cuando se guarda en la carpeta. 6. En la lista desplegable, seleccione una política de	

Tarea	Descripción	Habilidades requeridas
	conservación. A modo de ejemplo, seleccione Year1 para retener el documento durante 1 año. 7. Seleccione Ok (Aceptar) para guardar los cambios.	

Tarea	Descripción	Habilidades requeridas
Cree una definición de informe.	1. Conéctese a su instancia LRS PageCenter X EC2. 2. En el menú Start (Inicio) de Windows, abra PCX Web Interface. 3. En Folder Explorer (Explorador de carpetas) , seleccione Admin, Advanced Import (Importación avanzada), Report Definition (Definición de informe) y, a continuación, Add (Agregar). 4. En la página Report definition maintenance (Mantenimiento de la definición del informe), busque la pestaña General y especifique el Report Definition Name (nombre de la definición de informe). 5. En la pestaña General, busque Fields (Campos), donde puede especificar criterios de selección como Job Name (Nombre del trabajo), Form (Formulario), Class (Clase) y Author (Autor). Así, por ejemplo, puede especificar un Job Name de MFIDEMO. El valor Job Name será el nombre del trabajo por lotes	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	que generará la salida de impresión. 6. En la pestaña Destination, busque Available Destination (Destino disponible) y seleccione el destino creado anteriormente (Form). 7. Seleccione Add (Agregar) para agregar el destino del Form (Formulario) como Assigned destination (Destino asignado). Nota: Este ejemplo incluye una definición de informe en la que una salida generada por el MFIDEMO y enviada al LRS PageCenter X se guarda en la estructura de carpetas definida en la definición de destino.	

Configurar la autenticación y autorización para administración de la producción

Tarea	Descripción	Habilidades requeridas
Cree un dominio de AWS Managed Microsoft AD con usuarios y grupos.	1. Para crear un directorio en AWS Managed Microsoft AD, siga las instrucciones de Create your AWS Managed Microsoft AD Directory.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	2. Para implementar una instancia de EC2 (administrador de Active Directory) e instalar herramientas de Active Directory con el fin de administrar su AWS Managed Microsoft AD, siga las instrucciones del Step 3: Deploy an EC2 instance to manage your AWS Managed Microsoft AD Paso 3: Implementar una instancia de EC2 para administrar su AWS Managed Microsoft AD). 3. Para conectarse a la instancia EC2, siga las instrucciones de la documentación de Amazon EC2. Nota: Cuando se conecte a la instancia EC2, en la ventana de seguridad de Windows, introduzca las credenciales de administrador del directorio que creó en el paso 1. 4. Una vez que haya iniciado sesión, en el menú Inicio, bajo Herramientas administrativas de Windows, seleccione Usuarios y equipos de Active Directory.	

Tarea	Descripción	Habilidades requeridas
	5. Para crear un usuario de impresión en el dominio de Active Directory, siga las instrucciones de Crear un usuario.	
La instancia de base de datos se une al dominio de AWS Managed Microsoft AD.	Une las instancias LRS VPSX/MFI y LRS X PageCenter EC2 a tu dominio de AWS Managed Microsoft AD de forma automática (documentación del AWS Knowledge Center) o manualmente (documentación de AWS Directory Service).	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Configure e integre LRS/DIS con AWS Managed Microsoft AD para la instancia LRS PageCenter X EC2.	1. Conéctese a su instancia LRS PageCenter X EC2. 2. En el menú Start (Inicio) de Windows, abra PCX Web Interface. 3. En Folder Explorer (Explorador de carpetas), seleccione Admin. 4. En la página Configuration, busque la sección Security Parameters y, en Security Type, seleccione LRS/DIS. 5. Especifique sus preferenc ias para el resto de las opciones en la sección Parámetros de seguridad. 6. En el menú Inicio de Windows, abra la carpeta PageCenterX, elija Server Start y, a continuación, seleccione Server Stop. 7. Inicie sesión en LRS PageCenter X con su nombre de usuario y contraseña de Active Directory.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Configure un grupo de importación para importar la salida de LRS VPSX a LRS X. PageCenter	1. Conéctese a su instancia LRS PageCenter X EC2. 2. En el menú Start (Inicio) de Windows, abra PCX Web Interface. 3. En Folder Explorer (Explorador de carpetas), seleccione Admin, Security admin y Groups. 4. En la sección Groups, seleccione Add (Agregar) para abrir el formulario Group preference. 5. En el formulario Group preference, especifique los valores de Group name y Description. 6. Expanda General options y, a continuación, seleccione la casilla Import. 7. Seleccione Ok (Aceptar) para guardar los cambios.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Agregue una regla de seguridad a Import group (Grupo de importación).	1. Abra el menú contextual (haga clic con el botón derecho) de Import group. 2. Seleccione Advance (Avanzado)y, a continuación, Security. 3. En la sección Security (Seguridad), seleccione Import (Importar) y marque la casilla de verificación Subfolder (Subcarpeta). 4. Seleccione Apply (Aplicar) para guardar los cambios.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Cree un usuario en LRS PageCenter X para importar la salida desde LRS VPSX/MFI.	Al crear un usuario en LRS PageCenter X para importar la salida, el nombre de usuario debe ser el mismo que el ID de VPSX de la cola de salida de impresión en LRS VPSX/MFI. En este ejemplo, el VPSX ID es VPS1. 1. Conéctese a su instancia LRS PageCenter X EC2. 2. En el menú Start (Inicio) de Windows, abra PCX Web Interface. 3. En Folder Explorer (Explorador de carpetas), seleccione Admin, Security admin y User. 4. Seleccione Add (Agregar) para abrir el formulario User profile maintenance (Mantenimiento del perfil de usuario). 5. En User profile maintenan ce (Mantenimiento del perfil de usuario), busque User name y escriba VPS1.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Agregue el usuario de importación de LRS PageCenter X al grupo de importación exclusiva.	Para conceder los permisos necesarios para la importación de documentos de LRS VPSX a LRS PageCenter X, haga lo siguiente: 1. Conéctese a su instancia LRS PageCenter X EC2. 2. En el menú Start (Inicio) de Windows, abra PCX Web Interface. 3. En Folder Explorer (Explorador de carpetas), seleccione Admin, Security admin y Groups. 4. En la sección Groups, abra el menú contextual (haga clic con el botón derecho) para el grupo Import only (Solo de importación) y, a continuación, seleccione Advance, Security. 5. En la página Registros de seguridad de carpetas (ImportOnly), seleccione la pestaña Usuario. 6. En la pestaña User, busque Name y seleccione el usuario VPS1 de la lista desplegable; seleccione Apply (Aplicar).	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Configure LRS/DIS con AWS Managed Microsoft AD para la instancia EC2 de VPSX/MFI.	1. Conéctese a la instancia EC2 de LRS VPSX/MFI. 2. En el menú Start (Inicio) de Windows, abra VPSX Web Interface. 3. En el panel de navegación, seleccione Security y, a continuación, la opción Configure (Configurar). 4. En la página Security Configuration, busque la sección Security Parameters y, en Security Type, seleccione LRS/DIS (External). 5. Especifique sus preferencias para el resto de las opciones en la sección Parámetros de seguridad. 6. En el menú Start (Inicio) de Windows, abra la carpeta LRS Output Management, seleccione Server Start (Inicio del servidor) y, a continuación, Server Stop. 7. Inicie sesión en LRS VPSX/MFI con su nombre de usuario y contraseña de Active Directory.	Arquitecto de la nube

Configure Amazon FSx for Windows File Server como almacén de datos operativos para PageCenter LRS X

Tarea	Descripción	Habilidades requeridas
Cree un sistema de archivos para LRS X. PageCenter	Para utilizar Amazon FSx for Windows File Server como almacén de datos operativo para PageCenter LRS X en un entorno Multi-AZ, siga las instrucciones del paso 1: Creación del sistema de archivos.	Arquitecto de la nube
Asigne el archivo compartido a la instancia EC2 de LRS X. PageCenter	Para asignar el recurso compartido de archivos creado en el paso anterior a la instancia LRS PageCenter X EC2, siga las instrucciones del paso 2: Asigne el recurso compartido de archivos a una instancia EC2 que ejecute Windows Server.	Arquitecto de la nube
Asigne el directorio de control y el directorio de carpetas maestras del LRS PageCente r X a la unidad compartida de red Amazon FSx.	1. Conéctese a su instancia LRS PageCenter X EC2 siguiendo las instrucciones de la documentación de Amazon EC2. 2. En el menú Start (Inicio) de Windows, abra PCX Web Interface. 3. En Folder Explorer (Explorador de carpetas) , seleccione Admin, Configuration.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	4. En la página Configuration, seleccione Directories y, a continuación, Control Directory (Directorio de control). 5. En Control Directories, especifique `\\FSx file share DNS name\share\cntl` . 6. En Master Folder Directory (Directorio de carpetas maestras), especifique `\\FSx file share DNS name\share\mstr` .	

Pruebe un flujo de trabajo de administración de la producción

Tarea	Descripción	Habilidades requeridas
Inicie una solicitud de impresión por lotes desde la aplicación OpenText Micro Focus. BankDemo	1. Abra el emulador de terminal 3270 en su instancia EC2 de OpenText Micro Focus Enterprise Server. 2. Conéctese a la BankDemo aplicación ejecutando el comando`connect 127.0.0.1:9278` . 3. En la interfaz de línea de BankDemo comandos, para ID de usuario, escriba B0001. En Password (Contraseña), especifique	Ingeniero de pruebas

Tarea	Descripción	Habilidades requeridas
	una clave que no esté en blanco. 4. Para la opción Request printed statement(s) (Solicitar extractos impresos), escriba X en la línea en blanco. 5. En la sección Send statement by (Enviar extracto por), para Mail, escriba Y (Sí) y, a continuación, pulse F10.	

Tarea	Descripción	Habilidades requeridas
Compruebe el resultado de impresión en el LRS X. PageCenter	1. Conéctese a su instancia LRS PageCenter X EC2 siguiendo las instrucciones de la documentación de Amazon EC2. 2. En el menú Start (Inicio) de Windows, abra PCX Web Interface. 3. En el panel de navegación, abra la carpeta Test, la carpeta STD y, a continuación, la carpeta con la fecha de ejecución de la tarea, por ejemplo `08-03-2023` (MM-DD-AAAA). Nota: Esta es la misma estructura de carpetas que se define en la historia Cree una regla para enrutar el documento de salida a una carpeta específica en LRS X. PageCenter 4. Abra el archivo `formtest-STD.txt` . Ya puede ver el resultado impreso de un extracto de cuenta con columnas para Account No. (Número de cuenta), Description, Date, Amount (Importe) y Balance (Saldo). Para ver un ejemplo, consulte	Ingeniero de pruebas

Tarea	Descripción	Habilidades requeridas
	el archivo `batch_print_output` adjunto de este patrón.	

Recursos relacionados

- LRS
- Advanced Function Presentation data stream (Flujo de datos de presentación de funciones avanzadas) (Documentación de IBM)
- Flujo de datos condicionado por línea (LCDS) (documentación de Compart)
- Micro Focus Enterprise Server en AWS (AWS Quick Starts)
- Empowering Enterprise Mainframe Workloads on AWS with Micro Focus (Capacitación de cargas de trabajo de mainframe empresarial en AWS) (publicación de blog)
- Modernize your mainframe online printing workloads on AWS (Modernice las cargas de trabajo de impresión online de mainframe en AWS) (Recomendaciones de AWS)
- Modernize your mainframe batch printing workloads on AWS (Modernice las cargas de trabajo de impresión por lotes de mainframe en AWS) (Recomendaciones de AWS)

Información adicional

Consideraciones

Durante su proceso de modernización, podría considerar la posibilidad de utilizar una amplia variedad de configuraciones para los procesos en línea y por lotes de mainframe, así como para la producción que generan. Todos los clientes y proveedores que utilizan la plataforma de mainframe la han personalizado con requisitos particulares que afectan directamente a la impresión. Así, por ejemplo, su plataforma actual podría incorporar el flujo de datos AFP de IBM o las pantallas LCD de Xerox en el flujo de trabajo actual. Además, los caracteres de control de carro de mainframe y las palabras del comando de canal pueden afectar al aspecto de la página impresa y requerir un manejo especial. Como parte del proceso de planificación de la modernización, le recomendamos evaluar y comprender las configuraciones de su entorno de impresión específico.

Captura de datos de impresión

OpenText Micro Focus Print Exit transmite la información necesaria para que el LRS VPSX/MFI procese eficazmente el archivo de impresión. La información consta de campos incluidos en los bloques de control correspondientes, como los siguientes:

- JOBNAME
- OWNER (USERID)
- DESTINATION
- FORM
- FILENAME
- WRITER

El LRS VPSX/MFI admite los siguientes mecanismos de procesamiento por lotes de ordenadores centrales para capturar datos de Micro Focus Enterprise Server: OpenText

- Procesamiento de impresión/spool BATCH COBOL mediante instrucciones estándar z/OS JCL SYSOUT DD/OUTPUT.
- Procesamiento de impresión/spool BATCH COBOL mediante instrucciones estándar z/OS JCL CA-SPOOL SUBSYS DD.
- Procesamiento de impresión/spool IMS/COBOL mediante la interfaz CBLTDLI. Para obtener una lista completa de los métodos y ejemplos de programación compatibles, consulte la documentación de LRS que se incluye con la licencia del producto.

Comprobaciones de estado de la flota de impresoras

LRS VPSX/MFI (LRS LoadX) puede llevar a cabo comprobaciones de estado exhaustivas, incluida la gestión de los dispositivos y la optimización operativa. La administración de dispositivos puede detectar un error en un dispositivo de impresión y dirigir la solicitud de impresión a una impresora en buen estado. Para obtener más información sobre las comprobaciones de estado exhaustivas de las flotas de impresoras, consulte la documentación de LRS que se incluye con la licencia del producto.

Autenticación y autorización de impresoras

LRS/DIS permite a las aplicaciones de LRS autenticar los ID de usuario y las contraseñas mediante Microsoft Active Directory o un servidor Lightweight Directory Access Protocol (LDAP). Además de la autorización básica de impresión, LRS/DIS también puede aplicar controles de seguridad de impresión detallados en los casos de uso siguientes:

- Gestione quién puede examinar el trabajo de impresión.
- Gestione el nivel de navegación de los trabajos de otros usuarios.
- Gestione las tareas operativas, por ejemplo, la seguridad en el nivel de comandos, como retener o liberar, purgar, modificar, copiar y redirigir. La seguridad se puede configurar mediante el ID de usuario o el grupo, de forma similar a un grupo de seguridad de Active Directory o a un grupo LDAP.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Modernice las cargas de trabajo de impresión por lotes de mainframe en AWS mediante Micro Focus Enterprise Server y LRS VPSX/MFI

Documento creado por Shubham Roy (AWS), Abraham Rondon (Micro Focus), Guy Tucker (Levi, Ray and Shoup Inc) y Kevin Yung (AWS)

Entorno: PoC o piloto	Origen: Mainframe de IBM	Destino: AWS
Tipo R: redefinir la plataforma	Carga de trabajo: IBM	Tecnologías: Mainframe; modernización
Servicios de AWS: AWS Managed Microsoft AD; Amazon EC2; Amazon S3; Amazon EBS		

Resumen

Este patrón le muestra cómo modernizar las cargas de trabajo de impresión por lotes de mainframe, vitales para la empresa, en la nube de Amazon Web Services (AWS) usando Micro Focus Enterprise Server como tiempo de ejecución para una aplicación de mainframe modernizada y LRS VPSX/MFI (Micro Focus Interface) como servidor de impresión. El patrón se basa en el enfoque de modernización del mainframe a través de redefinir la plataforma. Con este enfoque se migran los trabajos por lotes de mainframe a Amazon Elastic Compute Cloud (Amazon EC2), y se migra la base de datos de mainframe, como IBM DB2 para z/OS, a Amazon Relational Database Service (Amazon RDS). AWS Directory Service para Microsoft Active Directory, también conocido como AWS Managed Microsoft AD, se encarga de la autenticación y la autorización del flujo de trabajo de impresión modernizado. El servidor de información de directorio LRS (LRS/DIS) está integrado con AWS Managed Microsoft AD. Al modernizar sus cargas de trabajo de impresión por lotes, puede reducir los costos de infraestructura de TI, mitigar la carga técnica que supone el mantenimiento de los sistemas heredados, eliminar los silos de datos, aumentar la agilidad y la eficiencia con un DevOps modelo y aprovechar los recursos bajo demanda y la automatización en la nube de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una carga de trabajo de gestión de producción o impresión de mainframe
- Conocimientos básicos sobre cómo recompilar y entregar una aplicación de mainframe ejecutada en Micro Focus Enterprise Server (para obtener más información, consulte la hoja de datos de Enterprise Server en la documentación de Micro Focus).
- Conocimientos básicos de las soluciones y conceptos de impresión en la nube de LRS (para obtener más información, consulte Modernización de la producción en la documentación de LRS).
- Software y licencia de Micro Focus Enterprise Server (para obtener más información, póngase en contacto con el departamento de ventas de Micro Focus).
- Software y licencias de LRS VPSX/MFI, LRS/Queue y LRS/DIS (para obtener más información, póngase en contacto con el departamento de ventas de LRS).

Nota: Para obtener más información sobre las consideraciones de configuración de las cargas de trabajo de administración de la producción de mainframe, consulte Consideraciones en la sección Información adicional de este patrón.

Versiones de producto

- Micro Focus Enterprise Server 6.0 (actualización de producto 7)
- LRS VPSX/MFI V1R3 o superior

Arquitectura

Pila de tecnología de origen

- Sistema operativo: IBM z/OS
- Lenguaje de programación: Common Business-Oriented Language (COBOL), Job Control Language (JCL) y Customer Information Control System (CICS)
- Base de datos: IBM DB2 para z/OS y método de acceso a almacenamiento virtual (VSAM)
- Seguridad: Resource Access Control Facility (RACF), CA Top Secret para z/OS y Access Control Facility 2 (ACF2)

- Gestión de producción e impresión: productos de impresión z/OS para IBM mainframe (IBM Tivoli Output Manager para z/OS, LRS y CA View)

Pila de tecnología de destino

- Sistema operativo – Microsoft Windows Server que se ejecuta en Amazon EC2
- Procesamiento: Amazon EC2
- Lenguaje de programación: COBOL, JCL y CICS
- Bases de datos: Amazon RDS
- Seguridad: AWS Managed Microsoft AD
- Administración de impresión y producción: solución de impresión LRS en AWS
- Entorno de tiempo de ejecución de mainframe – Micro Focus Enterprise Server

Arquitectura de origen

El diagrama siguiente muestra una arquitectura de estado actual tipo para una carga de trabajo de administración de la producción de mainframe:

El diagrama muestra el siguiente flujo de trabajo:

1. Los usuarios llevan a cabo transacciones comerciales en un sistema de participación (SoE) que se basa en una aplicación CICS de IBM escrita en COBOL.
2. El SoE utiliza el servicio de mainframe, que registra los datos de las transacciones comerciales en una base de datos system-of-records (SoR), como IBM DB2 for z/OS.
3. El SoR conserva los datos comerciales del SoE.
4. El programador de trabajos por lotes inicia un trabajo por lotes para generar resultados de impresión.
5. El trabajo por lotes extrae datos de la base de datos, formatea los datos de acuerdo con los requisitos comerciales y, a continuación, genera producción empresarial, como extractos de facturación, tarjetas de identificación o extractos de préstamos. Por último, el trabajo por lotes dirige la producción a la administración de la impresión para procesar y enviar los resultados en función de los requisitos empresariales.
6. La gestión de los resultados de producción recibe la producción de impresión del trabajo por lotes y, a continuación, la envía a un destino específico, como el correo electrónico, un archivo

compartido que emplee un FTP seguro, una impresora física que use soluciones de impresión LRS (como se demuestra en este patrón) o IBM Tivoli.

Arquitectura de destino

El diagrama siguiente muestra una arquitectura para una carga de trabajo de administración de la producción de mainframe que se implementa en la nube de AWS:

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El programador de trabajos por lotes inicia un trabajo por lotes para generar la producción, como extractos de facturación, tarjetas de identificación o extractos de préstamos.
2. El trabajo por lotes de mainframe (con redefinición de la plataforma para Amazon EC2) utiliza el tiempo de ejecución de Micro Focus Enterprise Server para extraer datos de la base de datos de la aplicación, aplicar lógica empresarial a los datos y formatearlos, y luego enviar los datos para impresión mediante Micro Focus Print Exit (Documentación de Micro Focus).
3. La base de datos de la aplicación (un SoR que se ejecuta en Amazon RDS) conserva los datos para su impresión.
4. La solución de impresión LRS VPSX/MFI se implementa en Amazon EC2 y sus datos operativos se almacenan en Amazon Elastic Block Store (Amazon EBS). LRS VPSX/MFI emplea el agente de transmisión LRS/Queue, basado en TCP/IP, para recopilar los datos de impresión a través de la API JES Print Exit de Micro Focus y entregarlos a un destino de impresión específico.

Nota: La solución de destino no suele requerir cambios en la aplicación para adaptarse a los lenguajes de formato de mainframe, como IBM Advanced Function Presentation (AFP) o Xerox Line Condition Data Stream (LCDS). Para obtener más información sobre el uso de Micro Focus para la migración y modernización de aplicaciones de mainframe en AWS, consulte Potenciar las cargas de trabajo de mainframe empresarial en AWS con Micro Focus en la documentación de AWS.

Arquitectura de infraestructura de AWS

El diagrama siguiente muestra una arquitectura de infraestructura de AWS segura y de alta disponibilidad para una carga de trabajo de administración de la producción de mainframe:

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El programador de lotes inicia el proceso por lotes y se implementa en Amazon EC2 en varias zonas de disponibilidad para alta disponibilidad (HA). Nota: Este patrón no incluye la implementación del programador de lotes. Para obtener más información acerca de la implementación, consulte la documentación del proveedor de software del programador.
2. El trabajo por lotes del ordenador central (escrito en un lenguajes de programación como JCL o COBOL) utiliza la lógica empresarial básica para procesar y generar la producción de impresión, como extractos de facturación, tarjetas de identificación y extractos de préstamos. El trabajo se implementa en Amazon EC2, en dos zonas de disponibilidad, para conseguir una alta disponibilidad, y emplea Micro Focus Print Exit para enrutar la producción de impresión a LRS VPSX/MFI y que los usuarios finales realicen la impresión.
3. LRS VPSX/MFI utiliza LRS/Queue para recopilar o capturar datos de impresión a través de la interfaz de programación de salida de impresión JES de OpenText Micro Focus. Print Exit transmite la información necesaria para que LRS VPSX/MFI procese eficazmente el archivo de impresión y genere comandos LRS/Queue de forma dinámica. A continuación, los comandos se ejecutan mediante una función estándar integrada de Micro Focus. Nota: para obtener más información sobre los datos de impresión transferidos de Micro Focus Print Exit a LRS/Queue y los mecanismos de procesamiento por lotes de mainframe compatibles con LRS VPSX/MFI, consulte Captura de datos de impresión en la sección Información adicional de este patrón.
4. Un Equilibrador de carga de red proporciona un nombre DNS para integrar el servidor de Micro Focus Enterprise con VPSX/MFI de LRS. Nota: LRS VPSX/MFI admite un equilibrador de carga de capa 4. El equilibrador de carga de red también realiza una comprobación básica del estado de VPSX/MFI de LRS y enruta el tráfico a los destinos registrados cuyo estado es correcto.
5. El servidor de impresión LRS VPSX/MFI se implementa en Amazon EC2 en dos zonas de disponibilidad, para lograr una alta disponibilidad, y emplea Amazon EBS como almacén de datos operativos. LRS VPSX/MFI admite los modos de servicio tanto activo-activo como activo-pasivo. Esta arquitectura emplea múltiples AZ en un par activo-pasivo como activo y modo de espera activa. El equilibrador de carga de red realiza una comprobación de estado de las instancias EC2 de LRS VPSX/MFI y enruta el tráfico a las instancias en espera activas de la otra zona de disponibilidad si una instancia activa se encuentra en estado incorrecto. Las solicitudes de impresión se mantienen en la cola de trabajos del LRS de forma local en cada una de las instancias de EC2. En caso de recuperación, se debe reiniciar una instancia fallida para que los servicios de LRS reanuden el procesamiento de la solicitud de impresión. Nota: El LRS VPSX/MFI también puede realizar comprobaciones de estado a nivel de flota de impresoras. Para obtener más información, consulte Comprobaciones de estado de la flota de impresoras en la sección de Información adicional de este patrón.

6. AWS Managed Microsoft AD se integra con LRS/DIS para llevar a cabo la autenticación y autorización del flujo de trabajo de impresión. Para obtener más información, consulte Autenticación y autorización de impresión en la sección de Información adicional de este patrón.
7. LRS VPSX/MFI emplea Amazon EBS para el almacenamiento en bloques. Puede hacer copias de seguridad de los datos de Amazon EBS de las instancias EC2 activas en Amazon S3 como point-in-time instantáneas y restaurarlos en volúmenes de EBS activos en espera. Para automatizar la creación, retención y eliminación de instantáneas de volúmenes de Amazon EBS, puede usar Amazon Data Lifecycle Manager para establecer la frecuencia de las instantáneas automatizadas y restaurarlas en función de sus necesidades de RTO/RPO.

Herramientas

Servicios de AWS

- Amazon EBS: Amazon Elastic Block Store (Amazon EBS) proporciona volúmenes de almacenamiento por bloques para su uso con instancias de EC2. Los volúmenes de EBS se comportan como dispositivos de bloques sin formatear. Puede montar estos volúmenes como dispositivos en sus instancias.
- Amazon EC2: Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de AWS. Puede utilizar Amazon EC2 para lanzar tantos servidores virtuales como necesite, y puede escalar horizontalmente o reducir horizontalmente.
- Amazon RDS: Amazon Relational Database Service (Amazon RDS) es un servicio web que facilita la configuración, el funcionamiento y el escalado de una base de datos relacional en la nube de AWS. Proporciona una capacidad rentable y de tamaño ajustable para una base de datos relacional y se ocupa de las tareas comunes de administración de bases de datos.
- AWS Managed Microsoft AD: AWS Directory Service para Microsoft Active Directory, también conocido como AWS Managed Microsoft Active Directory, permite que sus cargas de trabajo compatibles con directorios y recursos de AWS empleen Active Directory administrado en AWS.

Otras herramientas

- LRS VPSX/MFI (Micro Focus Interface): VPSX/MFI desarrollada conjuntamente por LRS y Micro Focus, captura la producción en spool de JES de Micro Focus Enterprise Server y la envía con fiabilidad a un destino de impresión específico.
- LRS Directory Integration Server (LRS/DIS): LRS/DIS se utiliza para la autenticación y la autorización durante el flujo de trabajo de impresión.

- LRS/Queue: LRS VPSX/MFI utiliza el agente de transmisión de LRS/Queue en TCP/IP para recopilar o capturar datos de impresión a través de la interfaz de programación de salida de impresión JES de Micro Focus.
- Micro Focus Enterprise Server: Micro Focus Enterprise Server es un entorno de implementación de aplicaciones para aplicaciones de mainframe. Proporciona el entorno de ejecución para las aplicaciones de mainframe que se migran o crean con cualquier versión de Micro Focus Enterprise Developer.

Epics

Configure Micro Focus Enterprise Server en Amazon EC2 e implemente una aplicación por lotes para mainframe

Tarea	Descripción	Habilidades requeridas
Configure Micro Focus Enterprise Server e implemente una aplicación de demostración.	Configure Micro Focus Enterprise Server en Amazon EC2 y, a continuación, despliegue la aplicación de BankDemo demostración de Micro Focus en Amazon EC2 siguiendo las instrucciones de la guía de implementación de Micro Focus Enterprise Server en AWS. La BankDemo aplicación es una aplicación por lotes para mainframe que crea y, a continuación, inicia la impresión.	Arquitecto de la nube

Configurar un servidor de impresión LRS en Amazon EC2

Tarea	Descripción	Habilidades requeridas
Obtenga una licencia de producto LRS para imprimir.	Para obtener una licencia de producto LRS para LRS VPSX/MFI, LRS/Queue y LRS/DIS, póngase en contacto con el Equipo de gestión de producción de LRS. Debe proporcionar los nombres de host de las instancias EC2 en las que se instalarán los productos LRS.	Responsable de compilación
Cree una instancia de Windows en Amazon EC2 para instalar LRS VPSX/MFI.	Lance una instancia de Amazon EC2 para Windows siguiendo las instrucciones del Paso 1: Lanzar una instancia de la documentación de Amazon EC2. La instancia debe cumplir los siguiente s requisitos de hardware y software para LRS VPSX/MFI: • CPU: doble núcleo • RAM: 16 GB • Unidad – 500 GB • Instancia EC2 mínima: m5.xlarge • Sistema operativo: Windows/Linux • Software: Servicio de Información de Internet (IIS) o Apache	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	Nota: Los requisitos de hardware y software anteriores están pensados para una flota de impresoras pequeña (alrededor de 500 a 1000). Para conocer todos los requisitos, consulte a sus personas de contacto en LRS y AWS. Cuando cree la instancia de Windows, haga lo siguiente: 1. Confirme que el nombre de host de EC2 es el mismo nombre de host utilizado para la licencia del producto LRS. 2. Para habilitar CGI en Amazon EC2, siga estos pasos: a. Conéctese a la instancia EC2 siguiendo las instrucciones del Paso 2: Conéctese a su instancia en la documentación de Amazon EC2. b. En el menú Inicio de Windows, busque y abra Server Manager. c. En el panel de Server Manager, elija Panel de control, Inicio rápido, Agregar roles y características. A continuación,	

Tarea	Descripción	Habilidades requeridas
	seleccione Roles de servidor. d. En Funciones de servidor, elija WebServer (IIS) y, a continuac ión, elija Desarrollo de aplicaciones. e. En Desarrollo de aplicaciones, seleccione la casilla de verificación CGI. f. Para instalar CGI, siga las instrucciones del asistente en Agregar roles y características de Windows Server Manager. g. Abra el puerto 5500 en el firewall de Windows de la instancia EC2 para la comunicación entre LRS/ Queue.	

Tarea	Descripción	Habilidades requeridas
Instale LRS VPSX/MFI en la instancia EC2.	1. Conéctese a la instancia EC2 siguiendo las instrucciones del Paso 2: Conéctese a su instancia en la documentación de Amazon EC2. 2. Abra el enlace a la página de descarga del producto que se incluye en el correo electrónico de LRS que debería haber recibido. Nota: Los productos de LRS se distribuyen mediante transferencia de archivos electrónica (EFT). 3. Descargue LRS VPSX/MFI y descomprima el archivo (carpeta predeterminada: `c:\LRS`). 4. Inicie el instalador de productos LRS desde la carpeta descomprimida para instalar LRS VPSX/MFI. 5. En el menú Seleccionar características, seleccione VPSX® Server (V1R3.022) y, a continuación, seleccione Siguiente para iniciar el proceso de instalación. Cuando se complete la instalación, recibirá un mensaje de confirmación.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Instale LRS/Queue.	1. Conéctese a su instancia EC2 de Micro Focus Enterprise Server siguiendo las instrucciones del Paso 2: Conéctese a su instancia en la documentación de Amazon EC2. 2. Abra el enlace a la página de descarga del producto LRS desde el correo electrónico de LRS que debería recibir, descargue LRS/Queue y, a continuación, descomprima el archivo. 3. Vaya a la ubicación en la que descargó los archivos y, a continuación, inicie el instalador del producto LRS para instalar LRS/Queue.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Instale LRS/DIS.	1. Conéctese a la instancia EC2 de LRS VPSX/MFI siguiendo las instrucciones del Paso 2: Conéctese a su instancia en la documentación de Amazon EC2. 2. Abra el enlace a la página de descarga del producto LRS que se incluye en el correo electrónico de LRS que habrá recibido, descargue LRS/DIS y, a continuación, descomprima el archivo. 3. Vaya a la ubicación en la que descargó los archivos y, a continuación, inicie el instalador de producto de LRS. 4. En el instalador de producto de LRS, amplíe LRS Misc Tools, seleccione LRS DIS y, a continuación, Siguiente. 5. Siga el resto de las instrucciones del instalador del producto de LRS para completar el proceso de instalación.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Cree un grupo de destino y registre LRS VPSX/MFI EC2 como destino.	Cree un grupo de destino siguiendo las instrucciones de Crear un grupo de destino para el equilibrador de carga de red en la documentación en el equilibrador de carga de red elástico. Al crear la grupo objetivo, haga lo siguiente: 1. En la página Especific ar los detalles del grupo, en Seleccione un Tipo de destino, seleccione Instancias. 2. En Protocol, seleccione TCP. 3. En Puerto, seleccione 5500. 4. En la página Registrar destinos, en la sección Instancias disponibles, seleccione las instancias EC2 de LRS VPSX/MFI.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Crear un equilibrador de carga de red.	Siga las instrucciones para Crear el equilibrador de carga de red en la documentación de Equilibrador de carga elástico. Su equilibrador de carga de red dirige el tráfico desde Micro Focus Enterpris e Server a la instancia EC2 de LRS VPSX/MFI. Al crear el equilibrador de carga de red, siga los pasos siguientes en la página Listeners and Routing (Oyentes y enrutamiento): 1. En Protocol, seleccione TCP. 2. En Puerto, seleccione 5500. 3. En Default action (Acción predeterminada), seleccion e Forward to (Reenviar a) para el grupo de destino que ha creado.	Arquitecto de la nube

Integrar Micro Focus Enterprise Server con LRS VPSX/MFI y LRS/Queue

Tarea	Descripción	Habilidades requeridas
Configure Micro Focus Enterprise Server para la integración de LRS/Queue.	1. Conéctese a la instancia EC2 de Micro Focus Enterprise Server siguiendo las instrucciones del Paso 2: Conéctese a su instancia	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	en la documentación de Amazon EC2. 2. En el menú Start (Inicio) de Windows, abra la interfaz de usuario de administración de Micro Focus Enterprise Server. 3. En la barra de menús, seleccione NATIVE. 4. En el panel de navegación, seleccione Directory Server y, a continuación, BANKDEMO. 5. En General , busque el panel de navegación izquierdo, despláce hacia abajo hasta la sección Adicional para configurar las variables del entorno (LRSQ_ADDRESS, LRSQ_PORT, LRSQ_COMMAND) de modo que dirijan hacia LRSQ. 6. Para LRSQ_ADDRESS, escriba la dirección IP o el nombre DNS del equilibrador de carga de red que creó anteriormente. 7. Para LRSQ_PORT, especifique VPSX LRSQ Listener Port (5500).	

Tarea	Descripción	Habilidades requeridas
	8. Para LRSQ_COMMAND, especifique la ubicación de la ruta del ejecutable de LRSQ. Nota: actualmente, LRS admite un límite máximo de 50 caracteres para los nombres de DNS, pero este aspecto cambiará en el futuro. Si el nombre DNS tiene más de 50 caracteres, puede utilizar la dirección IP del equilibrador de carga de red como alternativa.	

Tarea	Descripción	Habilidades requeridas
Configure Micro Focus Enterprise Server para la integración de LRS VPSX/MFI.	1. Copie la carpeta `VPSX_MFI_R2` del instalador de LRS VPSX/MFI a la ubicación del servidor Micro Focus Enterprise en `C\BANKDEMO\print` . 2. Conéctese a la instancia EC2 de Micro Focus Enterprise Server siguiendo las instrucciones del Paso 2: Conéctese a su instancia en la documentación de Amazon EC2. 3. En el menú Start (Inicio) de Windows, abra la interfaz de usuario de administración de Micro Focus Enterprise Server. 4. En la barra de menús, seleccione NATIVE. 5. En el panel de navegación, seleccione Directory Server y, a continuación, BANKDEMO. 6. En BANKDEMO, seleccione JES. 7. En JES Program Path, agregue la ruta `DLL(VPSX_MFI_R2)` de `C\BANKDEMO\print` .	Arquitecto de la nube

Configure impresoras y usuarios de impresión en Micro Focus Enterprise Server y LRS VPSX/MFI

Tarea	Descripción	Habilidades requeridas
Asocie el módulo Micro Focus Print Exit al proceso de ejecución del servidor de la impresora por lotes del Micro Focus Enterprise Server.	1. Conéctese a la instancia EC2 de Micro Focus Enterprise Server siguiendo las instrucciones del Paso 2: Conéctese a su instancia en la documentación de Amazon EC2. 2. En el menú Start (Inicio) de Windows, abra la interfaz de usuario de administración de Micro Focus Enterprise Server. 3. En la barra de menús, seleccione NATIVE. 4. En el panel de navegación, seleccione Directory Server y, a continuación, BANKDEMO. 5. En BANKDEMO, seleccione JES y desplácese hacia abajo hasta Printers (Impresoras). 6. En Printers (Impresoras),asocie el módulo Micro Focus Print Exit (LRSPRTE6 for Batch) al Server Execution Process (SEP) (proceso de ejecución del servidor) de la impresora por lotes de Micro Focus Enterprise Server. Esto permite	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	enrutar la salida de impresión a LRS VPSX/MFI. 7. Inicie sesión en la interfaz de usuario de Enterprise Server Administration. Para obtener más información sobre la configuración, consulte Using the Exit (Uso de la salida) en la documentación de Micro Focus.	

Tarea	Descripción	Habilidades requeridas
Añada una impresora en LRS VPSX/MFI.	1. Conéctese a la instancia EC2 de LRS VPSX/MFI siguiendo las instrucciones del Paso 2: Conéctese a su instancia en la documentación de Amazon EC2. 2. Abra la interfaz web de VPSX desde el menú Inicio de Windows. 3. En el panel de navegación, seleccione Impresoras. 4. Seleccione Add (Agregar) y, después, Add Printer (Agregar impresora). 5. En la página Printer Configuration (Configuración de la impresora), busque Printer Name (Nombre de impresora) y especifique Local. 6. Para VPSX ID, introduzca VPS1. 7. Para CommType, seleccione TCPIP/LRSQ. 8. En Host/Dirección IP, introduzca la dirección IP de la impresora física que desee agregar. 9. En Dispositivo, introduzca el nombre de su dispositivo. 10. Seleccione Controlador de Windows o Controlador de Linux/Mac.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	11. Seleccione Add (Agregar).	

Tarea	Descripción	Habilidades requeridas
Cree un usuario de impresión en LRS VPSX/MFI.	1. Conéctese a su instancia EC2 de LRS VPSX/MFI siguiendo las instrucciones del Paso 2: Conéctese a su instancia en la documentación de Amazon EC2. 2. Abra la interfaz web de VPSX desde el menú Inicio de Windows. 3. En el panel de navegación, elija Seguridad y luego elija la opción Usuarios. 4. En la columna Nombre de usuario, seleccione admin y, a continuación, seleccione Copiar. 5. En la ventana Mantenimiento del perfil de usuario, en Nombre de usuario, introduzca un nombre de usuario (por ejemplo,). PrintUser 6. En Descripción, escriba una descripción breve (por ejemplo, Usuario para impresión de prueba). 7. Seleccione Update (Actualizar). Esto crea un usuario de impresión (por ejemplo, PrintUser). 8. En el panel de navegación, en Usuario, seleccion	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	e el nuevo usuario que ha creado. 9. En el menú Comandos, seleccione Seguridad. 10. En la página Reglas de seguridad, seleccione todas las opciones de seguridad de la impresora y seguridad laboral aplicables y, a continuación, seleccione Guardar. 11. Para añadir el nuevo usuario de impresión al grupo Administrador, vaya al panel de navegación, seleccione Seguridad y, a continuación, seleccione Configurar. 12. En la ventana Configuración de seguridad, añada su nuevo usuario de impresión a la columna Administrador.	

Configure imprimir autenticación y autorización

Tarea	Descripción	Habilidades requeridas
Cree un dominio de AWS Managed Microsoft AD con usuarios y grupos.	1. Para crear un directorio Active en AWS Managed Microsoft AD, siga las instrucciones de ree su directorio de AWS	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	Managed Microsoft AD en la documentación de AWS Directory Service. 2. Implemente una instancia EC2 (administrador de Active Directory) e instale las herramientas de Active Directory para administrar su AD de Microsoft administrado por AWS siguiendo las instrucciones del Paso 3: Implementar una instancia EC2 para administrar su AD de Microsoft administrado por AWS en la documentación de AWS Directory Service. 3. Conéctese a la instancia EC2 siguiendo las instrucciones del Paso 2: Conéctese a su instancia en la documentación de Amazon EC2. Nota: Cuando se conecte a la instancia EC2, introduzca sus credenciales de administrador (para el directorio que creó en el primer paso) en la ventana de seguridad de Windows. 4. En el menú Inicio de Windows, bajo Herramientas administrativas de Windows, seleccione	

Tarea	Descripción	Habilidades requeridas
	Usuarios y equipos de Active Directory. 5. Cree un usuario de impresión en el dominio de Active Directory siguiendo los pasos de Crear un usuario de la documentación de AWS Directory Service.	
Una LRS VPSX/MFI EC2 a un dominio de AWS Managed Microsoft AD.	Una LRS VPSX/MFI EC2 a su dominio de AWS Managed Microsoft AD de forma automática (documentación del Centro de conocimientos de AWS) o manualmente (documentación de AWS Directory Service).	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Configure e integre LRS/DIS con AWS Managed Microsoft AD.	1. Conéctese a su instancia EC2 de LRS VPSX/MFI siguiendo las instrucciones del Paso 2: Conéctese a su instancia en la documentación de Amazon EC2. 2. En el menú Start (Inicio) de Windows, abra VPSX Web Interface. 3. En el panel de navegación, elija Seguridad y, a continuación, elija Configurar. 4. En la página Configuración de seguridad, en la sección Parámetros de seguridad, en Tipo de seguridad, seleccione Interna. 5. Especifique sus preferencias para el resto de las opciones en la sección Parámetros de seguridad. 6. Abra la carpeta LRS Output Management desde el menú Inicio de Microsoft Windows, seleccione Iniciar el servidor y, a continuación, seleccione Detener el servidor. 7. Inicie sesión en LRS VPSX/MFI con su nombre de usuario y contraseña de Active Directory.	Arquitecto de la nube

Pruebe un flujo de trabajo de impresión

Tarea	Descripción	Habilidades requeridas
Inicie una solicitud de impresión por lotes desde la BankDemo aplicación Micro Focus.	1. Abra el emulador de terminal 3270 en su instancia EC2 de Micro Focus Enterprise Server. 2. Conéctese a la BankDemo aplicación ejecutando el siguiente comando: `connect 127.0.0.1 :9278` 3. En la interfaz de línea de BankDemo comandos, para ID de usuario, escriba B0001. En Password (Contraseña), especifique una clave que no esté en blanco. 4. Para la opción Request printed statement(s) (Solicitar extractos impresos), escriba X en la línea en blanco. 5. En la sección Send statement by (Enviar extracto por), para Mail, escriba Y (Sí) y, a continuación, pulse F10.	Ingeniero de pruebas
Compruebe la producción de impresión en LRS VPSX/MFI.	1. Conéctese a la instancia EC2 de LRS VPSX/MFI siguiendo las instrucciones del Paso 2: Conéctese a su	Ingeniero de pruebas

Tarea	Descripción	Habilidades requeridas
	instancia en la documentación de Amazon EC2. 2. En el menú Start (Inicio) de Windows, abra VPSX Web Interface. 3. En el panel de navegación, seleccione Impresoras y, a continuación, seleccione Cola de producción. 4. En la columna ID de bobina, seleccione la ID de bobina de la solicitud en la cola de impresora. 5. En la pestaña Acciones, en la columna COMANDO, seleccione Examinar. Ya puede ver el resultado impreso de un extracto de cuenta con columnas para Account No. (Número de cuenta), Description, Date, Amount (Importe) y Balance (Saldo). Para ver un ejemplo, consulte el archivo adjunto batch_print_output para este patrón.	

Recursos relacionados

- Modernización de la producción de LRS (documentación de LRS)
- Controles ANSI y de carro de máquinas (documentación de IBM)
- Palabras de comando de canal (documentación de IBM)

- Empowering Enterprise Mainframe Workloads on AWS with Micro Focus (Capacitación de cargas de trabajo de mainframe empresarial en AWS) (publicación de blog de socio de AWS)
- Compilación de un PAC de Micro Focus Enterprise Server con Amazon EC2 Auto Scaling y Systems Manager (documentación de Recomendaciones de AWS)
- Flujo de datos de Presentación de funciones avanzadas (AFP) (documentación de IBM)
- Flujo de datos condicionado por línea (LCDS) (documentación de Compart)
- Micro Focus Enterprise Server en AWS (AWS Quick Starts)

Información adicional

Consideraciones

Durante su proceso de modernización, podría considerar la posibilidad de utilizar una amplia variedad de configuraciones para los procesos en línea y por lotes de mainframe, así como para la producción que generan. Todos los clientes y proveedores que utilizan la plataforma de mainframe la han personalizado con requisitos particulares que afectan directamente a la impresión. Por ejemplo, su plataforma actual puede incorporar Advanced Function Presentation (AFP) de IBM o Line Condition Data Stream (LCDS) de Xerox en el flujo de trabajo actual. Además, los caracteres de control de carro de mainframe y las palabras de comando de canal pueden afectar al aspecto de la página impresa y pueden requerir un tratamiento especial. Como parte del proceso de planificación de la modernización, le recomendamos evaluar y comprender las configuraciones de su entorno de impresión específico.

Captura de datos de impresión

Micro Focus Print Exit transmite la información necesaria para que LRS VPSX/MFI procese eficazmente el archivo en spool. La información consta de campos incluidos en los bloques de control correspondientes, como los siguientes:

- JOBNAME
- OWNER (USERID)
- DESTINATION
- FORM
- FILENAME
- ESCRITOR

LRS VPSX/MFI admite los siguientes mecanismos de procesamiento por lotes de mainframe para capturar datos de QMicro Focus Enterprise Server.

- Procesamiento de impresión/spool BATCH COBOL mediante instrucciones estándar z/OS JCL SYSOUT DD/OUTPUT
- Procesamiento de impresión/spool BATCH COBOL mediante instrucciones estándar z/OS JCL CA-SPOOL SUBSYS DD
- Procesamiento de impresión/spool IMS/COBOL mediante la interfaz CBLTDLI (Para obtener una lista completa de los métodos y ejemplos de programación compatibles, consulte la documentación de LRS que se incluye con la licencia del producto).

Comprobación de estado de la flota de impresoras

LRS VPSX/MFI (LRS LoadX) puede llevar a cabo comprobaciones de estado exhaustivas, incluida la gestión de los dispositivos y la optimización operativa. La administración de dispositivos puede detectar un error en un dispositivo de impresión y dirigir la solicitud de impresión a una impresora en buen estado. Para obtener más información sobre las comprobaciones de estado exhaustivas de las flotas de impresoras, consulte la documentación de LRS que se incluye con la licencia del producto.

Imprimir autenticación y autorización

LRS/DIS permite a las aplicaciones de LRS autenticar los ID de usuario y las contraseñas mediante Microsoft Active Directory o un servidor LDAP. Además de la autorización básica de impresión, LRS/DIS también puede aplicar controles de seguridad de impresión detallados en los casos de uso siguientes:

- Gestione quién puede examinar el trabajo de impresión.
- Gestione el nivel de navegación de los trabajos de otros usuarios.
- Gestione las tareas operativas. Por ejemplo, la seguridad en el nivel de comandos, como retener o liberar, purgar, modificar, copiar y redirigir. La seguridad se puede configurar mediante el ID de usuario o el grupo, (similar a un grupo AD o a un grupo LDAP).

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Modernizar las cargas de trabajo de impresión en línea de mainframe en AWS mediante Micro Focus Enterprise Server y LRS VPSX/MFI

Creado por Shubham Roy (AWS), Abraham Rondon (Micro Focus), Guy Tucker (Levi, Ray and Shoup Inc) y Kevin Yung (AWS)

Entorno: PoC o piloto	Origen: Mainframe	Destino: AWS
Tipo R: redefinir la plataforma	Carga de trabajo: IBM	Tecnologías: mainframe; migración; modernización
Servicios de AWS: Microsoft AD gestionado por AWS; Amazon EC2; Amazon RDS; Amazon EBS		

Resumen

Este patrón le muestra cómo modernizar sus cargas de trabajo de impresión en línea de mainframe vitales para su empresa en la nube de Amazon Web Services (AWS) mediante el uso de Micro Focus Enterprise Server como tiempo de ejecución para una aplicación de mainframe modernizada y LRS VPSX/MFI (Interfaz Micro Focus) como servidor de impresión. El patrón se basa en el enfoque de modernización del mainframe a través de redefinir la plataforma. Con este enfoque, se migra la aplicación en línea de mainframe a Amazon Elastic Compute Cloud (Amazon EC2) y se migra la base de datos de mainframe, como IBM DB2 para z/OS, a Amazon Relational Database Service (Amazon RDS). AWS Directory Service para Microsoft Active Directory, también conocido como AWS Managed Microsoft AD, se encarga de la autenticación y la autorización del flujo de trabajo de impresión modernizado. El servidor de información de directorio LRS (LRS/DIS) está integrado con AWS Managed Microsoft AD para autenticar y autorizar el flujo de trabajo de impresión. Al modernizar sus cargas de trabajo de impresión en línea, puede reducir los costos de infraestructura de TI, mitigar la carga técnica que supone el mantenimiento de los sistemas heredados, eliminar los silos de datos, aumentar la agilidad y la eficiencia con un DevOps modelo y aprovechar los recursos bajo demanda y la automatización en la nube de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una carga de trabajo de impresión en línea o administración de producción de mainframe
- Conocimientos básicos sobre cómo recompilar y entregar una aplicación de mainframe ejecutada en Micro Focus Enterprise Server (para obtener más información, consulte la hoja de datos de Enterprise Server en la documentación de Micro Focus).
- Conocimientos básicos de las soluciones y conceptos de impresión en la nube de LRS (para obtener más información, consulte Modernización de la producción en la documentación de LRS).
- Software y licencia de Micro Focus Enterprise Server (para obtener más información, póngase en contacto con el departamento de ventas de Micro Focus).
- Software y licencias de LRS VPSX/MFI, LRS/Queue y LRS/DIS (para obtener más información, póngase en contacto con el departamento de ventas de LRS).

Nota: Para obtener más información sobre las consideraciones de configuración de las cargas de trabajo de impresión en línea de mainframe, consulte Consideraciones en la sección de Información adicional de este patrón.

Versiones de producto

- Micro Focus Enterprise Server 8.0 o posterior
- LRS VPSX/MFI V1R3 o posterior

Arquitectura

Pila de tecnología de origen

- Sistema operativo: IBM z/OS
- Lenguaje de programación – Common Business-Oriented Language (COBOL), y Customer Information Control System (CICS)
- Base de datos – IBM DB2 para z/OS, Sistema de Gestión de la Información de IBM (IMS) y Método de acceso al almacenamiento virtual (VSAM).
- Seguridad: Resource Access Control Facility (RACF), CA Top Secret para z/OS y Access Control Facility 2 (ACF2)

- Gestión de impresión y producción – Productos de impresión z/OS para mainframe de IBM (IBM Infoprint Server para z/OS, LRS y CA View)

Pila de tecnología de destino

- Sistema operativo – Microsoft Windows Server que se ejecuta en Amazon EC2
- Procesamiento: Amazon EC2
- Lenguaje de programación – COBOL y CICS
- Bases de datos: Amazon RDS
- Seguridad: AWS Managed Microsoft AD
- Administración de impresión y producción: solución de impresión LRS en AWS
- Entorno de tiempo de ejecución de mainframe – Micro Focus Enterprise Server

Arquitectura de origen

El siguiente diagrama muestra una arquitectura de estado actual típica para una carga de trabajo de impresión en línea de un mainframe.

El diagrama muestra el siguiente flujo de trabajo:

1. Los usuarios llevan a cabo transacciones comerciales en un sistema de participación (SoE) que se basa en una aplicación CICS de IBM escrita en COBOL.
2. El SoE invoca el servicio de mainframe, que registra los datos de las transacciones comerciales en una base de datos system-of-records (SoR), como IBM DB2 for z/OS.
3. El SoR conserva los datos comerciales del SoE.
4. Un usuario inicia una solicitud para generar un resultado de impresión desde el CICS SoE, que inicia una solicitud de transacción de impresión para procesar la solicitud de impresión.
5. La aplicación de transacciones de impresión (como un programa CICS y COBOL) extrae los datos de la base de datos, los formatea de acuerdo con los requisitos empresariales y genera resultados empresariales (datos impresos), como extractos de facturación, tarjetas de identidad o extractos de préstamos. A continuación, la aplicación envía una solicitud de impresión mediante el método de acceso virtual a las telecomunicaciones (VTAM). Un servidor de impresión z/OS (como IBM Infoprint Server) utiliza NetSpool o un componente VTAM similar para interceptar las solicitudes

de impresión y, a continuación, crea conjuntos de datos de salida de impresión en la bobina de JES mediante los parámetros de salida de JES. Los parámetros de salida del JES especifican la información de enrutamiento que el servidor de impresión utiliza para transmitir la salida a una impresora de red determinada. El término VTAM se refiere al servidor de comunicaciones z/OS y al elemento de servicios de la arquitectura de red del sistema (SNA) de z/OS.

6. El componente de transmisión de la producción de impresión transmite los conjuntos de datos de impresión de salida desde la bobina JES a impresoras o servidores de impresión remotos, como LRS (como se demuestra en este patrón), IBM Infoprint Server o destinos de correo electrónico.

Arquitectura de destino

El siguiente diagrama muestra una arquitectura para una carga de trabajo de impresión en línea de mainframe que se implementa en la nube de AWS:

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un usuario inicia una solicitud de impresión desde una interfaz de usuario en línea (CICS) para crear la producción de impresión, como extractos de facturación, tarjetas de identificación o extractos de préstamos.
2. La aplicación en línea del mainframe (plataforma redefinida para Amazon EC2) utiliza el tiempo de ejecución de Micro Focus Enterprise Server para extraer datos de la base de datos de la aplicación, aplicar lógica empresarial a los datos, formatear los datos y, a continuación, enviarlos a un destino de impresión mediante Micro Focus CICS Print Exit (DFHUPRNT).
3. La base de datos de la aplicación (un SoR que se ejecuta en Amazon RDS) conserva los datos para su impresión.
4. La solución de impresión LRS VPSX/MFI se implementa en Amazon EC2 y sus datos operativos se almacenan en Amazon Elastic Block Store (Amazon EBS). LRS VPSX/MFI utiliza un agente de transmisión LRS/Queue basado en TCP/IP para recopilar los datos de impresión a través de la API Print Exit (DFHUPRNT) de Micro Focus CICS y entregar los datos a un destino de impresión específico. El TERMID (TERM) original que se utiliza en la aplicación CICS modernizada se utiliza como nombre de la cola de VPSX/MFI.

Nota: La solución de destino no suele requerir cambios en la aplicación para adaptarla a los lenguajes de formato de mainframe, como IBM Advanced Function Presentation (AFP) o Xerox Line Condition Data Stream (LCDS). Para obtener más información sobre el uso de Micro Focus para la

migración y modernización de aplicaciones de mainframe en AWS, consulte Potenciar las cargas de trabajo de mainframe empresarial en AWS con Micro Focus en la documentación de AWS.

Arquitectura de infraestructura de AWS

El siguiente diagrama muestra una arquitectura de infraestructura de AWS segura y de alta disponibilidad para una carga de trabajo de impresión en línea de mainframe:

En el diagrama, se muestra el siguiente flujo de trabajo:

1. La aplicación en línea para mainframe (escrita en un lenguaje de programación como CICS o COBOL) utiliza la lógica empresarial básica para procesar y generar la producción de impresión, como extractos de facturación, tarjetas de identidad y extractos de préstamos. La aplicación en línea se implementa en Amazon EC2 en dos Zonas de disponibilidad (AZ) para una alta disponibilidad (HA) y utiliza Micro Focus CICS Print Exit para enrutar la producción de impresión a LRS VPSX/MFI para que los impriman los usuarios finales.
2. El LRS VPSX/MFI utiliza un agente de transmisión LRS/Queue basado en TCP/IP para recopilar o capturar los datos de impresión desde la interfaz de programación Print Exit en línea de Micro Focus. Online Print Exit transmite la información necesaria para que LRS VPSX/MFI procese eficazmente el archivo de impresión y cree comandos LRS/Queue de forma dinámica.

   Nota: Para obtener más información sobre los distintos métodos de programación de aplicaciones CICS para la impresión y sobre su compatibilidad con el servidor Micro Focus Enterprise y LRS VPSX/MFI, consulte Captura de datos de impresión en la sección de Información adicional de este patrón.
3. Un Equilibrador de carga de red proporciona un nombre DNS para integrar Micro Focus Enterprise Server con LRS VPSX/MFI. Nota: LRS VPSX/MFI admite un equilibrador de carga de capa 4. El equilibrador de carga de red también realiza una comprobación básica del estado de VPSX/MFI de LRS y enruta el tráfico a los destinos registrados cuyo estado es correcto.
4. El servidor de impresión LRS VPSX/MFI se implementa en Amazon EC2 en dos zonas de disponibilidad, para lograr una alta disponibilidad, y emplea Amazon EBS como almacén de datos operativos. LRS VPSX/MFI admite los modos de servicio tanto activo-activo como activo-pasivo. Esta arquitectura utiliza varias zonas de disponibilidad en un par activo-pasivo como activo y modo de espera activa. El equilibrador de carga de red realiza una comprobación de estado de las instancias EC2 de LRS VPSX/MFI y enruta el tráfico a las instancias en espera activas de otra zona de disponibilidad si una instancia activa se encuentra en mal estado. Las solicitudes

de impresión se mantienen en la cola de trabajos del LRS de forma local en cada una de las instancias de EC2. En caso de recuperación, se debe reiniciar una instancia fallida para que los servicios de LRS reanuden el procesamiento de la solicitud de impresión.

Nota: El LRS VPSX/MFI también puede realizar comprobaciones de estado a nivel de flota de impresoras. Para obtener más información, consulte Comprobaciones de estado de la flota de impresoras en la sección de Información adicional de este patrón.

5. AWS Managed Microsoft AD se integra con LRS/DIS para llevar a cabo la autenticación y autorización del flujo de trabajo de impresión. Para obtener más información, consulte Autenticación y autorización de impresión en la sección de Información adicional de este patrón.
6. LRS VPSX/MFI emplea Amazon EBS para el almacenamiento en bloques. Puede hacer copias de seguridad de los datos de Amazon EBS de las instancias EC2 activas en Amazon S3 como point-in-time instantáneas y restaurarlos en volúmenes de EBS activos en espera. Para automatizar la creación, retención y eliminación de instantáneas de volúmenes de Amazon EBS, puede usar Amazon Data Lifecycle Manager para establecer la frecuencia de las instantáneas automatizadas y restaurarlas en función de sus necesidades de RTO/RPO.

Herramientas

Servicios de AWS

- Amazon Elastic Block Store (Amazon EBS) proporciona volúmenes de almacenamiento de nivel de bloque para su uso con instancias de Amazon EC2. Los volúmenes de EBS se comportan como dispositivos de bloques sin formatear. Puede montar estos volúmenes como dispositivos en sus instancias.
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon Relational Database Service (Amazon RDS) le ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS.
- AWS Directory Service para Microsoft Active Directory (AD), también conocido como AWS Managed Microsoft Active Directory, permite que sus cargas de trabajo compatibles con directorios y los recursos de AWS utilicen Active Directory administrado en AWS.

Otras herramientas

- LRS VPSX/MFI (Micro Focus Interface), una interfaz desarrollada conjuntamente por LRS y Micro Focus, captura la producción de una bobina JES de Micro Focus Enterprise Server y la entrega de forma fiable a un destino de impresión específico.
- El servidor de información de directorio LRS (LRS/DIS) se utiliza para la autenticación y la autorización durante el flujo de trabajo de impresión.
- El LRS/Queue es un agente de transmisión LRS/Queue basado en TCP/IP que utiliza LRS VPSX/MFI para recopilar o capturar datos de impresión a través de la interfaz de programación Print Exit en línea de Micro Focus.
- Micro Focus Enterprise Server es un entorno de implementación de aplicaciones para aplicaciones de mainframe. Proporciona el entorno de ejecución para las aplicaciones de mainframe que se migran o crean con cualquier versión de Micro Focus Enterprise Developer.

Epics

Configurar Micro Focus Enterprise Server en Amazon EC2 e implementar una aplicación en línea para mainframe

Tarea	Descripción	Habilidades requeridas
Configure Micro Focus Enterprise Server e implemente una aplicación en línea de demostración.	Configure Micro Focus Enterprise Server en Amazon EC2 y, a continuación, implemente la aplicación Micro Focus Account Demo (ACCT Demo) en Amazon EC2 siguiendo las instrucciones del Tutorial: soporte de CICS de la documentación de Micro Focus. La aplicación ACCT Demo es una aplicación en línea para mainframe (CICS) que crea y, a continuación, inicia la producción de impresión.	Arquitecto de la nube

Configurar un servidor de impresión LRS en Amazon EC2

Tarea	Descripción	Habilidades requeridas
Obtenga una licencia de producto LRS para imprimir.	Para obtener una licencia de producto LRS para LRS VPSX/MFI, LRS/Queue y LRS/DIS, póngase en contacto con el Equipo de gestión de producción de LRS. Debe proporcionar los nombres de host de las instancias EC2 en las que se instalarán los productos LRS.	Responsable de compilación
Cree una instancia de Windows en Amazon EC2 para instalar LRS VPSX/MFI.	Lance una instancia de Amazon EC2 para Windows siguiendo las instrucciones del Paso 1: Lanzar una instancia de la documentación de Amazon EC2. La instancia debe cumplir los siguiente s requisitos de hardware y software para LRS VPSX/MFI: • CPU: doble núcleo • RAM: 16 GB • Unidad: 500 GB • Instancia EC2 mínima: m5.xlarge • Sistema operativo: Windows/Linux • Software: Servicio de Información de Internet (IIS) o Apache	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	Nota: Los requisitos de hardware y software anteriores están pensados para una flota de impresoras pequeña (alrededor de 500 a 1000). Para conocer todos los requisitos, consulte a sus personas de contacto en LRS y AWS. Cuando cree la instancia de Windows, haga lo siguiente: 1. Confirme que el nombre de host de EC2 es el mismo nombre de host utilizado para la licencia del producto LRS. 2. Para habilitar CGI en Amazon EC2, siga estos pasos: a. Conéctese a la instancia EC2 siguiendo las instrucciones del Paso 2: Conéctese a su instancia en la documentación de Amazon EC2. b. En el menú Inicio de Windows, busque y abra Server Manager. c. En el panel de Server Manager, elija Panel de control, Inicio rápido, Agregar roles y características. A continuación,	

Tarea	Descripción	Habilidades requeridas
	seleccione Roles de servidor. d. En Funciones de servidor, elija WebServer (IIS) y, a continuación, Desarrollo de aplicaciones. e. En Desarrollo de aplicaciones, seleccione la casilla CGI. f. Siga las instrucciones del asistente para Agregar roles y características de Windows Server Manager para instalar CGI. g. Abra el puerto 5500 en el firewall de Windows de la instancia EC2 para la comunicación entre LRS/Queue.	

Tarea	Descripción	Habilidades requeridas
Instale LRS VPSX/MFI en la instancia EC2.	1. Conéctese a la instancia EC2 siguiendo las instrucciones del Paso 2: Conéctese a su instancia en la documentación de Amazon EC2. 2. Abra el enlace a la página de descarga del producto que se incluye en el correo electrónico de LRS que debería haber recibido. Nota: Los productos de LRS se distribuyen mediante transferencia de archivos electrónica (EFT). 3. Descargue LRS VPSX/MFI y descomprima el archivo (carpeta predeterminada: `c:\LRS`). 4. Inicie el instalador de productos LRS desde la carpeta descomprimida para instalar LRS VPSX/MFI. 5. En el menú Seleccionar características, seleccione VPSX® Server (V1R3.022) y, a continuación, seleccione Siguiente para iniciar el proceso de instalación. Cuando se complete la instalación, recibirá un mensaje de confirmación.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Instale LRS/Queue.	1. Conéctese a su instancia EC2 de Micro Focus Enterprise Server siguiendo las instrucciones del Paso 2: Conéctese a su instancia en la documentación de Amazon EC2. 2. Abra el enlace a la página de descarga del producto LRS desde el correo electrónico de LRS que debería recibir, descargue LRS/Queue y, a continuación, descomprima el archivo. 3. Vaya a la ubicación en la que descargó los archivos y, a continuación, inicie el instalador del producto LRS para instalar LRS/Queue.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Instale LRS/DIS.	1. Conéctese a la instancia EC2 de LRS VPSX/MFI siguiendo las instrucciones del Paso 2: Conéctese a su instancia en la documentación de Amazon EC2. 2. Abra el enlace a la página de descarga del producto LRS que se incluye en el correo electrónico de LRS que habrá recibido, descargue LRS/DIS y, a continuación, descomprima el archivo. 3. Vaya a la ubicación en la que descargó los archivos y, a continuación, inicie el instalador de producto de LRS. 4. En el instalador de producto de LRS, amplíe LRS Misc Tools, seleccione LRS DIS y, a continuación, Siguiente. 5. Siga el resto de las instrucciones del instalador del producto de LRS para completar el proceso de instalación.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Cree un grupo de destino y registre LRS VPSX/MFI EC2 como destino.	Cree un grupo de destino siguiendo las instrucciones de Crear un grupo de destino para el equilibrador de carga de red en la documentación en el equilibrador de carga de red elástico. Al crear el grupo de destino, haga lo siguiente: 1. En la página Especific ar detalles del grupo, seleccione un Tipo de destino y luego, Instancias. 2. En Protocol, seleccione TCP. 3. En Puerto, seleccione 5500. 4. En la página Register targets (Registrar destinos), busque la sección Available instances (Instancias disponibles) y seleccione la instancia EC2 de LRS VPSX/MFI.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Crear un equilibrador de carga de red.	Siga las instrucciones de Crear un equilibrador de carga de red en la documentación de Elastic Load Balancing. Su equilibrador de carga de red dirige el tráfico desde Micro Focus Enterprise Server a la instancia EC2 de LRS VPSX/MFI. Al crear el equilibrador de carga de red, siga los pasos siguientes en la página Listeners and Routing (Oyentes y enrutamiento): 1. En Protocol, seleccione TCP. 2. En Puerto, seleccione 5500. 3. En Default action (Acción predeterminada), seleccione Forward to (Reenviar a) para el grupo de destino que ha creado.	Arquitecto de la nube

Integrar Micro Focus Enterprise Server con LRS VPSX/MFI y LRS/Queue

Tarea	Descripción	Habilidades requeridas
Configure Micro Focus Enterprise Server para la integración de LRS/Queue.	1. Conéctese a la instancia EC2 de Micro Focus Enterprise Server siguiendo las instrucciones del Paso 2: Conéctese a su instancia	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	en la documentación de Amazon EC2. 2. En el menú Start (Inicio) de Windows, abra la interfaz de usuario de administración de Micro Focus Enterprise Server. 3. En la barra de menús, seleccione NATIVE. 4. En el panel de navegación, seleccione Directory Server y, a continuación, BANKDEMO o su región de Enterprise Server. 5. En General en el panel de navegación izquierdo, despláce hacia abajo hasta la sección Adicional para configurar las variables de entorno (LRSQ_ADDRESS, LRSQ_PORT, LRSQ_COMMAND) para que dirijan hacia LRSQ. 6. Para LRSQ_ADDRESS, escriba la dirección IP o el nombre DNS del equilibrador de carga de red que creó anteriormente. 7. Para LRSQ_PORT, especifique VPSX LRSQ Listener Port (5500).	

Tarea	Descripción	Habilidades requeridas
	8. Para LRSQ_COMMAND, especifique la ubicación de la ruta del ejecutable de LRSQ. 9. Nota: Actualmente, LRS admite un límite máximo de 50 caracteres para los nombres de DNS, pero este aspecto cambiará en el futuro. Si el nombre DNS tiene más de 50 caracteres, puede utilizar la dirección IP del equilibrador de carga de red como alternativa.	

Tarea	Descripción	Habilidades requeridas
Haga que CICS Print Exit (DFHUPRNT) esté disponible para la inicialización de Micro Focus Enterprise Server.	1. Conéctese a su instancia EC2 de Micro Focus Enterprise Server siguiendo las instrucciones del Paso 2: Conéctese a su instancia en la documentación de Amazon EC2. 2. Copie CICS Print Exit (DFHUPRNT) de la carpeta ejecutable de LRS VPSX/MFI (denominada `VPSX_MFI_R2`) a la ubicación de la instancia EC2 de Micro Focus Enterprise Server. Para los sistemas de 32 bits, la ubicación es `C:\Program Files (x86) \Micro Focus\Enterprise Server\bin` . Para los sistemas de 64 bits, la ubicación es `C:\Program Files (x86) \Micro Focus\Enterprise Server\bin64` . Nota: Se debe cambiar el nombre del archivo `DFHUPRNT_64.dll` a `DFHUPRNT.dll` al copiarlo. Comprobar que Micro Focus Enterprise Server haya detectado CICS Print Exit (DFHUPRNT)	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	1. Detenga e inicie Micro Focus Enterprise Server. 2. En el panel de administración de Micro Focus Enterprise Server, abra Supervisar, Registros, Registros de consola. 3. Compruebe los registros de la consola para ver el siguiente mensaje: “El usuario de la impresora 3270 salió correctamente de DFHUPRNT y se instaló correctamente”.	

Tarea	Descripción	Habilidades requeridas
Defina el ID de terminal de la impresora CICS (TermIDS) como Micro Focus Enterprise Server.	Habilitar la impresión 3270 en Micro Focus Enterprise Server 1. En el panel de administración de Micro Focus Enterprise Server, abra CICS, Recuros, Por grupo. 2. En el panel de navegación izquierdo, seleccione SIT (tabla de inicialización del sistema) y, a continuación, seleccione BNKCICV. 3. En la sección General, desplácese hacia abajo hasta 3270 y, a continuación, seleccione la casilla Imprimir 3270. Defina el terminal de la impresora CICS en Micro Focus Enterprise Server 1. En el panel de administración de Micro Focus Enterprise Server, abra CICS, Recursos, Por tipo. 2. En el panel de navegación izquierdo, seleccione Término y, a continuación, Nuevo. Se abre el formulario Crear recurso de terminal. 3. En Nombre, introduzca el nombre de la cola de impresión del LRS. (Nota:	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	Este patrón utiliza "P275" como ID de terminal de la impresora CICS y la cola de impresión LRS VPSX). 4. Para Grupo, introduzca BANKTERM. 5. Para Instalación automátic a: Modelo, introduzca NO. 6. En Identificadores de terminal: Tipo de terminal, introduzca DFHPRT32. 7. En Nombre de red, introduzca VTAMP275. 8. Para el Uso del terminal, seleccione la casilla En servicio. 9. Desplácese hasta la parte superior de la página y, a continuación, seleccione Guardar. 10. Elija Instalar. Se muestra un mensaje emergente que indica que la instalación se ha realizado correctamente.	

Configure impresoras y usuarios de impresión en Micro Focus Enterprise Server y LRS VPSX/MFI

Tarea	Descripción	Habilidades requeridas
Cree una cola de impresión en LRS VPSX.	1. Conéctese a su instancia EC2 de LRS VPSX/MFI siguiendo las instrucciones del Paso 2: Conéctese a su	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	instancia en la documentación de Amazon EC2. 2. Abra la interfaz web de VPSX desde el menú Inicio de Windows. 3. En el panel de navegación, seleccione Impresoras. 4. Seleccione Agregar y, a continuación, Agregar impresora. 5. En la página de Configuración de la impresora, en Nombre de impresora, introduzca P275. 6. Para VPSX ID, introduzca VPS1. 7. Para CommType, seleccione TCPIP/LRSQ. 8. En Host/Dirección IP, introduzca la dirección IP de la impresora física que desee agregar. 9. En Dispositivo, introduzca el nombre de su dispositivo. 10. Seleccione Controlador de Windows o Controlador de Linux/Mac. 11. Elija Añadir. Nota: La cola de impresión debe ser equivalente a los TERMID de impresión creados	

Tarea	Descripción	Habilidades requeridas
	en Micro Focus Enterprise Server.	

Tarea	Descripción	Habilidades requeridas
Cree un usuario de impresión en LRS VPSX/MFI.	1. Conéctese a su instancia EC2 de LRS VPSX/MFI siguiendo las instrucciones del Paso 2: Conéctese a su instancia en la documentación de Amazon EC2. 2. Abra la interfaz web de VPSX desde el menú Inicio de Windows. 3. En el panel de navegación, elija Seguridad y luego elija la opción Usuarios. 4. En la columna Nombre de usuario, seleccione admin y, a continuación, seleccione Copiar. 5. En la ventana Mantenimiento del perfil de usuario, en Nombre de usuario, introduzca un nombre de usuario (por ejemplo,). PrintUser 6. En Descripción, escriba una descripción breve (por ejemplo, Usuario para impresión de prueba). 7. Seleccione Update (Actualizar). Esto crea un usuario de impresión (por ejemplo, PrintUser). 8. En el panel de navegación, en Usuario, seleccion	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	e el nuevo usuario que ha creado. 9. En el menú Comandos, seleccione Seguridad. 10. En la página Reglas de seguridad, seleccione todas las opciones de seguridad de la impresora y seguridad laboral aplicables y, a continuación, seleccione Guardar. 11. Para añadir el nuevo usuario de impresión al grupo Administrador, vaya al panel de navegación, seleccione Seguridad y, a continuación, seleccione Configurar. 12. En la ventana Configuración de seguridad, añada su nuevo usuario de impresión a la columna Administrador.	

Configure imprimir autenticación y autorización

Tarea	Descripción	Habilidades requeridas
Cree un dominio de AWS Managed Microsoft AD con usuarios y grupos.	1. Para crear un directorio Active en AWS Managed Microsoft AD, siga las instrucciones de ree su directorio de AWS	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	Managed Microsoft AD en la documentación de AWS Directory Service. 2. Implemente una instancia EC2 (administrador de Active Directory) e instale las herramientas de Active Directory para administrar su AD de Microsoft administrado por AWS siguiendo las instrucciones del Paso 3: Implementar una instancia EC2 para administrar su AD de Microsoft administrado por AWS en la documentación de AWS Directory Service. 3. Conéctese a la instancia EC2 siguiendo las instrucciones del Paso 2: Conéctese a su instancia en la documentación de Amazon EC2. Nota: Cuando se conecte a la instancia EC2, introduzca sus credenciales de administrador (para el directorio que creó en el primer paso) en la ventana de seguridad de Windows. 4. En el menú Inicio de Windows, bajo Herramientas administrativas de Windows, seleccione	

Tarea	Descripción	Habilidades requeridas
	Usuarios y equipos de Active Directory. 5. Cree un usuario de impresión en el dominio de Active Directory siguiendo los pasos de Crear un usuario de la documentación de AWS Directory Service.	
Una LRS VPSX/MFI EC2 a un dominio de AWS Managed Microsoft AD.	Una LRS VPSX/MFI EC2 a su dominio de AWS Managed Microsoft AD de forma automática (documentación del Centro de conocimientos de AWS) o manualmente (documentación de AWS Directory Service).	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Configure e integre LRS/DIS con AWS Managed Microsoft AD.	1. Conéctese a su instancia EC2 de LRS VPSX/MFI siguiendo las instrucciones del Paso 2: Conéctese a su instancia en la documentación de Amazon EC2. 2. En el menú Inicio de Windows , abra la Interfaz web de VPSX. 3. En el panel de navegación, seleccione Seguridad y, a continuación, la opción Configurar. 4. En la página Security Configuration, busque la sección Security Parameters y, en Security Type, seleccione Internal. 5. Especifique sus preferencias para el resto de las opciones en la sección Parámetros de seguridad. 6. En el menú Start (Inicio) de Windows, abra la carpeta LRS Output Management, seleccione Server Start y, a continuación, Server Stop. 7. Inicie sesión en LRS VPSX/MFI con su nombre de usuario y contraseña de Active Directory.	Arquitecto de la nube

Probar un flujo de trabajo de impresión en línea

Tarea	Descripción	Habilidades requeridas
Inicie una solicitud de impresión en línea desde la aplicación Micro Focus ACCT Demo.	1. Abra el emulador de terminal TN3270 en su instancia EC2 de Micro Focus Enterprise Server. (Nota: Este patrón utiliza emuladores de terminal 3270). 2. Conéctese al emulador de terminal TN3270 (Rumba). Para la Dirección del nombre de host, utilice 127.0.0.1. Para el Puerto Telnet, utilice 9270. 3. Tras conectarse a la pantalla 3270, presione CTL+SHIFT+Z para borrar la pantalla. 4. Para iniciar la aplicació n ACCT Demo, en una pantalla transparente, introduzca ACCT. Esto abre la pantalla principal de la aplicación ACCT Demo online (CICS). Nota: La pantalla principal incluye opciones de menú como el Archivo de cuenta, Para buscar por nombre, introducir, Tipo de solicitud, Cuenta e Impresora. 5. Para enviar una solicitud de impresión desde la	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	aplicación ACCT Demo Online (CICS), introduzc a P en el campo tipo de solicitud, 11111 en el campo cuenta y P275 en el campo impresora. Asegúrese de establece r el valor del campo de la impresora en el valor del ID de terminal de la impresora CICS. 6. Pulse Intro. El mensaje “Solicitud de impresión programada” se muestra en la parte inferior de la pantalla. Esto confirma que se generó una solicitud de impresión en línea desde la aplicación ACCT Demo y se envió a LRS VPS/MFI para su procesamiento de impresión.	

Tarea	Descripción	Habilidades requeridas
Compruebe la producción de impresión en LRS VPSX/MFI.	1. Conéctese a su instancia EC2 de LRS VPSX/MFI siguiendo las instrucciones del Paso 2: Conéctese a su instancia en la documentación de Amazon EC2. 2. En el menú Inicio de Windows, abra la Interfaz web de VPSX. 3. En el panel de navegación, seleccione Impresoras y, a continuación, seleccione Cola de producción. Busque la cola de impresión P275 que creó anteriormente para la impresión en línea. 4. Para la cola de impresión (P275), en la columna ID de bobina, seleccione el ID de bobina para la solicitud de la cola de impresoras. 5. En la pestaña Acciones, en la columna COMANDO, seleccione Examinar. Ahora puede ver el resultado de impresión de un extracto de cuenta con columnas para el número de cuenta, el apellido, el nombre, la dirección, el teléfono, el número de tarjetas emitidas, la	Ingeniero de pruebas

Tarea	Descripción	Habilidades requeridas
	fecha de emisión, el importe y el saldo. Para ver un ejemplo, consulte el archivo adjunto online_print_output para ver este patrón.	

Recursos relacionados

- Modernización de la producción de LRS (documentación de LRS)
- Conceptos de redes VTAM (documentación de IBM)
- Resumen de los tipos de unidades lógicas (LU) (documentación de IBM)
- Controles ANSI y de carro de máquinas (documentación de IBM)
- Capacitación de las cargas de trabajo de mainframe empresariales en AWS con Micro Focus (blog de AWS Partner Network)
- Compilación de un PAC de Micro Focus Enterprise Server con Amazon EC2 Auto Scaling y Systems Manager (documentación de Recomendaciones de AWS)
- Flujo de datos de Presentación de funciones avanzadas (AFP) (documentación de IBM)
- Flujo de datos condicionado por línea (LCDS) (documentación de Compart)

Información adicional

Consideraciones

Durante su proceso de modernización, puede considerar una amplia variedad de configuraciones para los procesos en línea del mainframe y la producción que generan. Todos los clientes y proveedores que utilizan la plataforma de mainframe la han personalizado con requisitos particulares que afectan directamente a la impresión. Por ejemplo, su plataforma actual puede incorporar Advanced Function Presentation (AFP) de IBM o Line Condition Data Stream (LCDS) de Xerox en el flujo de trabajo actual. Además, los caracteres de control de carro de mainframe y las palabras de comando de canal pueden afectar al aspecto de la página impresa y pueden requerir un tratamiento

especial. Como parte del proceso de planificación de la modernización, le recomendamos evaluar y comprender las configuraciones de su entorno de impresión específico.

Captura de datos de impresión

En esta sección se resumen los métodos de programación de aplicaciones CICS que puede utilizar en un entorno de mainframe de IBM para la impresión. Los componentes VPSX/MFI de LRS proporcionan técnicas que permiten a los mismos programas de aplicación crear datos de la misma manera. En la siguiente tabla se describe cómo se admite cada método de programación de aplicaciones en una aplicación CICS modernizada que se ejecuta en AWS y Micro Focus Enterprise Server con un servidor de impresión LRS VPSX/MFI.

Método	Descripción	Soporte para el método en un entorno modernizado
EXEC CICS SEND TEXT.. or EXEC CICS SEND MAP..	Estos métodos CICS y VTAM son responsables de crear y entregar flujos de datos de impresión 3270/SCS a los dispositivos de impresión LUTYPE0, LUTYPE1 y LUTYPE3.	La interfaz de programación de aplicaciones (API) de programación Print Exit en línea de Micro Focus (DFHUPRNT) permite procesar los datos de impresión mediante VPSX/MFI cuando se crean flujos de datos de impresión 3270/SCS mediante cualquiera de estos métodos.
EXEC CICS SEND TEXT.. or EXEC CICS SEND MAP.. (con software de mainframe de IBM de terceros)	Los métodos CICS y VTAM se encargan de crear y entregar los flujos de datos de impresión 3270/SCS a los dispositivos de impresión LUTYPE0, LUTYPE1 y LUTYPE3. Los productos de software de terceros interceptan los datos de impresión, los convierten en datos de formato de impresión estándar	La API de programación Print Exit en línea de Micro Focus (DFHUPRNT) permite procesar los datos de impresión mediante VPSX/MFI cuando se crean flujos de datos de impresión 3270/SCS mediante cualquiera de estos métodos.

	con un carácter de control ASA/MCH y colocan los datos en la bobina JES para que los procesen sistemas de impresión basados en mainframe que utilizan JES.	
EXEC CICS SPOOLOPEN	Los programas de aplicación CICS utilizan este método para escribir datos directamente en la bobina JES. A continuación, los datos están disponibles para ser procesados por sistemas de impresión basados en mainframe que utilizan JES.	Micro Focus Enterprise Server envía los datos a la bobina de Enterprise Server, donde los puede procesar el VPSX/MFI Batch Print Exit (LRSPRTE6), que envía los datos a VPSX.
DRS/API	Se utiliza una interfaz de programación proporcionada por LRS para escribir los datos de impresión en JES.	VPSX/MFI proporciona una interfaz de reemplazo que envía los datos de impresión directamente al VPSX.

Comprobación de estado de la flota de impresoras

LRS VPSX/MFI (LRS LoadX) puede llevar a cabo comprobaciones de estado exhaustivas, incluida la gestión de los dispositivos y la optimización operativa. La administración de dispositivos puede detectar un error en un dispositivo de impresión y dirigir la solicitud de impresión a una impresora en buen estado. Para obtener más información sobre las comprobaciones de estado exhaustivas de las flotas de impresoras, consulte la documentación de LRS que se incluye con la licencia del producto.

Imprimir autenticación y autorización

LRS/DIS permite a las aplicaciones de LRS autenticar los ID de usuario y las contraseñas mediante Microsoft Active Directory o un servidor LDAP. Además de la autorización básica de impresión, LRS/DIS también puede aplicar controles de seguridad de impresión detallados en los casos de uso siguientes:

- Gestione quién puede examinar el trabajo de impresión.

- Gestione el nivel de navegación de los trabajos de otros usuarios.
- Gestione las tareas operativas. Por ejemplo, la seguridad a nivel de comandos, como retener o liberar, purgar, modificar, copiar y redirigir. La seguridad se puede configurar mediante el ID de usuario o el grupo (similar al grupo AD o al grupo LDAP).

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Mover los archivos de mainframe directamente a Amazon S3 mediante Transfer Family

Creado por Luis Gustavo Dantas (AWS)

Entorno: Producción	Origen: Mainframe	Destino: Amazon S3
Tipo R: N/D	Carga de trabajo: IBM	Tecnologías: Mainframe; almacenamiento y copia de seguridad; modernización
Servicios de AWS: AWS Transfer Family; Amazon S3		

Resumen

Como parte del proceso de modernización, puede afrontar el desafío de transferir archivos entre sus servidores en las instalaciones y la nube de Amazon Web Services (AWS). La transferencia de datos desde mainframes puede suponer un desafío importante, ya que los mainframes normalmente no pueden acceder a los almacenes de datos modernos como Amazon Simple Storage Service (Amazon S3), Amazon Elastic Block Store (Amazon EBS) o Amazon Elastic File System (Amazon EFS).

Muchos clientes utilizan recursos de almacenamiento provisional intermedios, como servidores Linux, Unix o Windows en las instalaciones, para transferir archivos a la nube de AWS. Puede evitar este método indirecto si utiliza AWS Transfer Family con el protocolo de File Transfer (SFTP) de Secure Shell (SSH) para cargar archivos de mainframe directamente a Amazon S3.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una nube privada virtual (VPC) con una subred a la que pueda acceder la plataforma antigua
- Un punto de conexión de Transfer Family para su VPC

- Archivos del método de acceso al almacenamiento virtual (VSAM) de mainframe convertidos en archivos de longitud fija secuenciales (documentación de IBM)

Limitaciones

- SFTP transfiere los archivos en modo binario de forma predeterminada, lo que significa que los archivos se cargan en Amazon S3 conservando la codificación EBCDIC. Si el archivo no contiene datos binarios o empaquetados, puede utilizar el sftp ascii subcommand (documentación de IBM) para convertir los archivos en texto durante la transferencia.
- Debe desempaquetar los archivos de mainframe (Recomendaciones de AWS) que contengan contenido empaquetado y binario para poder utilizar estos archivos en el entorno de destino.
- El tamaño de los objetos de Amazon S3 puede oscilar entre un mínimo de 0 bytes y un máximo de 5 TB. Para obtener más información acerca de las capacidades de Amazon S3, consulte Preguntas frecuentes de Amazon S3.

Arquitectura

Pila de tecnología de origen

- Lenguaje de control de tareas (JCL)
- Intérprete de comandos e ISPF para z/OS Unix
- SFTP
- VSAM y archivos planos

Pila de tecnología de destino

- Transfer Family
- Amazon S3
- Amazon Virtual Private Cloud (Amazon VPC)

Arquitectura de destino

El diagrama siguiente muestra una arquitectura de referencia para usar Transfer Family con SFTP para cargar archivos de mainframe directamente a un bucket de S3.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Se utiliza un trabajo de JCL para transferir los archivos de mainframe del mainframe heredado a la nube de AWS a través de Direct Connect.
2. Direct Connect permite que el tráfico de la red permanezca en la red global de AWS y evite la Internet pública. Direct Connect también mejora la velocidad de la red, empezando en 50 Mbps y escalando verticalmente hasta 100 Gbps.
3. El punto de conexión de VPC permite las conexiones entre los recursos de la VPC y los servicios compatibles sin utilizar la Internet pública. El acceso a Transfer Family y Amazon S3 logra una alta disponibilidad al realizarse a través de las interfaces de red elásticas ubicadas en dos subredes privadas y zonas de disponibilidad.
4. Transfer Family autentica a los usuarios y usa SFTP para recibir los archivos del entorno heredado y moverlos a un bucket de S3.

Automatizar y escalar

Una vez implementado el servicio Transfer Family, puede transferir un número ilimitado de archivos desde el mainframe a Amazon S3 utilizando un trabajo de JCL como cliente SFTP. También puede automatizar la transferencia de archivos mediante el uso de un programador de trabajos por lotes del mainframe para ejecutar los trabajos de SFTP cuando esté todo a punto para transferir los archivos del mainframe.

Herramientas

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esta red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.
- AWS Transfer Family le permite escalar de forma segura sus transferencias de business-to-business archivos recurrentes a Amazon S3 y Amazon EFS mediante los protocolos SFTP, FTPS y FTP.

Epics

Crear el bucket de S3 y la política de acceso

Tarea	Descripción	Habilidades requeridas
Cree el bucket de S3.	Cree un bucket de S3 para alojar los archivos que transfiera desde su entorno anterior.	AWS general
Cree una política y un rol de IAM.	Transfer Family utiliza el rol de AWS Identity and Access Management (IAM) para conceder acceso al bucket de S3 que se creó con anteriori dad. Cree un rol de IAM que incluya la siguiente política de IAM: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "UserFolderListing", "Action": [ "s3:ListBucket", "s3:GetBucketLocation" ], "Effect": "Allow", "Resource": [`	AWS general

Tarea	Descripción	Habilidades requeridas
	<pre>"arn:aws:s3:::<your-bucket-name>"] }, { "Sid": "HomeDirObjectAccess", "Effect": "Allow", "Action": ["s3:PutObject", "s3:GetObjectAcl", "s3:GetObject", "s3:DeleteObjectVersion", "s3:DeleteObject", "s3:PutObjectAcl", "s3:GetObjectVersion"], "Resource": "arn:aws:s3:::<your-bucket-name>/*" }] }</pre> Nota: Debe elegir el caso de uso de Transfer al crear el rol de IAM.	

Definir el servicio de transferencia

Tarea	Descripción	Habilidades requeridas
Cree el servidor SFTP.	1. Inicie sesión en la consola de administración de AWS, abra la consola Transfer Family y, a continuación, seleccione Create server (Crear servidor). 2. Seleccione únicamente SFTP (SSH File Transfer Protocol) - file transfer over Secure Shell protocol (SFTP [Protocolo de transferencia de archivos SSH]: transferencia de archivos a través del protocolo Secure Shell) y, a continuación, elija Next (Siguiente). 3. En Identity provider (Proveedor de identidad), seleccione Service managed (Administ rado por el servicio) y, a continuación, Next (Siguient e). 4. En Endpoint Type (Tipo de punto de conexión), seleccione VPC hosted (Alojado en VPC). 5. En Access (Acceso), seleccione Internal. 6. En VPC, elija su VPC.	AWS general

Tarea	Descripción	Habilidades requeridas
	7. En la sección Availability Zones (Zonas de disponibilidad), seleccione sus zonas de disponibilidad y subredes. 8. En la sección Security Groups (Grupos de seguridad), seleccione su grupo de seguridad y, a continuación, Next (Siguiente). 9. En Domain (Dominio, seleccione Amazon S3 y, a continuación, Next (Siguiente). 10. Deje las opciones predeterminadas en la página Configure additional details (Configurar detalles adicionales) y, a continuación, seleccione Next (Siguiente). 11. Seleccione Create server (Crear servidor). Nota: Para obtener más información sobre cómo configurar un servidor SFTP, consulte Create an SFTP-enabled server (Crear un servidor compatible con SFTP) (Guía del usuario de AWS Transfer Family).	

Tarea	Descripción	Habilidades requeridas
Obtenga la dirección del servidor.	1. Abra la consola de Transfer Family y seleccione el ID de servidor en la columna Server ID. 2. En la sección Endpoint details (Detalles del punto de conexión), en Endpoint type (Tipo de punto de conexión), seleccione el ID del punto de conexión. Esto dirige a la consola de Amazon VPC. 3. En la pestaña Details (Detalles) de la consola de Amazon VPC, busque los nombres DNS junto a DNS names.	AWS general
Cree el par de claves del cliente SFTP.	Cree un par de claves SSH para Microsoft Windows o macOS/Linux/UNIX.	AWS general, SSH

Tarea	Descripción	Habilidades requeridas
Cree el servidor SFTP.	1. Abra la consola de Transfer Family, seleccione Servers en el panel de navegación y, a continuación, seleccione su servidor. 2. En la columna Server ID, seleccione el ID de servidor para su servidor y, a continuación, Add user (Agregar usuario). 3. En Username (Nombre de usuario), escriba un nombre de usuario que coincida con el nombre de usuario del par de claves SSH. 4. En Role, seleccione el rol de IAM que creó anteriormente. 5. En Home directory (Directorio principal), seleccione el bucket de S3 que creó anteriormente. 6. En SSH public keys (Claves SSH públicas), escriba el par de claves que creó anteriormente. 7. Elija Añadir.	AWS general

Transferir el archivo de mainframe

Tarea	Descripción	Habilidades requeridas
Envíe la clave privada SSH a la computadora central.	Utilice SFTP o SCP para enviar la clave privada SSH al entorno heredado. Ejemplo de SFTP: `sftp [USERNAME@mainframeIP]` `[password]` `cd [/u/USERNAME]` `put [your-key-pair-file]` Ejemplos de SCP: `scp [your-key-pair-file] [USERNAME@MainframeIP]:/[u/USERNAME]` A continuación, guarde la clave SSH en el sistema de archivos z/OS Unix con el nombre de usuario que ejecutará posteriormente el trabajo de transferencia de archivos por lotes (por ejemplo, `/u/CONTROLM`). Nota: Para obtener más información sobre el intérprete de comandos de z/OS Unix, consulte An introduction to the z/OS shells (Introducción a los intérpretes de comandos	Mainframe, intérprete de comandos de z/OS Unix, FTP, SCP

Tarea	Descripción	Habilidades requeridas
	de z/OS) (documentación de IBM).	

Tarea	Descripción	Habilidades requeridas
Cree el cliente SFTP de JCL.	Como los mainframes no tienen un cliente SFTP nativo, debe usar la utilidad BPXBATCH para ejecutar el cliente SFTP desde el intérprete de comandos de z/OS Unix. En el editor ISPF, cree el cliente SFTP JCL. Por ejemplo: `//JOBNAM JOB ...` `//************` `******************` `******************` `******************` `****` `//SFTP EXEC PGM=BPXBA` `TCH,REGION=0M` `//STDPARM DD *` `SH cp "//'MAINF` `RAME.FILE.NAME'"` ` filename.txt;` `echo 'put filename.txt'` ` > uplcmd;` `sftp -b uplcmd -i` ` ssh_private_key_fi` `le ssh_username@<tran` `sfer service ip or` ` DNS>;` `//SYSPRINT DD SYSOUT=*` `//STDOUT DD SYSOUT=*` `//STDENV DD *` `//STDERR DD SYSOUT=*` Nota: Para obtener más información sobre cómo	JCL, Mainframe, intérprete de comandos de z/OS Unix

Tarea	Descripción	Habilidades requeridas
	ejecutar un comando en el intérprete de comandos de z/OS Unix, consulte la utilidad BPXBATCH (documentación de IBM). Para obtener más información sobre cómo crear o editar trabajos de JCL en z/OS, consulte What is ISPF? (¿Qué es el ISPF?) y The ISPF editor (El editor ISPF) (documentación de IBM).	
Ejecute el cliente SFTP de JCL.	1. En el editor ISPF, escriba SUB y, a continuación, pulse la tecla INTRO, una vez creada la tarea JCL. 2. Supervise la actividad de los trabajos por lotes de transferencia de archivos del mainframe en SDSF. Nota: Para obtener más información sobre cómo comprobar la actividad de los trabajos por lotes, consulte la Guía del usuario de z/OS SDSF (documentación de IBM).	Mainframe, JCL, ISPF

Tarea	Descripción	Habilidades requeridas
Valide la transferencia de archivos.	1. Inicie sesión en la consola de administración de AWS, abra la consola de Amazon S3 y, a continuación, seleccione Buckets en el panel de navegación. 2. Seleccione el bucket que está asociado a su Transfer Family. 3. En la sección Objects de la pestaña Objects, busque el archivo que ha transferido desde el mainframe.	AWS general
Automatice el cliente SFTP de JCL.	Utilice el programador de tareas para activar automáticamente el cliente SFTP de JCL. Nota: Puede utilizar planificadores de trabajos de mainframe, como BMC Control-M o CA Workload Automation, para automatizar los trabajos por lotes para la transferencia de archivos en función del tiempo y otras dependencias de los trabajos por lotes.	Programador de trabajos

Recursos relacionados

- How AWS Transfer Family works (Cómo funciona AWS Transfer Family)
- Mainframe Modernization with AWS (Modernización del mainframe con AWS)

Transfiera datos de Db2 z/OS a gran escala a Amazon S3 en archivos CSV

Creado por Bruno Sahinoglu (AWS), Ivan Schuster (AWS) y Abhijit Kshirsagar (AWS)

Repositorio de código: descargue DB2 z/OS a S3	Entorno: producción	Origen: Db2
Destino: Amazon S3	Tipo R: redefinir la plataforma	Carga de trabajo: IBM
Tecnologías: mainframe ; lagos de datos; bases de datos; desarrollo y pruebas de software; migración	Servicios de AWS: Amazon Aurora; AWS Glue; Amazon S3; AWS Transfer Family; Amazon Athena	

Resumen

Un mainframe sigue siendo el sistema de registro de muchas empresas que conservan una enorme cantidad de datos, incluidas entidades de datos maestros con registros de las transacciones comerciales actuales e históricas. A menudo está aislado, y los sistemas distribuidos de la misma empresa no pueden acceder fácilmente a él. Con la aparición de la tecnología en la nube y la democratización de los macrodatos, las empresas tratan de usar la información oculta en los datos del mainframe para desarrollar nuevas capacidades empresariales.

Con ese objetivo, las empresas buscan abrir sus datos Db2 de mainframe a su entorno de nube de Amazon Web Services (AWS). Los motivos empresariales son varios, y los métodos de transferencia varían de un caso a otro. Es posible que prefiera conectar la aplicación directamente al mainframe, o que prefiera replicar los datos prácticamente en tiempo real. Si el caso de uso es alimentar un almacén de datos o un lago de datos, disponer de una up-to-date copia ya no es un problema y el procedimiento descrito en este patrón puede ser suficiente, especialmente si se quiere evitar los costes de licencia de productos de terceros. Otro caso de uso podría ser la transferencia de datos de un mainframe para un proyecto de migración. En un escenario de migración, es necesario contar con datos para realizar las pruebas de equivalencia funcional. El enfoque descrito en esta publicación es una forma rentable de transferir los datos de Db2 al entorno de nube de AWS.

Dado que Amazon Simple Storage Service (Amazon S3) es uno de los servicios de AWS más integrados, puede acceder a los datos desde allí y recopilar información directamente mediante otros servicios de AWS, como Amazon Athena, AWS Lambda Functions o Amazon. QuickSight También puede cargar los datos en Amazon Aurora o Amazon DynamoDB mediante AWS Glue o AWS Database Migration Service (AWS DMS). Con ese objetivo en mente, este patrón describe cómo descargar datos de Db2 en archivos CSV en formato ASCII en el mainframe y transferir los archivos a Amazon S3.

Para ello, se han desarrollado scripts de mainframe que le ayudan a generar lenguajes de control de tareas (JCL) para descargar y transferir tantas tablas de Db2 como necesite.

Requisitos previos y limitaciones

Requisitos previos

- Un usuario del sistema operativo IBM z/OS con autorización para ejecutar scripts Restructured Extended Executor (REXX) y JCL.
- Acceso a z/OS Unix System Services (USS) para generar claves públicas y privadas de SSH (Secure Shell).
- Un bucket de S3 con permisos de escritura. Para obtener más información, consulte la sección Cree su primer bucket de S3 en la documentación de Amazon S3.
- Un servidor habilitado para el protocolo SSH File Transfer (SFTP) de AWS Transfer Family con Service Managed como proveedor de identidad y Amazon S3 como servicio de almacenamiento de AWS. Para obtener más información, consulte Crear un servidor habilitado para SFTP en la documentación de AWS Transfer Family.

Limitaciones

- Este enfoque no es adecuado para la sincronización de datos prácticamente en tiempo real o en tiempo real.
- Los datos solo se pueden trasladar de Db2 z/OS a Amazon S3, y no al revés.

Arquitectura

Pila de tecnología de origen

- Mainframe que ejecuta Db2 en z/OS

Pila de tecnología de destino

- AWS Transfer Family
- Amazon S3
- Amazon Athena
- Amazon QuickSight
- AWS Glue
- Amazon Relational Database Service (Amazon RDS)
- Amazon Aurora
- Amazon Redshift

Arquitectura de origen y destino

El siguiente diagrama muestra el proceso de generación, extracción y transferencia de datos de Db2 z/OS en formato CSV ASCII a un bucket de S3.

1. Se selecciona una lista de tablas para la migración de datos del catálogo de Db2.
2. La lista se usa para impulsar la generación de trabajos de descarga con las columnas numéricas y de datos en formato externo.
3. A continuación, los datos se transfieren a Amazon S3 mediante AWS Transfer Family.
4. Un trabajo de extracción, transformación y carga (ETL) de AWS Glue puede transformar los datos y cargarlos en un bucket procesado en el formato especificado, o bien AWS Glue puede introducir los datos directamente en la base de datos.
5. Amazon Athena y Amazon se QuickSight pueden usar para consultar y renderizar los datos para impulsar el análisis.

En el siguiente diagrama se muestra un flujo lógico de todo el proceso.

1. El primer JCL, denominado TABNAME, usará la utilidad DSNTIAUL de Db2 para extraer y generar la lista de tablas que planea descargar de Db2. Para elegir las tablas, debe adaptar manualmente la entrada SQL para seleccionar y añadir criterios de filtro que incluyan uno o más esquemas de Db2.

2. El segundo JCL, denominado REXXEXEC, usará un esqueleto de JCL y el programa REXX proporcionado para procesar la lista de tablas creada por el JCL TABNAME y generar un JCL por nombre de tabla. Cada JCL incluirá un paso para descargar la tabla y otro paso para enviar el archivo al bucket de S3 mediante el protocolo SFTP.
3. El último paso consiste en ejecutar el JCL para descargar la tabla y transferir el archivo a AWS. Todo el proceso se puede automatizar con AWS o mediante un programador en las instalaciones.

Herramientas

Servicios de AWS

- Amazon Athena es un servicio interactivo de consultas que le permite analizar datos directamente en Amazon Simple Storage Service (Amazon S3) usando SQL estándar.
- Amazon Aurora es un motor de base de datos relacional completamente administrado diseñado para la nube y compatible con MySQL y PostgreSQL.
- AWS Glue es un servicio de extracción, transformación y carga (ETL) completamente administrado. Ayuda a clasificar, limpiar, enriquecer y mover datos de forma fiable entre almacenes de datos y flujos de datos.
- Amazon QuickSight es un servicio de inteligencia empresarial (BI) a escala de nube que le ayuda a visualizar, analizar y elaborar informes sobre sus datos en un único panel de control.
- Amazon Redshift es un servicio de almacenamiento de datos administrado de varios petabytes en la nube de AWS.
- Amazon Relational Database Service (Amazon RDS) le ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Transfer Family es un servicio de transferencia segura que le permite transferir archivos dentro y fuera de los servicios de almacenamiento de AWS.

Herramientas de mainframe

- El Protocolo SSH File Transfer (SFTP) es un protocolo seguro de transferencia de archivos que permite el inicio de sesión remoto y la transferencia de archivos entre servidores. SSH proporciona seguridad al cifrar todo el tráfico.
- DSNTIAUL es un programa de muestra proporcionado por IBM para descargar datos.

- DSNUTILB es un programa de utilidades por lotes proporcionado por IBM para descargar datos con diferentes opciones de DSNTIAUL.
- z/OS OpenSSH es un puerto SSH de software de código abierto que se ejecuta en Unix System Service bajo el sistema operativo z/OS de IBM. SSH es un programa de conexión segura y cifrada entre dos computadoras que se ejecutan en una red TCP/IP. Proporciona múltiples utilidades, como ssh-keygen.
- El script REXX (Restructured Extended Executor) se usa para automatizar la generación de JCL con los pasos Db2 Unload y SFTP.

Código

El código de este patrón está disponible en el repositorio GitHub unloaddb2.

Prácticas recomendadas

En la primera descarga, los JCL generados deberían descargar todos los datos de la tabla.

Tras la primera descarga completa, realice descargas graduales para mejorar el rendimiento y ahorrar costos. Actualice la consulta SQL de la plantilla JCL para adaptarla a cualquier cambio en el proceso de descarga.

Puede convertir el esquema manualmente o mediante un script de Lambda con SYSPUNCH de Db2 como entrada. Para un proceso industrial, la herramienta de conversión de esquemas (SCT) de AWS es la opción recomendada.

Por último, use un programador basado en mainframe o un programador en AWS con un agente en el mainframe para ayudar a gestionar y automatizar todo el proceso.

Epics

Configuración del bucket de S3

Tarea	Descripción	Habilidades requeridas
Cree el bucket de S3.	Para obtener instrucciones, consulte Crear su primer bucket de S3.	AWS general

Configure el servidor Transfer Family

Tarea	Descripción	Habilidades requeridas
Cree un servidor compatible con SFTP.	Para abrir y crear un servidor SFTP en la consola de AWS Transfer Family, haga lo siguiente: 1. En la página Elegir protocolos, active la casilla SFTP (Protocolo SSH File Transfer): transferencia de archivos a través de Secure Shell. 2. Para el proveedor de identidad, seleccione Service managed (Administrado por el servicio). 3. En el punto de conexión, seleccione Acceso público. 4. En el dominio, seleccione Amazon S3. 5. En la página Configurar detalles adicionales, mantenga la configuración predeterminada. 6. Cree el servidor.	AWS general
Cree un rol de IAM para Transfer Family.	Para crear un rol de AWS Identity and Access Management (IAM) que permita a Transfer Family obtener acceso a Amazon S3, siga las instrucciones de Crear una política y rol de IAM.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Añada un usuario gestionado por el servicio Amazon S3.	Para añadir el usuario gestionado por el servicio Amazon S3, siga las instrucciones de la documentación de AWS y use su ID de usuario de mainframe.	AWS general

Proteja el protocolo de comunicación

Tarea	Descripción	Habilidades requeridas
Cree la clave de SSH.	En el entorno de USS de su servidor principal, ejecute el siguiente comando. `ssh-keygen -t rsa` Nota: Cuando se le pida una contraseña, deje el campo vacío.	Desarrollador de Mainframe
Proporcione los niveles de autorización correctos a la carpeta SSH y a los archivos de clave.	De forma predeterminada, las claves públicas y privadas se almacenarán en el directorio de usuario `/u/home/username/.ssh` . Debe conceder autorización 644 a los archivos de clave, y 700 a la carpeta. `chmod 644 .ssh/id_rsa` `chmod 700 .ssh`	Desarrollador de Mainframe

Tarea	Descripción	Habilidades requeridas
Copie el contenido de la clave pública a su usuario gestionado o por el servicio Amazon S3.	Para copiar el contenido de clave pública generado por USS abra la consola de AWS Transfer Family. 1. En el panel de navegación, seleccione Servers (Servidores). 2. Seleccione el identificador en la columna Server ID (ID de servidor) para ver los Server details (Detalles del servidor) 3. En Usuarios, seleccione un nombre de usuario para ver la página de Detalles del usuario 4. En SSH public keys, seleccione Add SSH public key (Añadir clave pública de SSH) para añadir una nueva clave SSH pública a un usuario. En la clave pública de SSH, introduzca su clave pública. El servicio valida su clave antes de que añada al nuevo usuario. 5. Elija Agregar clave.	Desarrollador de Mainframe

Genere los JCL

Tarea	Descripción	Habilidades requeridas
Genere la lista de tablas Db2 incluidas.	Proporcione el código SQL de entrada para crear una lista de las tablas destinadas a la migración de datos. Este paso requiere que especifique los criterios de selección consultando la tabla SYSIBM.SYSTABLES del catálogo de Db2 mediante una cláusula where de SQL. Los filtros se pueden personalizar para incluir un esquema específico, o bien nombres de tablas que comiencen con un prefijo concreto o en función de una marca de tiempo para la descarga gradual. El resultado se captura en un conjunto de datos secuencial físico (PS) en el mainframe. Este conjunto de datos servirá de entrada para la siguiente fase de generación de JCL. Antes de usar JCL TABNAME (puede renombrarlo si es necesario), realice los siguientes cambios: 1. Sustituya <Jobcard> por una clase de trabajo y un usuario autorizado a	Desarrollador de Mainframe

Tarea	Descripción	Habilidades requeridas
	ejecutar las utilidades de Db2. 2. Sustituya <HLQ1> o personalice los nombres de los conjuntos de datos de salida para adecuarlos los estándares de su sitio. 3. Actualice la pila de PDSE de STEPLIB (conjunto de datos particionado ampliado) según los estándares de su sitio. El ejemplo de este patrón emplea los valores predeterminados de IBM. 4. Sustituya el nombre de PLAN y el LIB por los valores específicos de su instalación. 5. Sustituya <Schema> y <Prefix> por sus criterios de selección del catálogo de Db2. 6. Guarde el JCL resultant e en una biblioteca PDS (conjunto de datos particion ado). 7. Envíe el JCL. Trabajo de extracción de lista de tablas de Db2 `<Jobcard>` `//*`	

Tarea	Descripción	Habilidades requeridas
	`//* UNLOAD ALL THE TABLE NAMES FOR A PARTICULAR SCHEMA` `//*` `//STEP01  EXEC PGM=IEFBR14` `//*` `//DD1  DD  DISP=(MOD,DELETE,DELETE),` `//  UNIT=SYSDA,` `//  SPACE=(1000,(1,1)),` `//  DSN=<HLQ1>.DSN81210.TABLIST` `//*` `//DD2  DD  DISP=(MOD,DELETE,DELETE),` `//  UNIT=SYSDA,` `//  SPACE=(1000,(1,1)),` `//  DSN=<HLQ1>.DSN81210.SYSPUNCH` `//*` `//UNLOAD  EXEC PGM=IKJEFT01,DYNAMNBR=20` `//SYSTSPRT DD SYSOUT=*` `//STEPLIB  DD DISP=SHR,DSN=DSNC10.DBCG.SDSNEXIT` `//  DD  DISP=SHR,DSN=DSNC10.SDSNLOAD` `//  DD  DISP=SHR,DSN=CEE.SCEERUN` `//  DD  DISP=SHR,DSN=DSNC10.DBCG.RUNLIB.LOAD` `//SYSTSIN  DD  *` `  DSN SYSTEM(DBCG)` `  RUN  PROGRAM(DSNTIAUL) PLAN(DSNTIB12) PARMS('SQL') -`	

Tarea	Descripción	Habilidades requeridas
	<pre>LIB('DSNC 10.DBCG.RUNLIB.LOAD') END //SYSPRINT DD SYSOUT=* //* //SYSUDUMP DD SYSOUT=* //* //SYSREC00 DD DISP=(NEW ,CATLG,DELETE), // UNIT=SYSD A,SPACE=(32760,(10 00,500)), // DSN=<HLQ1 >.DSN81210.TABLIST //* //SYSPUNCH DD DISP=(NEW ,CATLG,DELETE), // UNIT=SYSD A,SPACE=(32760,(10 00,500)), // VOL=SER=S CR03,RECFM=FB,LREC L=120,BLKSIZE=12 // DSN=<HLQ1 >.DSN81210.SYSPUNCH //* //SYSIN DD * SELECT CHAR(CREA TOR), CHAR(NAME) FROM SYSIBM.SY STABLES WHERE OWNER = '<Schema>' AND NAME LIKE '<Prefix>%' AND TYPE = 'T'; /*</pre>	

Tarea	Descripción	Habilidades requeridas
Modifique las plantillas de JCL.	Las plantillas JCL proporcionadas con este patrón contienen una tarjeta de trabajo y nombres de bibliotecas genéricas. Sin embargo, la mayoría de los sitios de mainframe tendrán sus propios estándares de nomenclatura para los nombres de conjuntos de datos, bibliotecas y tarjetas de trabajo. Por ejemplo, es posible que necesite una clase de trabajo específica para ejecutar trabajos de Db2. Las implementaciones del subsistema de entrada de trabajos JES2 y JES3 pueden imponer cambios adicionales. Las bibliotecas de carga estándar pueden tener un primer calificador diferente a SYS1, que es el predeterminado de IBM. Por lo tanto, personalice las plantillas para adecuarlas a los estándares específicos de su sitio antes de ejecutarlas. Realice los siguientes cambios en el esqueleto de JCL UNLDSKEL: 1. Sustituya la tarjeta de trabajo por una clase	Desarrollador de Mainframe

Tarea	Descripción	Habilidades requeridas
	de trabajo y un usuario autorizado a ejecutar las utilidades de Db2. 2. Personalice los nombres de los conjuntos de datos de salida para adecuarlos los estándares de su sitio. 3. Actualice la pila de PDSE de STEPLIB según los estándares de su sitio. El ejemplo de este patrón emplea los valores predeterminados de IBM. 4. Sustituya <DSN> por el nombre y la ID de correlaci ón del subsistema Db2. 5. Guarde el JCL resultante en una biblioteca de PDS que forme parte de su pila de ISPSLIB, biblioteca básica de plantillas estándar para ISPF. Descargue el esqueleto de JCL mediante SFTP `//&USRPFX.U JOB (DB2UNLOAD),'JOB', CLASS=A,MSGCLASS=A, //  TIME=1440 ,NOTIFY=&USRPFX //* DELETE DATASETS //STEP01  EXEC PGM=IEFBR14`	

Tarea	Descripción	Habilidades requeridas
	`//DD01 DD DISP=(MOD ,DELETE,DELETE), // UNIT=SYSD A, // SPACE=(TR K,(1,1)), // DSN=&USRPFX..DB2.P UNCH.&JOBNAME //DD02 DD DISP=(MOD ,DELETE,DELETE), // UNIT=SYSD A, // SPACE=(TR K,(1,1)), // DSN=&USRPFX..DB2.U NLOAD.&JOBNAME //* //* RUNNING DB2 EXTRACTION BATCH JOB FOR AWS DEMO //* //UNLD01 EXEC PGM=DSNUTILB,REGIO N=0M, // PARM='<DSN>,UNLOAD' //STEPLIB DD DISP=SHR,DSN=DSNC1 0.DBCG.SDSNEXIT // DD DISP=SHR, DSN=DSNC10.SDSNLOAD //SYSPRINT DD SYSOUT=* //UTPRINT DD SYSOUT=* //SYSOUT DD SYSOUT=* //SYSPUN01 DD DISP=(NEW,CATLG,DE LETE), // SPACE=(CY L,(1,1),RLSE), // DSN=&USRPFX..DB2.P UNCH.&JOBNAME`	

Tarea	Descripción	Habilidades requeridas
	`//SYSREC01 DD` ` DISP=(NEW,CATLG,DE` `LETE),` `//  SPACE=(CY` `L,(10,50),RLSE),` `// DSN=&USRPFX..DB2.U` `NLOAD.&JOBNAME` `//SYSPRINT DD SYSOUT=*` `//SYSIN  DD *` `  UNLOAD` `  DELIMITED COLDEL ','` `  FROM TABLE &TABNAME` `  UNLDDN SYSREC01` `  PUNCHDDN SYSPUN01` `  SHRLEVEL CHANGE` ` ISOLATION UR;` ` /*` `//*` `//* FTP TO AMAZON S3` ` BACKED FTP SERVER IF` ` UNLOAD WAS SUCCESSFUL` `//*` `//SFTP EXEC PGM=BPXBA` `TCH,COND=(4,LE),RE` `GION=0M` `//STDPARM DD *` ` SH cp "//'&USRP` `FX..DB2.UNLOAD.&JO` `BNAME'"` `  &TABNAME..csv;` ` echo "ascii` ` " >> uplcmd;` ` echo "PUT &TABNAME.` `.csv " >>>> uplcmd;` ` sftp -b uplcmd -i .ssh/` `id_rsa &FTPUSER.` `@&FTPSITE;` ` rm &TABNAME..csv;` ` //SYSPRINT DD SYSOUT=*` ` //STDOUT DD SYSOUT=*` ` //STDENV DD *`	

Tarea	Descripción	Habilidades requeridas
	`//STDERR DD SYSOUT=*`	

Tarea	Descripción	Habilidades requeridas
Genere el JCL de descarga masiva.	Este paso implica ejecutar un script REXX en un entorno ISPF mediante JCL. Proporcione la lista de tablas incluidas en el primer paso como entrada para la generación masiva de JCL con el nombre `TABLIST DD`. El JCL generará un nuevo JCL por nombre de tabla en un conjunto de datos particionado definido por el usuario y especificado con el nombre `ISPFILE DD`. Asigne esta biblioteca de antemano. Cada nuevo JCL tendrá dos pasos: uno para descargar la tabla de Db2 en un archivo y otro para enviar el archivo al bucket de S3. Realice los siguientes cambios en el JCL REXXEXEC (puede cambiar el nombre): 1. Sustituya `Job card user ID` por una ID de usuario de mainframe con autoridad de descarga de las tablas. Sustituya `SYSPROC`, `ISPPLIB`, `ISPSLIB`, `ISPMLIB` y los valores `ISPTLIB` y `<HLQ1>`, o personalice `DSN` según los estándares de	Desarrollador de Mainframe

Tarea	Descripción	Habilidades requeridas
	su sitio. Para averiguar los valores específicos de su instalación, ejecute el comando `TSO ISRDDN`. 2. Sustituya `<MFUSER>` por un ID de usuario con privilegios de ejecución de tareas en la instalación. 3. Sustituya `<FTPUSER>` por un ID de usuario con privilegios de USS y FTP en la instalación. Se presupone que esta ID de usuario y sus claves de seguridad SSH se encuentran en el directorio de Unix Systems Services correspondiente de la computadora central. 4. Sustituya `<AWS TransferFamily IP>` por la dirección IP o el nombre de dominio de AWS Transfer Family. Esta dirección se utilizará para el paso de SFTP. 5. Envíe el JCL después de solicitar el alojamiento estándar del sitio y actualizar el programa REXX como se describe a continuación.	

Tarea	Descripción	Habilidades requeridas
	Generación masiva de trabajos JCL `//RUNREXX JOB (CREATEJCL),'RUNS ISPF TABLIST', CLASS=A,MSGCLASS=A,` `//  TIME=1440 ,NOTIFY=&SYSUID` `//* Most of the values required can be updated to your site specific` `//* values using the command 'TSO ISRDDN' in your ISPF session.` `//* Update all the lines tagged with //update marker to desired` `//* site specific values.` `//ISPF EXEC PGM=IKJEFT01,REGION=2048K,DYNAMNBR=25` `//SYSPROC DD DISP=SHR,DSN=USER.Z23D.CLIST` `//SYSEXEC DD DISP=SHR,DSN=<HLQ1>.TEST.REXXLIB` `//ISPPLIB DD DISP=SHR,DSN=ISP.SISPPENU` `//ISPSLIB DD DISP=SHR,DSN=ISP.SISPSENU` `//  DD DISP=SHR,DSN=<HLQ1>.TEST.ISPSLIB` `//ISPMLIB DD DSN=ISP.SISPMENU,DISP=SHR`	

Tarea	Descripción	Habilidades requeridas
	`//ISPTLIB DD` `DDNAME=ISPTABL` `// DD DSN=ISP.S` `ISPTENU,DISP=SHR` `//ISPTABL DD` `LIKE=ISP.SISPTENU,` `UNIT=VIO` `//ISPPROF DD` `LIKE=ISP.SISPTENU,` `UNIT=VIO` `//ISPLOG DD` `SYSOUT=*,RECFM=VA,` `LRECL=125` `//SYSPRINT DD SYSOUT=*` `//SYSTSPRT DD` `SYSOUT=*` `//SYSUDUMP DD` `SYSOUT=*` `//SYSDBOUT DD` `SYSOUT=*` `//SYSTSPRT DD` `SYSOUT=*` `//SYSUDUMP DD` `SYSOUT=*` `//SYSDBOUT DD` `SYSOUT=*` `//SYSHELP DD` `DSN=SYS1.HELP,DISP` `=SHR` `//SYSOUT DD SYSOUT=*` `//* Input list of` `tablenames` `//TABLIST DD` `DISP=SHR,DSN=<HLQ1` `>.DSN81210.TABLIST` `//* Output pds` `//ISPFILE DD` `DISP=SHR,DSN=<HLQ1` `>.TEST.JOBGEN` `//SYSTSIN DD *`	

Tarea	Descripción	Habilidades requeridas
	ISPSTART CMD(ZSTEPS <MFUSER> <FTPUSER> <AWS TransferFamily IP>) /* Antes de ejecutar el script REXX, realice los siguientes cambios: 1. Guarde el script REXX en una biblioteca PDS definida en la pila SYSEXEC del JCL REXXEXEC, editada en el paso anterior con el nombre de miembro ZSTEPS. Si desea renombrarlo, actualice el JCL según sus necesidades. 2. Este script usa la opción de rastreo para imprimir información adicional en caso de que se produzcan errores. En su lugar, puede añadir un código de gestión de errores después de las instrucciones EXECIO, ISPEXEC y TSO, y eliminar la línea de rastreo. 3. Este script genera nombres de miembro con la convención de nomenclatura L0Dnnnnn, con capacidad para hasta 100 000 miembros. Si tiene más de 100 000 tablas, use un	

Tarea	Descripción	Habilidades requeridas
	prefijo más corto y ajuste los números de la instrucción `tempjob`. Script ZSTEPS REXX `/*REXX - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - */` `/* 10/27/2021 - added new parms to accommodate ftp */` `Trace "o"` `parse arg usrpfx ftpuser ftpsite` `Say "Start"` `Say "Ftpuser: " ftpuser "Ftpsite:" ftpsite` `Say "Reading table name list"` `"EXECIO * DISKR TABLIST (STEM LINE. FINIS"` `DO I = 1 TO LINE.0` `Say I` `suffix = I` `Say LINE.i` `Parse var LINE.i schema table rest` `tabname = schema !! "." !! table` `Say tabname` `tempjob= "LOD" !! RIGHT("0000" !! i, 5)` `jobname=tempjob` `Say tempjob` `ADDRESS ISPEXEC "FTOPEN "`	

Tarea	Descripción	Habilidades requeridas
	<pre>ADDRESS ISPEXEC "FTINCL UNLDSKEL" /* member will be saved in ISPDSN library allocated in JCL */ ADDRESS ISPEXEC "FTCLOSE NAME("tem pjob")" END ADDRESS TSO "FREE F(TABLIST) " ADDRESS TSO "FREE F(ISPFILE) " exit 0</pre>	

Ejecutar JCL

Tarea	Descripción	Habilidades requeridas
Realice el paso de descarga de Db2.	Tras la generación de los JCL, tendrá tantos JCL como tablas necesite descargar. Esta historia emplea un ejemplo generado por el JCL para explicar la estructura y los pasos más importantes. No tiene que hacer nada. La siguiente información es solo para referencia. Si desea enviar los JCL que ha generado en el paso anterior, pase a la tarea Enviar los JCL LODnnnnn.	Desarrollador de mainframe, ingeniero de sistemas

Tarea	Descripción	Habilidades requeridas
	Al descargar datos de Db2 usando un JCL con la utilidad DSNUTILB Db2 proporcionada por IBM, debe asegurarse de que los datos descargados no contengan datos numéricos comprimidos. Para ello, utilice el parámetro de DSNUTILB `DELIMITED` . El parámetro `DELIMITED` permite descargar los datos en formato CSV añadiendo un carácter como delimitador y comillas dobles para el campo de texto, eliminando el relleno de la columna VARCHAR y convirtiendo todos los campos numéricos a FORMATO EXTERNO, incluidos los campos de FECHA. El siguiente ejemplo muestra el aspecto del paso de descarga en el JCL generado, usando el carácter de coma como delimitador. `UNLOAD` `DELIMITED COLDEL ','` `FROM TABLE SCHEMA_NAME.TBNAME` `UNLDDN SYSREC01` `PUNCHDDN SYSPUN01`	

Tarea	Descripción	Habilidades requeridas
	`SHRLEVEL CHANGE ISOLATION UR;`	
Realice el paso de SFTP.	Para usar el protocolo SFTP de un JCL, emplee la utilidad BPXBATCH. La utilidad SFTP no puede acceder directamente a los conjuntos de datos de MVS. Puede usar el comando de copia (`cp`) para copiar el archivo secuencial `&USRPFX..DB2.UNLOAD.&JOBNAME` al directorio USS, donde se convierte en `&TABNAME..csv` . Ejecute el comando `sftp` con la clave privada (`id_rsa`) y la ID de usuario de RACF como nombre de usuario para conectarse a la dirección IP de AWS Transfer Family. `SH cp "//'&USRPFX..DB2.UNLOAD.&JOBNAME'" &TABNAME..csv; echo "ascii " >> uplcmd; echo "PUT &TABNAME..csv " >>>> uplcmd; sftp -b uplcmd -i .ssh/id_rsa &FTPUSER.@&FTP_TF_SITE; rm &TABNAME..csv;`	Desarrollador de mainframe, ingeniero de sistemas

Tarea	Descripción	Habilidades requeridas
Envíe los JCL de LODnnnnn.	El JCL anterior genera todas las tablas JCL de LODnnnnn que deben descargarse, transformarse en CSV y transferirse al bucket de S3. Ejecute el comando `submit` en todos los JCL que se hayan generado.	Desarrollador de mainframe, ingeniero de sistemas

Recursos relacionados

Para obtener más información sobre las diferentes herramientas y soluciones usadas en este documento, consulte lo siguiente:

- Guía del usuario de z/OS OpenSSH
- Db2 z/OS: ejemplos de instrucciones de control UNLOAD
- Db2 z/OS: descarga de archivos delimitados
- Transfer Family: cree un servidor habilitado para SFTP
- Transfer Family: trabajar con usuarios gestionados por servicios

Información adicional

Una vez que tenga sus datos de Db2 en Amazon S3, podrá obtener información de múltiples maneras. Como Amazon S3 se integra con los servicios de análisis de datos de AWS, puede consumir o exponer libremente estos datos de forma distribuida. Por ejemplo, puede hacer lo siguiente:

- Cree un lago de datos en Amazon S3 y extraiga información valiosa mediante query-in-place el uso de herramientas de análisis y aprendizaje automático sin mover los datos.
- Iniciar una función de Lambda configurando un flujo de trabajo de procesamiento posterior a la carga integrado con AWS Transfer Family.

- Desarrollar nuevos microservicios para acceder a los datos en Amazon S3 o en una base de datos totalmente administrada con AWS Glue, un servicio de integración de datos sin servidor que facilita la detección, preparación y combinación de datos para el análisis, el machine learning y el desarrollo de aplicaciones.

En un caso de uso de migración, dado que puede transferir cualquier dato del mainframe a S3, puede hacer lo siguiente:

- Retirar la infraestructura física y crear una estrategia de archivado de datos rentable con Amazon S3 Glacier y S3 Glacier Deep Archive.
- Crear soluciones de copia de seguridad y restauración escalables, duraderas y seguras con Amazon S3 y otros servicios de AWS, como S3 Glacier y Amazon Elastic File System (Amazon EFS), para mejorar o reemplazar las capacidades existentes en las instalaciones.

Más patrones

- Replicar bases de datos de unidades centrales en AWS mediante Precisely Connect

Gestión y gobernanza

Temas

- Identifique y avise cuando los recursos de Amazon Data Firehose no estén cifrados con una clave de AWS KMS
- Automatice la adición o actualización de entradas de registro de Windows con AWS Systems Manager
- Detenga e inicie automáticamente una instancia de base de datos de Amazon RDS mediante Ventanas de mantenimiento de AWS Systems Manager
- Centralice la distribución de paquetes de software en AWS Organizations mediante Terraform
- Configure los registros de VPC Flow para centralizarlos en todas las cuentas de AWS
- Configure el registro para aplicaciones.NET en Amazon CloudWatch Logs mediante nLog
- Copiar los productos de AWS Service Catalog en diferentes cuentas y regiones de AWS
- Cree alarmas para métricas personalizadas mediante la detección de CloudWatch anomalías de Amazon
- Documente el diseño de su zona de aterrizaje de AWS
- Configure la detección de CloudFormation desviaciones de AWS en una organización multirregional y multicuenta
- Mejore el rendimiento operativo al habilitar Amazon DevOps Guru en varias regiones, cuentas y unidades organizativas de AWS con la AWS CDK
- Implemente Account Factory for Terraform (AFT) mediante una canalización de arranque
- Administre los productos de AWS Service Catalog en varias cuentas y regiones de AWS
- Migración de una cuenta de miembro de AWS de AWS Organizations a AWS Control Tower
- Supervisar el uso de una imagen de máquina de Amazon compartida en varias cuentas de AWS
- Configure alertas para el cierre programático de cuentas en AWS Organizations
- Más patrones

Identifique y avise cuando los recursos de Amazon Data Firehose no estén cifrados con una clave de AWS KMS

Creado por Ram Kandaswamy (AWS)

Entorno: producción	Tecnologías: administración y gobierno; análisis; macrodatos; nativas en la nube; infraestructura; seguridad, identidad, conformidad	Servicios de AWS: AWS CloudTrail; Amazon CloudWatch; AWS Identity and Access Management; Amazon Kinesis; AWS Lambda; Amazon SNS

Resumen

Para cumplir con las normas, algunas organizaciones deben tener el cifrado activado en los recursos de entrega de datos, como Amazon Data Firehose. Este patrón muestra una forma de monitorear, detectar y notificar cuando los recursos no cumplen con las normas.

Para mantener el requisito de cifrado, este patrón se puede utilizar en Amazon Web Services (AWS) para proporcionar una supervisión y detección automatizadas de los recursos de entrega de Firehose que no están cifrados con la clave de AWS Key Management Service (AWS KMS). La solución envía notificaciones de alerta y se puede ampliar para que se corrija automáticamente. Esta solución se puede aplicar a una cuenta individual o a un entorno de varias cuentas, como un entorno que utilice AWS Landing Zone o AWS Control Tower.

Requisitos previos y limitaciones

Requisitos previos

- Flujo de entrega de Firehose
- Permisos suficientes y familiaridad con AWS CloudFormation, que se utiliza en la automatización de esta infraestructura

Limitaciones

La solución no es en tiempo real porque utiliza CloudTrail eventos de AWS para la detección y hay un retraso entre el momento en que se crea un recurso sin cifrar y el momento en que se envía la notificación.

Arquitectura

Pila de tecnología de destino

La solución utiliza tecnología sin servidor y los siguientes servicios:

- AWS CloudTrail
- Amazon CloudWatch
- Interfaz de la línea de comandos de AWS (AWS CLI)
- AWS Identity y Access Management (IAM)
- Amazon Data Firehose
- AWS Lambda
- Amazon Simple Notification Service (Amazon SNS)

Arquitectura de destino

1. Un usuario crea o modifica Firehose.
2. Se detecta un CloudTrail evento y se hace coincidir.
3. Lambda es invocado.
4. Se identifican los recursos que no cumplen con las normas.
5. Se envía una notificación por correo electrónico.

Automatizar y escalar

Con AWS CloudFormation StackSets, puede aplicar esta solución a varias regiones o cuentas de AWS con un solo comando.

Herramientas

- AWS CloudTrail: AWS CloudTrail es un servicio de AWS que le ayuda a habilitar la gobernanza, el cumplimiento y la auditoría operativa y de riesgos de su cuenta de AWS. Las acciones realizadas

por un usuario, un rol o un servicio de AWS se registran como eventos en CloudTrail. Los eventos incluyen las acciones realizadas en la consola de administración de AWS, la interfaz de la línea de comandos de AWS y las operaciones de API y los SDK de AWS.

- Amazon CloudWatch Events: Amazon CloudWatch Events ofrece una near-real-time secuencia de eventos del sistema que describen los cambios en los recursos de AWS.
- AWS CLI: la interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.
- IAM: AWS Identity and Access Management (IAM) es un servicio web que le ayuda a controlar de forma segura el acceso a los recursos de AWS. Utilice IAM para controlar quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos.
- Amazon Data Firehose: Amazon Data Firehose es un servicio totalmente gestionado que ofrece datos de streaming en tiempo real. Con Firehose, no necesitas escribir aplicaciones ni administrar recursos. Usted configura sus generadores de datos para que envíen datos a Firehose, y esta entrega automáticamente los datos al destino que especificó.
- AWS Lambda: AWS Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo. Solo pagará por el tiempo de computación que consuma, no se aplican cargos cuando el código no se está ejecutando.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) es un servicio administrado con el que se ofrece la entrega de mensajes de los publicadores a los suscriptores (también conocido como productores y consumidores).

Epics

Aplique el cifrado para garantizar el cumplimiento

Tarea	Descripción	Habilidades requeridas
Implemente AWS CloudFormation StackSets.	En la AWS CLI, utilice la `firehose-encryption-checker.yaml` plantilla (adjunta) para crear el conjunto de pilas ejecutand	Arquitecto de la nube, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	o el siguiente comando. Proporcione un Nombre de recurso de Amazon (ARN) de tema de Amazon SNS válido para el parámetro. La implementación debe crear correctamente las reglas de CloudWatch eventos, la función Lambda y un rol de IAM con los permisos necesarios, tal y como se describe en la plantilla. `aws cloudformation create-stack-set --stack-set-name my-stack-set --template-body file://firehose-encryption-checker.yaml`	

Tarea	Descripción	Habilidades requeridas
Cree instancias de pila.	Las pilas deben crearse en las regiones de AWS que elija, así como en una o más cuentas. Para crear instancias de pila, ejecute el siguiente comando y reemplace el nombre de pila, los números de cuenta y las regiones por los suyos. `aws cloudformation create-stack-instances --stack-set-name my-stack-set --accounts 123456789012 223456789012 --regions us-east-1 us-east-2 us-west-1 us-west-2 --operation-preferences FailureToleranceCount=1`	Arquitecto de la nube, administrador de sistemas

Recursos relacionados

- Trabajando con AWS CloudFormation StackSets
- ¿Qué es Amazon CloudWatch Events?

Información adicional

AWS Config no admite el tipo de recurso Firehose Delivery Stream, por lo que no se puede usar una regla de AWS Config en la solución.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Automatice la adición o actualización de entradas de registro de Windows con AWS Systems Manager

Creado por Appasaheb Bagali (AWS)

Creado por: AWS	Entorno: PoC o piloto	Tecnologías: nativas de la nube; infraestructura DevOps; modernización; seguridad, identidad y cumplimiento; administración y gobierno
Carga de trabajo: Microsoft	Servicios de AWS: AWS Systems Manager	

Resumen

AWS Systems Manager es una herramienta de administración remota para instancias de Amazon Elastic Compute Cloud (Amazon EC2). Systems Manager proporciona visibilidad y control sobre su infraestructura en Amazon Web Services. Esta versátil herramienta permite corregir los cambios en el registro de Windows identificados como vulnerabilidades por el informe de análisis de vulnerabilidades de seguridad.

Este patrón describe los pasos para proteger las instancias de EC2 que ejecutan el sistema operativo Windows automatizando los cambios de registro recomendados para mantener la seguridad de su entorno. El patrón emplea Run Command para ejecutar un documento de comandos. Se adjunta el código, y una parte del mismo se incluye en la sección de código.

Requisitos previos y limitaciones

- Una cuenta de AWS activa
- Permisos para acceder a la instancia de EC2 y a Systems Manager

Arquitectura

Pila de tecnología de destino

- Una nube privada virtual (VPC), con dos subredes y una puerta de enlace de traducción de direcciones de red (NAT)
- Un documento de comandos de Systems Manager para añadir o actualizar el nombre y el valor del registro
- Run Command de Systems Manager para ejecutar el documento de comandos en las instancias de EC2 especificadas

Arquitectura de destino

Herramientas

Herramientas

- Políticas y roles de IAM: AWS Identity and Access Management (IAM) es un servicio web que le ayuda a controlar de forma segura el acceso a los recursos de AWS. Utilice IAM para controlar quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos.
- Amazon Simple Storage Service (Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet. Está diseñado para facilitar a los desarrolladores recursos de computación escalables basados en Web. En este patrón se usa un bucket de S3 para almacenar los registros de Systems Manager.
- AWS Systems Manager: AWS Systems Manager es un servicio que puede utilizar para ver y controlar su infraestructura en AWS. Systems Manager le ayuda a mantener la seguridad y la conformidad mediante el análisis de sus instancias administradas y el informe sobre las infracciones de las políticas que detecte (o la toma de medidas correctivas con respecto a estas).
- Documento de comandos de AWS Systems Manager: Run Command emplea los documentos de comandos de AWS Systems Manager. La mayoría de los documentos de Command son compatibles con todos los sistemas operativos Linux y Windows, que a su vez son compatibles con Systems Manager.
- AWS Systems Manager Run Command: AWS Systems Manager Run Command le ofrece una forma de gestionar la configuración de sus instancias administradas de forma remota y segura. Run Command le permite automatizar las tareas administrativas comunes y llevar a cabo cambios de configuración únicas a escala.

Código

Puede utilizar el siguiente código de ejemplo para agregar o actualizar un nombre de registro de Microsoft Windows en `Version`, una ruta de registro a `HKCU:\Software\ScriptingGuys\Scripts` y un valor a 2.

```
#Windows registry path which needs to add/update
$registryPath ='HKCU:\\Software\\ScriptingGuys\\Scripts'
#Windows registry Name  which needs to add/update
$Name = 'Version'
#Windows registry value  which needs to add/update
$value = 2
# Test-Path cmdlet to see if the registry key exists.
IF(!(Test-Path $registryPath))
        {
           New-Item -Path $registryPath -Force | Out-Null
           New-ItemProperty -Path $registryPath -Name $name -Value     $value ` -
PropertyType DWORD -                 Force | Out-        Null
        } ELSE {
                      New-ItemProperty -Path $registryPath -Name $name -Value $value `
 -PropertyType            DWORD        -Force | Out-Null
            }
echo 'Registry Path:'$registryPath
 echo 'Registry Name:'$registryPath
 echo 'Registry Value:'(Get-ItemProperty -Path $registryPath -Name $Name).version
```

Se adjunta el ejemplo de código de notación de JavaScript objetos (JSON) completo del documento de comandos de Systems Manager.

Epics

Configurar una VPC

Tarea	Descripción	Habilidades requeridas
Cree una VPC.	En la consola de administración de AWS, cree una VPC con subredes públicas y privadas y una puerta de enlace NAT. Para obtener más información, consulte la documentación de AWS.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Creación de los grupos de seguridad.	Asegúrese de que cada grupo de seguridad permita el acceso al Protocolo de escritorio remoto (RDP) desde la dirección IP de origen.	Administrador de la nube

Crear una política y un rol de IAM

Tarea	Descripción	Habilidades requeridas
Cree una política de IAM.	Cree una política de IAM que proporcione acceso a Amazon S3, Amazon EC2 y Systems Manager.	Administrador de la nube
Crear un rol de IAM.	Cree una política de IAM y adjunte la política de IAM que proporcione acceso a Amazon S3, Amazon EC2 y Systems Manager.	Administrador de la nube

Ejecute la automatización

Tarea	Descripción	Habilidades requeridas
Cree un documento de comandos de Systems Manager.	Cree un documento de comandos de Systems Manager que implemente la adición o actualización de cambios del registro de Microsoft Windows.	Administrador de la nube
Ejecute Run Command de Systems Manager.	Ejecute Run Command de Systems Manager y seleccion	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	e el documento de comandos y las instancias de destino de Systems Manager. Se transferirá el cambio de registro de Microsoft Windows en el documento de comandos seleccionado a las instancias de destino.	

Recursos relacionados

- AWS Systems Manager
- Documentos de AWS Systems Manager
- AWS Systems Manager Run Command

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Detenga e inicie automáticamente una instancia de base de datos de Amazon RDS mediante Ventanas de mantenimiento de AWS Systems Manager

Creado por Ashita Dsilva (AWS)

Entorno: producción	Tecnologías: gestión y gobierno; administración de costos; bases de datos; nativo en la nube	Servicios de AWS: AWS Systems Manager; Amazon RDS

Resumen

Este patrón muestra cómo detener e iniciar automáticamente una instancia de base de datos de Amazon Relational Database Service (Amazon RDS) según un cronograma específico (por ejemplo, cerrar una instancia de base de datos fuera del horario laboral para reducir los costos) mediante Ventanas de mantenimiento de AWS Systems Manager.

La Automatización de AWS Systems Manager proporciona los manuales de procedimientos de `AWS-StopRdsInstance` y `AWS-StartRdsInstance` para detener e iniciar las instancias de base de datos de Amazon RDS. Esto significa que no necesita escribir una lógica personalizada con las funciones de AWS Lambda ni crear una regla de Amazon CloudWatch Events.

AWS Systems Manager ofrece dos capacidades para programar tareas: State Manager y Maintenance Windows. State Manager establece y mantiene la configuración de estado requerida para los recursos de su cuenta de Amazon Web Services (AWS) una vez o según un cronograma específico. Maintenance Windows ejecuta tareas en los recursos de su cuenta durante un período de tiempo específico. Si bien puede utilizar el enfoque de este patrón con State Manager o Maintenance Windows, le recomendamos que utilice Maintenance Windows, ya que puede ejecutar una o más tareas en función de la prioridad asignada y también puede ejecutar funciones de AWS Lambda y tareas de AWS Step Functions. Para obtener más información sobre State Manager y Maintenance Windows, consulte Elegir entre State Manager y Maintenance Windows en la documentación de AWS Systems Manager.

Este patrón proporciona pasos detallados para configurar dos ventanas de mantenimiento independientes que utilizan expresiones cron para detener y, a continuación, iniciar una instancia de base de datos de Amazon RDS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una instancia de base de datos de Amazon RDS existente que desee detener e iniciar según un cronograma específico.
- Expresiones cron para el cronograma requerido. Por ejemplo, la expresión cron `(0 9 * * 1-5)` aparece por la mañana a las 09:00 de lunes a viernes.
- Familiaridad con Systems Manager.

Limitaciones

- Una instancia de base de datos de Amazon RDS se puede detener durante un máximo de siete días a la vez. Transcurridos siete días, la instancia de la base de datos se reinicia automáticamente para garantizar que reciba las actualizaciones de mantenimiento necesarias.
- No puede detener una instancia de base de datos que tenga una réplica de lectura o que sea una réplica de lectura.
- No puede detener una instancia de base de datos de Amazon RDS para SQL Server que esté en una configuración Multi-AZ.
- Service quotas se aplican a Maintenance Windows y Systems Manager Automation. Para obtener más información sobre las Service quotas, consulte Puntos de conexión y cuotas de AWS Systems Manager en la documentación de referencia general de AWS.

Arquitectura

El siguiente diagrama muestra el flujo de trabajo para detener e iniciar automáticamente una instancia de base de datos de Amazon RDS.

El flujo de trabajo tiene los siguientes pasos:

1. Cree un período de mantenimiento y utilice expresiones cron para definir el cronograma de parada e inicio de sus instancias de la base de datos de Amazon RDS.

2. Registre una tarea de automatización de Systems Manager en el periodo de mantenimiento mediante el manual de procedimientos `AWS-StopRdsInstance` o `AWS-StartRdsInstance`.

3. Registre un objetivo en el periodo de mantenimiento mediante un grupo de recursos basado en etiquetas para sus instancias de la base de datos de Amazon RDS.

Pila de tecnología

- AWS CloudFormation
- AWS Identity y Access Management (IAM)
- Amazon RDS
- Systems Manager

Automatizar y escalar

Puede detener e iniciar varias instancias de la base de datos de Amazon RDS al mismo tiempo etiquetando las instancias de la base de datos de Amazon RDS necesarias, creando un grupo de recursos que incluya todas las instancias de la base de datos etiquetadas y registrando este grupo de recursos como destino para el período de mantenimiento.

Herramientas

- AWS CloudFormation es un servicio que le ayuda a modelar y configurar sus recursos de AWS.
- AWS Identity and Access Management (IAM) es un servicio web que le ayuda a controlar de forma segura el acceso a los recursos de AWS.
- Amazon Relational Database Service (Amazon RDS) es un servicio web que facilita la configuración, el funcionamiento y el escalado de una base de datos relacional en la nube de AWS.
- AWS Resource Groups le ayuda a organizar los recursos de AWS en grupos, etiquetarlos y gestionar, supervisar y automatizar las tareas en los recursos agrupados.
- AWS Systems Manager es un servicio de AWS que puede utilizar para ver y controlar su infraestructura en AWS.

- Automatización de AWS Systems Manager simplifica las tareas comunes de mantenimiento e implementación de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) y otros recursos de AWS.
- Las ventanas de mantenimiento de AWS Systems Manager le ayudan a definir un cronograma para realizar acciones potencialmente disruptivas en sus instancias.

Epics

Crear y configurar el rol de servicio IAM para Systems Manager Automation

Tarea	Descripción	Habilidades requeridas
Configure el rol de servicio de IAM para Systems Manager Automation.	Inicie sesión en la Consola de administración de AWS y cree un rol de servicio para Systems Manager Automatio n. Puede usar uno de los dos métodos siguientes para crear este rol de servicio: • Utilice AWS CloudForm ation para configurar un rol de servicio para Systems Manager Automation • Uso de IAM a fin de configurar roles para Systems Manager Automation El flujo de trabajo de Systems Manager Automation invoca a Amazon RDS mediante un rol de servicio para realizar acciones de inicio y detención en la instancia de la base de datos de Amazon RDS.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	El rol de servicio debe configurarse con la siguiente política en línea que tenga permisos para iniciar y detener la instancia de la base de datos de Amazon RDS: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "RdsStartStop", "Effect": "Allow", "Action": [ "rds:StopDBInstance", "rds:StartDBInstance" ], "Resource": "<RDS_Instance_ARN>" }, { "Sid": "RdsDescribe", "Effect": "Allow", "Action": "rds:DescribeDBInstances", "Resource": "*" } ] }`	

Tarea	Descripción	Habilidades requeridas
	Asegúrese de reemplazar `<RDS_Instance_ARN>` por el nombre de recurso de Amazon (ARN) de la instancia de la base de datos de Amazon RDS. Importante: asegúrese de registrar el ARN del rol de servicio.	

Crear un grupo de recursos

Tarea	Descripción	Habilidades requeridas
Etiquete las instancias de base de datos de Amazon RDS.	Abra la consola de Amazon RDS y etiquete las instancias de la base de datos de Amazon RDS que desee añadir al grupo de recursos. Una etiqueta es un metadato asignado a un recurso de AWS y consiste en un par clave-valor. Le recomendamos que utilice Acción como clave de etiqueta y StartStopcomo valor. Para obtener más información al respecto, consulte Cómo añadir, publicar y eliminar etiquetas en la documentación de Amazon RDS.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Cree un grupo de recursos para las instancias de la base de datos de Amazon RDS etiquetadas.	Abra la consola AWS Resource Groups y cree un grupo de recursos basado en la etiqueta que creó para las instancias de la base de datos de Amazon RDS. En Criterios de agrupació n, asegúrese de elegir AWS: :RDS: :DBInstance como tipo de recurso y, a continuación, proporcione el par clave-valor de la etiqueta (por ejemplo, «Action- «). StartStop Esto garantiza que el servicio solo compruebe las instancias de la base de datos de Amazon RDS y no otros recursos que tengan esta etiqueta. Asegúrese de registrar el nombre del grupo de recursos. Para obtener más información y pasos detallados, consulte Crear una consulta basada en etiquetas y crear un grupo en la documentación de AWS Resource Groups.	Administrador de AWS

Configure un período de mantenimiento para detener las instancias de la base de datos de Amazon RDS

Tarea	Descripción	Habilidades requeridas
Crear un período de mantenimiento.	1. Abra la consola de AWS Systems Manager, elija Maintenance Windows y, a continuación, elija Crear un periodo de mantenimiento. Proporcione un nombre para el período de mantenimiento (por ejemplo, «StopRdsInstancia»), introduzca una descripción y, a continuación, desactive la casilla Permitir objetivos no registrados. 2. Elija la expresión CRON/Expresión de frecuencia y proporcione la expresión de programación para definir cuándo deben detenerse las instancias de la base de datos de Amazon RDS. Introduzca 1 para la duración y 0 para dejar de iniciar las tareas. De forma predeterminada, la zona horaria muestra UTC. Puede cambiar la zona horaria para iniciar el período de mantenimiento en función de la marca	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	de tiempo definida en su expresión cron. 3. Elija Create maintenance window (Crear periodo de mantenimiento). El sistema vuelve a la página del periodo de mantenimiento y el estado del periodo de mantenimiento es Habilitado. Importante: la tarea de detener la instancia de la base de datos se ejecuta casi al instante cuando se inicia y no abarca todo el período de mantenimiento. Este patrón proporciona los valores mínimos de duración y parada de las tareas de inicio, ya que son los parámetros necesarios para un período de mantenimiento. Para obtener más información y los pasos detallados, consulte Crear un periodo mantenimiento (consola) en la documentación de AWS Systems Manager.	

Tarea	Descripción	Habilidades requeridas
Asigne un objetivo al periodo de mantenimiento.	1. En la consola de AWS Systems Manager, elija Maintenance Windows, Acciones y, a continuación, Registrar destinos. 2. En el área Objetivos , especifique Elegir un grupo de recursos y, a continuación, elija el nombre de un grupo de recursos existente en su cuenta. 3. En Tipos de recursos, elija AWS::RDS::DBInstance y, a continuación, elija Registrar destino. Para obtener más información y pasos detallados, consulte Asignar destinos a un periodo de mantenimiento (consola) en la documentación de AWS Systems Manager.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Asigne una tarea al periodo de mantenimiento.	1. En la consola de AWS Systems Manager, elija Maintenance Windows y, a continuación, elija su periodo de mantenimiento. Elija Acciones y después seleccione Registrar tarea de automatización. 2. En Document, elija AWS-StopRds Instance. 3. En la sección Destinos, elija Seleccionar grupos de destinos registrados y, a continuación, elija el destino del periodo de mantenimi ento que registró en el periodo de mantenimiento actual. 4. Para Control de velocidad , especifique el 100 % para Simultaneidad y Umbral de error. Puede cambiar los valores de Control de velocidad según sus requisitos para la simultaneidad de tareas y el umbral de error. Para obtener más informaci ón al respecto, consulte Acerca de los umbrales de error y simultaneidad en la documentación de AWS Systems Manager.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	5. En la sección Función de servicio de IAM, en Función de servicio, deje esta casilla en blanco o cree su propia función personalizada. Si deja la casilla en blanco, Systems Manager crea automáticamente la función vinculada al servicio AWSServiceRoleForAmazonSSM y, a continuación, la asocia a la tarea. Para crear su propia función personalizada, consulte Crear una función de servicio personalizada para las ventanas de mantenimiento (consola) y, a continuación, asocie esa función personalizada a la tarea. 6. En la sección Parámetros a introducir, especifique los siguientes parámetros para el manual de procedimientos: • InstanceId: `{{RESOURCE_ID}}` • AutomationAssumeFunción: proporcione el ARN de la función de servicio que creó para Systems Manager Automation.	

Tarea	Descripción	Habilidades requeridas
	• Nota: Para InstanceId, se utiliza un pseudopar ámetro para extraer el ID de recurso de base de datos de Amazon RDS del ARN. Para obtener más información sobre los pseudoparámetros, consulte Acerca de los pseudoparámetros en la documentación de AWS Systems Manager. 7. Seleccione Registrar tarea de Automation Importante: la opción Rol de servicio define el rol de servicio necesario para que el período de mantenimi ento ejecute las tareas. Sin embargo, este rol no es idéntico al rol de servicio que creó anteriormente para Systems Manager Automation. Para obtener más información y pasos detallados, consulte Asignar tareas a un período de mantenimiento (consola en la documentación de AWS Systems Manager.	

Configurar un período de mantenimiento para iniciar las instancias de la base de datos de Amazon RDS

Tarea	Descripción	Habilidades requeridas
Configure un período de mantenimiento para iniciar las instancias de la base de datos de Amazon RDS.	Repita los pasos de la épica Configurar un período de mantenimiento para detener las instancias de la base de datos de Amazon RDS y configure otro período de mantenimiento para iniciar las instancias de la base de datos de Amazon RDS a una hora programada. Importante: debe realizar los siguientes cambios al configurar el período de mantenimiento para iniciar las instancias de la base de datos: • Utilice un nombre nuevo para la ventana de mantenimiento (por ejemplo, «StartRdsInstancia»). • Sustituya la expresión cron por la expresión cron que desee utilizar para iniciar las instancias de la base de datos. • Sustituya el manual de procedimientos de `AWS-StopRdsInstance` por `AWS-StartRdsInstance` en Tarea.	Administrador de AWS

Recursos relacionados

- Utilice los documentos de automatización de Systems Manager para gestionar las instancias y reducir los costos fuera del horario laboral (entrada del blog de AWS)

Centralice la distribución de paquetes de software en AWS Organizations mediante Terraform

Creado por Pradip kumar Pandey (AWS), Aarti Rajput (AWS), Chintamani Aphale (AWS), T.V.R.L.Phani Kumar Dadi (AWS), Mayuri Shinde (AWS) y Pratap Kumar Nanda (AWS)

Entorno: producción	Tecnologías: administración y gobierno; infraestructura	Servicios de AWS: AWS Organizations; AWS Systems Manager

Resumen

Las empresas suelen mantener varias Cuentas de AWS distribuidas Regiones de AWS en varias para crear una fuerte barrera de aislamiento entre las cargas de trabajo. Para garantizar la seguridad y la conformidad, sus equipos de administración instalan herramientas basadas en agentes CrowdStrike, como, o TrendMicroherramientas para el análisis de seguridad SentinelOne, y el agente de Amazon, el CloudWatch agente de Datadog o AppDynamics los agentes para la supervisión. Estos equipos suelen enfrentarse a desafíos cuando quieren automatizar de forma centralizada la administración y distribución de paquetes de software en este amplio panorama.

Distributor, una capacidad de AWS Systems Manager, automatiza el proceso de empaquetado y publicación de software en instancias administradas de Microsoft Windows y Linux en la nube y en los servidores locales a través de una única interfaz simplificada. Este patrón demuestra cómo puede utilizar Terraform para simplificar aún más el proceso de administración de la instalación del software y ejecutar scripts en un gran número de instancias y cuentas de miembros AWS Organizations con un mínimo esfuerzo.

Esta solución funciona para instancias de Amazon, Linux y Windows administradas por Systems Manager.

Requisitos previos y limitaciones

- Un paquete de distribuidor que incluye el software que se va a instalar
- Terraform versión 0.15.0 o posterior

- Instancias de Amazon Elastic Compute Cloud (Amazon EC2) gestionadas por Systems Manager y con permisos básicos para acceder a Amazon Simple Storage Service (Amazon S3) en la cuenta de destino
- Una landing zone para tu organización que se configura mediante AWS Control Tower
- (Opcional) Account Factory para Terraform (AFT)

Arquitectura

Detalles del recurso

Este patrón usa Account Factory for Terraform (AFT) para crear todos los AWS recursos necesarios y la canalización de código para implementar los recursos en una cuenta de implementación. La canalización de código se ejecuta en dos repositorios:

- La personalización global contiene el código de Terraform que se aplicará a todas las cuentas registradas en AFT.
- Las personalizaciones de la cuenta contienen el código de Terraform que se ejecutará en la cuenta de implementación.

También puede implementar esta solución sin usar AFT, ejecutando los comandos de Terraform en la carpeta de personalizaciones de la cuenta.

El código de Terraform implementa los siguientes recursos:

- AWS Identity and Access ManagementFunción y políticas (IAM)
  - SystemsManager- AutomationExecutionRole concede al usuario permisos para ejecutar automatizaciones en las cuentas de destino.
  - SystemsManager- AutomationAdministrationRole concede al usuario permisos para ejecutar automatizaciones en varias cuentas y unidades organizativas (OU).
- Archivos comprimidos y manifest.json para el paquete
  - En Systems Manager, un paquete incluye al menos un archivo.zip de software o activos instalables.
  - El manifiesto JSON incluye punteros a los archivos de código del paquete.
- Bucket de S3
  - El paquete distribuido que se comparte en toda la organización se almacena de forma segura en un bucket de Amazon S3.

- AWS Systems Managerdocumentos (documentos SSM)
  - `DistributeSoftwarePackage`contiene la lógica para distribuir el paquete de software a todas las instancias de destino de las cuentas de los miembros.
  - `AddSoftwarePackageToDistributor`contiene la lógica para empaquetar los activos de software instalables y añadirlos a la automatización, una capacidad deAWS Systems Manager.
- Asociación de de Systems Manager
  - Se utiliza una asociación de Systems Manager para implementar la solución.

Arquitectura y flujo de trabajo

El siguiente diagrama muestra los siguientes pasos:

1. Para ejecutar la solución desde una cuenta centralizada, debe cargar sus paquetes o software junto con los pasos de implementación en un bucket de S3.
2. El paquete personalizado estará disponible en la sección Documentos de la consola de Systems Manager, en la pestaña De mi propiedad.
3. State Manager, una función de Systems Manager, crea, programa y ejecuta una asociación para el paquete en toda la organización. La asociación especifica que el paquete de software debe estar instalado y ejecutándose en un nodo administrado antes de poder instalarse en el nodo de destino.
4. La asociación indica a Systems Manager que instale el paquete en el nodo de destino.
5. Para cualquier instalación o cambio posterior, los usuarios pueden ejecutar la misma asociación de forma periódica o manual desde una única ubicación para realizar despliegues en todas las cuentas.
6. En las cuentas de los miembros, Automation envía los comandos de despliegue al distribuidor.
7. El distribuidor distribuye paquetes de software en todas las instancias.

Esta solución utiliza la cuenta de administración que AWS Organizations contiene, pero también puede designar una cuenta (administrador delegado) para que la gestione en nombre de la organización.

Herramientas

Servicios de AWS

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos. Este patrón utiliza Amazon S3 para centralizar y almacenar de forma segura el paquete distribuido.
- AWS Systems Manager lo ayuda a administrar las aplicaciones y la infraestructura que se ejecutan en la Nube de AWS. Simplifica la administración de aplicaciones y recursos, reduce el tiempo requerido para detectar y resolver problemas operativos y ayuda a utilizar y administrar los recursos de AWS a gran escala. Este patrón utiliza las siguientes funciones de Systems Manager:
  - Distributor le ayuda a empaquetar y publicar software en las instancias gestionadas por Systems Manager.
  - La automatización simplifica las tareas comunes de mantenimiento, implementación y corrección de muchos AWS servicios.
  - Documents realiza acciones en las instancias gestionadas por Systems Manager en toda la organización y las cuentas.
- AWS Organizationses un servicio de administración de cuentas que le ayuda a consolidar varias AWS cuentas en una organización que puede crear y administrar de forma centralizada.

Otras herramientas

- Terraform es una herramienta de infraestructura como código (iAC) HashiCorp que le ayuda a crear y administrar recursos locales y en la nube.

Repositorio de códigos

Las instrucciones y el código de este patrón están disponibles en el repositorio GitHub centralizado de distribución de paquetes.

Prácticas recomendadas

- Para asignar etiquetas a una asociación, utilice AWS Command Line Interface(AWS CLI) o AWS Tools for PowerShell. No se admite agregar etiquetas a una asociación mediante la consola de Systems Manager. Para obtener más información, consulte los recursos de Etiquetado de Systems Manager en la documentación de Systems Manager.
- Para ejecutar una asociación mediante una nueva versión de un documento compartido desde otra cuenta, defina `default` la versión del documento en.
- Para etiquetar solo el nodo de destino, utilice una clave de etiqueta. Si quiere segmentar sus nodos mediante varias claves de etiquetas, utilice la opción de grupo de recursos.

Epics

Configure las cuentas y los archivos fuente

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	1. Clona el repositorio GitHub centralizado de distribución de paquetes: `git clone https://github.com/aws-samples/aws-organization-centralised-package-distribution` 2. El repositorio de código de Terraform requiere dos carpetas de personalización administradas por AFT. Confirme que su copia local del repositorio contenga estas carpetas: `$ cd centralised-package-distribution` `$ ls` `global-customization account-customization`	DevOps ingeniero
Actualizar las variables globales.	Actualice los siguientes parámetros de entrada en el `global-customization/variables.tf` archivo. Estas variables se aplican a todas las cuentas creadas y administradas por AFT.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	• `account_id` : El ID de la cuenta en la que se implementará la solución de distribuidor. • `aws_region` : El Región de AWS lugar donde se implementará la asociación.	
Actualizar las variables de la cuenta.	Actualice los siguientes parámetros de entrada en el `account-customization/variables.tf` archivo. Estas variables se aplican solo a cuentas específicas que AFT crea y administra. • `package_bucket_name` : el nombre del depósito de S3 que contiene el archivo de distribución del paquete. • `package_name` : el nombre del archivo de distribución del paquete. • `package_version` : la versión del paquete del instalador.	DevOps ingeniero

Personalice los parámetros y los archivos de despliegue

Tarea	Descripción	Habilidades requeridas
Actualice los parámetros de entrada de la asociación de administradores estatales.	Actualice los siguientes parámetros de entrada en el `account-customization/association.tf` archivo para definir el estado que desea mantener en las instancias. Puede usar los valores de los parámetros predeterminados si son compatibles con su caso de uso. • `targetAccounts` : los ID de las unidades organizativas (OU) de AWS Organizations que representan las cuentas con las instancias de destino para su distribución. Los ID de OU comienzan por «ou». • `targetRegions` : El Regiones de AWS (por ejemplo, «us-east-1″ o» ap-southeast-2») donde se ejecutan las instancias de destino. • `action`: especifique si desea instalar o desinstalar el paquete. • `installationType` : Uno de los siguientes tipos de instalación:	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	• `uninstall` : El paquete está desinstalado. • `reinstall` : La aplicación se desconecta hasta que se complete el proceso de reinstalación. • `In-place update`: La aplicación está disponibl e mientras se añaden archivos nuevos o actualizados a la instalaci ón. • `name`: el nombre del paquete que se va a instalar o desinstalar. • `version`: la versión del paquete que se va a instalar o desinstalar. Si no hay ninguna versión del paquete instalada, el sistema devuelve un error. • `bucketName` : El nombre del bucket de S3 en el que se implementó el paquete. Este depósito debe estar formado únicamente por los paquetes y el archivo de manifiesto. • `bucketPrefix` : El prefijo S3 donde se almacenan los activos del paquete. • `AutomationAssumeRo le` : El nombre del recurso	

Tarea	Descripción	Habilidades requeridas
	de Amazon (ARN) de. `SystemsManager-AutomationAdministrationRole`	
Prepare los archivos comprimidos y el `manifest.json` archivo para el paquete.	Este patrón proporciona ejemplos de archivos PowerShell instalables (.msi para Windows y .rpm para Linux) con scripts de instalación y desinstalación en la carpeta. `account-customization/package` 1. Sustituya los archivos PowerShell instalables por sus propios archivos o proporcione el archivo instalable, los scripts de instalación y desinstalación y el archivo de manifiesto para crear un paquete en la carpeta de su cuenta. `account-customization` 2. Personalice el `manifest.json` archivo predeterminado que Terraform genera en la `account-customization` carpeta según sus necesidades.	DevOps ingeniero

Ejecute los comandos de Terraform para aprovisionar recursos

Tarea	Descripción	Habilidades requeridas
Inicialice la configuración de Terraform.	Para implementar la solución automáticamente con AFT, inserte el código paraAWS CodeCommit: `$ git add *` `$ git commit -m "message"` `$ git push` También puede implement ar esta solución sin usar AFT ejecutando un comando de Terraform desde la `account-customization` carpeta. Para inicializar el directori o de trabajo que contiene los archivos de Terraform, ejecute: `$ terraform init`	DevOps ingeniero
Vista previa de los cambios.	Para obtener una vista previa de los cambios que Terraform realizará en la infraestructura, ejecute el comando: `$ terraform plan` Este comando evalúa la configuración de Terraform para determinar el estado deseado de los recursos que	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	se han declarado. También compara el estado deseado con la infraestructura real que se va a aprovisionar dentro del espacio de trabajo.	
Aplicar cambios.	Ejecute el siguiente comando para implementar los cambios que realizó en los `variables.tf` archivos: `$ terraform apply`	DevOps ingeniero

Valide los recursos

Tarea	Descripción	Habilidades requeridas
Valide la creación de documentos SSM.	1. En la consola de Systems Manager, en el panel de navegación izquierdo, elija Documentos. 2. Elija la pestaña De mi propiedad. Debería ver los `AddSoftwarePackageToDistributor` paquetes `DistributeSoftwarePackage` y.	DevOps ingeniero
Valide el despliegue exitoso de las automatizaciones.	1. En la consola de Systems Manager, en el panel de navegación izquierdo, elija Automation.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	2. En la lista de ejecucion es de automatización, debería ver las `AddSoftwa rePackageToDistrib utor` implementaciones `DistributeSoftware Package` y las más recientes. 3. Elija el ID de ejecución para comprobar que se han completado correctamente.	
Valide que el paquete se haya implementado en las instancia s de cuentas de los miembros de destino.	1. En la consola de Systems Manager, en el panel de navegación, elija Run Command. 2. En el historial de comandos, verá cada invocación y su estado. 3. Elija cualquier ID de comando para ver el historial de despliegue de cada instancia de destino. 4. Elija el ID de instancia y consulte la sección de resultados para ver la distribución.	DevOps ingeniero

Solución de problemas

Problema	Solución
La asociación de administradores estatales ha fracasado o se encuentra en estado pendiente.	Consulte la información de solución de problemas en el Centro de AWS conocimiento.
No se pudo ejecutar una asociación programada.	Es posible que la especificación de programación no sea válida. Actualmente, State Manager no permite especificar meses en las expresiones cron para las asociaciones. Usa expresiones cron o rate para confirmar la programación.

Recursos relacionados

- Distribución centralizada de paquetes (GitHub repositorio)
- Account Factory para Terraform (AFT)
- Casos de uso y mejores prácticas (AWS Systems Managerdocumentación)

Configure los registros de VPC Flow para centralizarlos en todas las cuentas de AWS

Creado por Benjamin Morris (AWS) y Aman Kaur Gandhi (AWS)

Entorno: Producción	Tecnologías: gestión y gobernanza	Servicios de AWS: Amazon VPC; Amazon S3

Resumen

En una nube privada virtual (VPC) de Amazon Web Services (AWS), la característica de registros de VPC Flow puede proporcionar datos útiles para la resolución de problemas operativos y de seguridad. Sin embargo, existen limitaciones en cuanto al uso de los registros de VPC Flow en entornos multicuenta. En concreto, no se admiten los registros de flujos entre cuentas de Amazon CloudWatch Logs. En su lugar, puede centralizar los registros configurando un bucket de Amazon Simple Storage Service (Amazon S3) con la política de bucket adecuada.

Nota: Este patrón detalla los requisitos para enviar los registros de flujo a una ubicación centralizada. Sin embargo, si también desea que los registros estén disponibles localmente en las cuentas de los miembros, puede crear varios registros de flujo para cada VPC. Los usuarios que no tengan acceso a la cuenta de Log Archive pueden ver los registros de tráfico para solucionar los problemas. Como alternativa, puede configurar un registro de flujo único para cada VPC que envíe registros a CloudWatch Logs. A continuación, puede utilizar un filtro de suscripción a Amazon Data Firehose para reenviar los registros a un bucket de S3. Para obtener más información, consulte la sección Recursos relacionados.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una organización de AWS Organizations con una cuenta usada para centralizar los registros (por ejemplo, Log Archive)

Limitaciones

Si usa la clave gestionada por AWS Key Management Service (AWS KMS) `aws/s3` para cifrar su bucket central, este no recibirá los registros de otra cuenta. En su lugar, verá un error como el siguiente.

```
"Unsuccessful": [
        {
            "Error": {
                "Code": "400",
                "Message": "LogDestination: <bucketName> is undeliverable"
            },
            "ResourceId": "vpc-1234567890123456"
        }
    ]
```

Esto se debe a que las claves administradas de AWS de una cuenta no se pueden compartir entre múltiples cuentas.

Puede solucionarlo usando el cifrado administrado de Amazon S3 (SSE-S3) o una clave administrada por el cliente de AWS KMS que pueda compartir con las cuentas de los miembros.

Arquitectura

Pila de tecnología de destino

En el siguiente diagrama se implementan dos registros de flujo para cada VPC. Uno envía los registros a un grupo de CloudWatch registros local. El otro envía los registros a un bucket de S3 en una cuenta de registro centralizada. La política de bucket permite al servicio de entrega de registros escribir registros en el bucket.

Importante: comprenda los riesgos asociados a la política de bucket necesaria para esta solución. Como la entidad principal que escribe en este bucket es una entidad principal de servicio y no una entidad de AWS Identity and Access Management (IAM), la condición `aws:PrincipalOrgID` no será válida. Esto significa que, actualmente, no es posible restringir las escrituras en función de la organización matriz de la cuenta.

Para proteger el depósito, utilice un nombre de hard-to-guess depósito y trátelo como un valor confidencial que no debe exponerse fuera de la organización. Asegúrese de usar permisos con privilegio mínimo en la política del bucket y de no conceder más permisos que los de `s3:putObject` y `s3:GetBucketAcl`. Si trabaja en un entorno con un conjunto de cuentas estáticas, puede usar el efecto de denegación para bloquear el acceso excepto desde cuentas

específicas, aunque esto no es factible desde el punto de vista operativo en la mayoría de las organizaciones.

Arquitectura de destino

Automatizar y escalar

Cada VPC está configurada para enviar registros al bucket de S3 en la cuenta de registro central. Use una de las siguientes soluciones de automatización para asegurarse de que los registros de flujo estén configurados correctamente:

- AWS CloudFormation StackSets
- AWS Control Tower Account Factory para Terraform (AFT)
- Una regla de AWS Config con correcciones

Herramientas

Herramientas

- Amazon CloudWatch Logs le ayuda a centralizar los registros de todos sus sistemas, aplicaciones y servicios de AWS para que pueda supervisarlos y archivarlos de forma segura.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esta red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS. Este patrón utiliza la característica Registros de flujo de la VPC para capturar información acerca del tráfico IP entrante y saliente de las interfaces de red de en su VPC.

Prácticas recomendadas

El uso de la infraestructura como código (IaC) puede simplificar en gran medida el proceso de implementación de los registros de VPC Flow. Al resumir las definiciones de implementación de sus VPC para incluir un constructo de recursos de registro de flujo, se implementarán automáticamente VPC con registros de flujo. Esto se demuestra en la siguiente sección.

Registros de flujo centralizados

Ejemplo de sintaxis para añadir registros de flujo centralizados a un módulo de VPC en Terraform HashiCorp

Este código crea un registro de flujo que envía los registros desde una VPC a un bucket de S3 centralizado. Tenga en cuenta que este patrón no incluye la creación del bucket de S3.

Para ver las instrucciones de política de bucket recomendadas, consulte la sección de Información adicional.

```
variable "vpc_id" {
  type        = string
  description = "ID of the VPC for which you want to create a Flow Log"
}

locals {
  # For more details: https://docs.aws.amazon.com/vpc/latest/userguide/flow-
logs.html#flow-logs-custom
  custom_log_format_v5 = "$${version} $${account-id} $${interface-id} $${srcaddr} $
${dstaddr} $${srcport} $${dstport} $${protocol} $${packets} $${bytes} $${start} $${end}
 $${action} $${log-status} $${vpc-id} $${subnet-id} $${instance-id} $${tcp-flags} $
${type} $${pkt-srcaddr} $${pkt-dstaddr} $${region} $${az-id} $${sublocation-type} $
${sublocation-id} $${pkt-src-aws-service} $${pkt-dst-aws-service} $${flow-direction} $
${traffic-path}"
}

resource "aws_flow_log" "centralized" {
  log_destination      = "arn:aws:s3:::centralized-vpc-flow-logs-
<log_archive_account_id>" # Optionally, a prefix can be added after the ARN.
  log_destination_type = "s3"
  traffic_type         = "ALL"
  vpc_id               = var.vpc_id
  log_format           = local.custom_log_format_v5 # If you want fields from VPC Flow
 Logs v3+, you will need to create a custom log format.
  tags                 = {
    Name = "centralized_flow_log"
  }
}
```

Registros de flujo locales

Ejemplo de sintaxis para añadir registros de flujo locales a un módulo de VPC en Terraform con los permisos necesarios

Este código crea un registro de flujo que envía registros desde una VPC a un grupo de CloudWatch registros local.

```
data "aws_region" "current" {}

variable "vpc_id" {
  type        = string
  description = "ID of the VPC for which you want to create a Flow Log"
}

resource "aws_iam_role" "local_flow_log_role" {
  name = "flow-logs-policy-${var.vpc_id
}"

  assume_role_policy = <<EOF
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "vpc-flow-logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
EOF
}

resource "aws_iam_role_policy" "logs_permissions" {
  name = "flow-logs-policy-${var.vpc_id}"
  role = aws_iam_role.local_flow_log_role.id

  policy = <<EOF
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:logs:${data.aws_region.current.name}:*:log-group:vpc-flow-
logs*"
    }
  ]
}
EOF
}

resource "aws_cloudwatch_log_group" "local_flow_logs" {
  # checkov:skip=CKV_AWS_338:local retention is set to 30, centralized S3 bucket can
 retain for long-term
  name              = "vpc-flow-logs/${var.vpc_id}"
  retention_in_days = 30
}

resource "aws_flow_log" "local" {
  iam_role_arn    = aws_iam_role.local_flow_log_role.arn
  log_destination = aws_cloudwatch_log_group.local_flow_logs.arn
  traffic_type    = "ALL"
  vpc_id          = var.vpc_id
  tags            = {
    Name = "local_flow_log"
  }
}
```

Epics

Implemente la infraestructura de registros de VPC Flow

Tarea	Descripción	Habilidades requeridas
Determine la estrategia de cifrado y cree la política para el bucket de S3 central.	El bucket central no admite la clave de AWS KMS `aws/s3`, por lo que deberá usar SSE-S3 o una clave administrada por el cliente de AWS KMS. Si usa una clave de AWS KMS, la política de claves debe permitir a las cuentas de los miembros usar la clave.	Conformidad
Cree el bucket de registro de flujo central.	Cree el bucket central al que se enviarán los registros de flujo y aplique la estrategia de cifrado que eligió en el paso anterior. Debe estar en un archivo de registro o en una cuenta con un propósito similar. Consulte la política de bucket en la sección de Información adicional y aplíquela a su bucket central después de actualizar los marcadores de posición con los valores específicos de su entorno.	AWS general
Configure los registros de VPC Flow para enviar los registros al bucket de registros de flujo central.	Agregue registros de flujo a cada VPC de la que desee recopilar datos. La forma más escalable de hacerlo es usar herramientas de IaC,	Administrador de red

Tarea	Descripción	Habilidades requeridas
	como AFT o AWS Cloud Development Kit (AWS CDK). Por ejemplo, puede crear un módulo Terraform que despliegue una VPC junto con un registro de flujo. Si es necesario, añada los registros de flujo manualmente.	
Configure los registros de flujo de VPC para enviarlos a los registros locales CloudWatch .	(Opcional) Si quieres que los registros de flujo estén visibles en las cuentas en las que se generan los registros, crea otro registro de flujo para enviar datos a los CloudWatch registros de la cuenta local. Como alternativa, puede enviar los datos a un bucket de S3 específico de la cuenta en la cuenta local.	AWS general

Recursos relacionados

- Cómo facilitar el análisis de datos y cumplir los requisitos de seguridad usando datos de registro de flujo centralizados (publicación del blog)
- Cómo habilitar automáticamente los registros de VPC Flow mediante reglas de AWS Config (publicación del blog)

Información adicional

Política de bucket

Este ejemplo de política de bucket se puede aplicar a su bucket central de S3 para los registros de flujo después de añadir valores en los nombres de los marcadores de posición.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::<BUCKET_NAME>/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::<BUCKET_NAME>"
        },
        {
            "Sid": "DenyUnencryptedTraffic",
            "Effect": "Deny",
            "Principal": {
                "AWS": "*"
            },
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::<BUCKET_NAME>/*",
                "arn:aws:s3:::<BUCKET_NAME>"
            ],
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
        }
```

```
    ]
}
```

Si tiene una lista estática de cuentas, puede agregar la siguiente instrucción para denegar cualquier cuenta que no esté incluida en esa lista.

```
{
    "Sid": "AccountDenyList",
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:PutObject",
    "NotResource": [
        "arn:aws:s3:::<BUCKET_NAME>/<OPTIONAL_PREFIX>/AWSLogs/<ACCOUNT_ID1>/*",
        "arn:aws:s3:::<BUCKET_NAME>/<OPTIONAL_PREFIX>/AWSLogs/<ACCOUNT_ID2>/*",
        "arn:aws:s3:::<BUCKET_NAME>/<OPTIONAL_PREFIX>/AWSLogs/<ACCOUNT_ID3>/*",
    ]
}
```

Como alternativa al anterior patrón `NotResource`-`Deny`, puede añadir condiciones a cada una de sus instrucciones `Allow` para especificar las cuentas aprobadas.

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": [
            "111111111111",
            "222222222222"
        ]
    }
}
```

Cómo añadir un prefijo

También puede restringir las escrituras a un prefijo conocido del bucket si le preocupa que se produzcan escrituras externas no deseadas en el bucket en caso de que su nombre quedara expuesto públicamente. Si lo implementa, actualice el `log_destination` en el recurso `aws_flow_log` para incluir el prefijo que sigue al nombre de recurso de Amazon (ARN) del bucket. Por ejemplo, la siguiente instrucción restringe las escrituras a un prefijo específico.

```
{
    "Sid": "PrefixAllowList",
    "Effect": "Deny",
```

```
    "Principal": "*",
    "Action": "s3:PutObject",
    "NotResource": [
        "arn:aws:s3:::<BUCKET_NAME>/<PREFIX>/*"
    ]
}
```

Configure el registro para aplicaciones.NET en Amazon CloudWatch Logs mediante nLog

Creado por Bibhuti Sahu (AWS) y Rob Hill (AWS) (AWS)

Entorno: producción	Tecnologías: gestión y gobierno DevOps; aplicaciones web y móviles	Carga de trabajo: Microsoft
Servicios de AWS: Amazon CloudWatch Logs		

Resumen

Este patrón describe cómo utilizar el marco de registro de código abierto NLog para registrar el uso y los eventos de las aplicaciones.NET en Amazon CloudWatch Logs. En la CloudWatch consola, puede ver los mensajes de registro de la aplicación prácticamente en tiempo real. También puede configurar métricas y alarmas para recibir notificaciones en caso de que se superen los umbrales de métrica. Con CloudWatch Application Insights, puede ver paneles automatizados o personalizados que muestran los posibles problemas de las aplicaciones monitoreadas. CloudWatch Application Insights está diseñado para ayudarlo a identificar rápidamente los problemas actuales de sus aplicaciones e infraestructura.

Para escribir mensajes de registro en CloudWatch Logs, agregue el `AWS.Logger.NLog` NuGet paquete al proyecto.NET. A continuación, actualiza el `NLog.config` archivo para usar CloudWatch Logs como destino.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una aplicación web o de consola .NET que:
  - Use versiones compatibles de .NET Framework o .NET Core. Para obtener más información, consulte Versiones de producto.
  - Use NLog para enviar datos de registro a Application Insights.

- Permisos para crear un rol de IAM para un servicio de AWS. Para obtener más información, consulte Permisos de roles de servicios.
- Permisos para transferir un rol a un servicio de AWS. Para obtener más información, consulte Concesión de permisos a un usuario para transferir un rol a un servicio de AWS.

Versiones de producto

- .NET Framework versión 3.5 o posterior
- .NET Core versiones 1.0.1, 2.0.0 o posterior

Arquitectura

Pila de tecnología de destino

- NLog
- Amazon CloudWatch Logs

Arquitectura de destino

1. La aplicación .NET escribe los datos de registro en el marco de registro NLog.
2. NLog escribe los datos de registro en Logs. CloudWatch
3. Se utilizan CloudWatch alarmas y paneles personalizados para supervisar la aplicación.NET.

Herramientas

Servicios de AWS

- Amazon CloudWatch Application Insights le ayuda a observar el estado de sus aplicaciones y los recursos de AWS subyacentes.
- Amazon CloudWatch Logs le ayuda a centralizar los registros de todos sus sistemas, aplicaciones y servicios de AWS para que pueda supervisarlos y archivarlos de forma segura.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.

- Las herramientas de AWS PowerShell son un conjunto de PowerShell módulos que le ayudan a programar operaciones en sus recursos de AWS desde la línea de PowerShell comandos.

Otras herramientas

- Logger.nlog es un objetivo de NLog que registra los datos de registro en Logs. CloudWatch
- NLog es un marco de registro de código abierto para plataformas .NET que le permite escribir datos de registro en los destinos, como bases de datos, archivos de registro o consolas.
- PowerShelles un programa de administración de automatización y configuración de Microsoft que se ejecuta en Windows, Linux y macOS.
- Visual Studio es un entorno de desarrollo integrado (IDE) que incluye compiladores, herramientas de finalización de código, diseñadores gráficos y otras características que facilitan el desarrollo de software.

Prácticas recomendadas

- Establezca una política de retención para el grupo de registro de destino. Esto debe hacerse fuera de la configuración de NLog. De forma predeterminada, los datos de registro se almacenan en CloudWatch los registros de forma indefinida.
- Respete las Prácticas recomendadas para administrar las claves de acceso de AWS.

Epics

Configure el acceso y las herramientas

Tarea	Descripción	Habilidades requeridas
Cree una política de IAM.	Siga las instrucciones indicadas en Crear políticas mediante el editor JSON, en la documentación de IAM. Introduce la siguiente política de JSON, que tiene los permisos de privilegios mínimos necesarios para	Administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	permitir que CloudWatch Logs lea y escriba registros. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "logs:CreateLogGroup", "logs:CreateLogStream", "logs:GetLogEvents", "logs:PutLogEvents", "logs:DescribeLogGroups", "logs:DescribeLogStreams", "logs:PutRetentionPolicy" ], "Resource": [ "*" ] } ] }`	

Tarea	Descripción	Habilidades requeridas
Crear un rol de IAM.	Para obtener instrucciones, consulte Creating a Role to Delegate Permissions to an AWS Service en la documentación de IAM. Seleccione la política que creó previamente. Esta es la función que asume CloudWatch Logs para realizar las acciones de registro.	Administrador de AWS, AWS DevOps
Configure las herramientas de AWS para PowerShell.	1. Siga las instrucciones para su sistema operativo que aparecen en Instalación de las herramientas de AWS para PowerShell. 2. Utilice las herramientas de AWS para PowerShell cmdlets para almacenar la clave de acceso y la clave secreta en un perfil. Para obtener instrucciones, consulte Administración de perfiles en las herramientas de AWS para ver PowerShell la documentación.	AWS general

Configure NLog

Tarea	Descripción	Habilidades requeridas
Instale el NuGet paquete.	1. En Visual Studio, seleccione Archivo y, a continuac	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	ión, elija Abrir un proyecto o solución. 2. Seleccione el proyecto en el que desea instalar NLog. 3. En Visual Studio, elija Tools, NuGet Package Manager, Package Manager Console. 4. Instale el `AWS.Logger.NLog` NuGet paquete introduciendo el siguiente comando. `Install-Package AWS.Logger.NLog -Version 3.1.0`	

Tarea	Descripción	Habilidades requeridas
Configure el destino de registro.	1. Abra el archivo `NLog.config` . 2. Para el destino `type`, introduzca `AWSTarget` . 3. Para el destino `logGroup`, escriba el nombre del grupo de registro que desea usar. Si el grupo de registro no existe aún, se creará automáticamente un nuevo grupo de registro con el nombre proporcionado. 4. Para el destino`region`, introduzca la región de AWS en la que está configurado CloudWatch Logs. 5. Para el destino `profile`, introduzca el nombre del perfil que creó anteriorm ente para almacenar la clave de acceso y la clave secreta. 6. Guarde y cierre el archivo `NLog.config` . Para obtener una copia de este archivo de configuración, consulte la sección Informaci ón adicional de este patrón. Cuando ejecute la aplicación, NLog escribirá los mensajes	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	de registro y los enviará a CloudWatch Logs.	

Valide y supervise los registros

Tarea	Descripción	Habilidades requeridas
Valide el registro.	Siga las instrucciones de la documentación sobre cómo ver los datos de registro enviados a CloudWatch CloudWatch Logs. Compruebe que los eventos de registro de la aplicación .NET se estén registrando. Si no constan eventos de registro, consulte la sección Solución de problemas de este patrón.	AWS general
Supervise la pila de la aplicación .NET.	Configure la supervisión CloudWatch según sea necesario para su caso de uso. Puede utilizar CloudWatch Logs Insights, CloudWatch Metrics Insights y CloudWatch Application Insights para supervisar su carga de trabajo de.NET. También puede configurar alarmas para recibir alertas y crear un panel personalizado para supervisar la carga de trabajo desde una vista única.	AWS general

Solución de problemas

Problema	Solución
Los datos de registro no aparecen en CloudWatch los registros.	Asegúrese de que la política de IAM esté asociada a la función de IAM que asume CloudWatch Logs. Para obtener más instrucciones, consulte la sección Configurar el acceso y las herramientas de la sección Épica.

Recursos relacionados

- Trabajar con grupos de registros y flujos de CloudWatch registros (documentación de registros)
- Amazon CloudWatch Logs y .NET Logging Frameworks (entrada del blog de AWS)

Información adicional

A continuación se muestra un archivo de muestra `NLog.config`.

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <configSections>
    <section name="nlog" type="NLog.Config.ConfigSectionHandler, NLog" />
  </configSections>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.7.2" />
  </startup>
  <nlog>
    <extensions>
      <add assembly="NLog.AWS.Logger" />
    </extensions>
    <targets>
      <target name="aws" type="AWSTarget" logGroup="NLog.TestGroup" region="us-east-1"
 profile="demo"/>
    </targets>
    <rules>
      <logger name="*" minlevel="Info" writeTo="aws" />
    </rules>
  </nlog>
```

```
</configuration>
```

Copiar los productos de AWS Service Catalog en diferentes cuentas y regiones de AWS

Creado por Sachin Vighe (AWS) y Santosh Kale (AWS)

Entorno: producción	Tecnologías: administración y gobierno; sin servidor	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: AWS Service Catalog; AWS Lambda		

Resumen

AWS Service Catalog es un servicio regional, lo que significa que las carteras y los productos de AWS Service Catalog solo están visibles en la región de AWS en la que se crearon. Si configura un centro de AWS Service Catalog en una nueva región, debe volver a crear sus productos existentes, lo que puede llevar mucho tiempo.

El enfoque de este patrón ayuda a simplificar este proceso al describir cómo copiar productos de un centro de AWS Service Catalog de una cuenta o región de AWS de origen a un nuevo centro de una cuenta o región de destino. Para obtener más información sobre el modelo hub and spoke de AWS Service Catalog, consulte AWS Service Catalog hub and spoke model: How to automate the deployment and management of AWS Service Catalog to many accounts en el blog AWS Management and Governance.

El patrón también proporciona los paquetes de códigos independientes necesarios para copiar los productos de AWS Service Catalog entre cuentas o a otras regiones. Al utilizar este patrón, su organización puede ahorrar tiempo, hacer que las versiones actuales y anteriores del producto estén disponibles en un nuevo centro de AWS Service Catalog, minimizar el riesgo de errores manuales y escalar el enfoque a varias cuentas o regiones.

Nota: la sección Epics de este patrón ofrece dos opciones para copiar productos. Puedes usar la opción 1 para copiar productos entre cuentas o elegir la opción 2 para copiar productos entre regiones.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Productos de AWS Service Catalog existentes en una cuenta o región de origen.
- Un centro de AWS Service Catalog existente en una cuenta o región de destino.
- Si desea copiar productos entre cuentas, debe compartir e importar la cartera de AWS Service Catalog que contiene los productos a su cuenta de destino. Para obtener más información al respecto, consulte Compartir e importar carteras en la documentación del AWS Service Catalog.

Limitaciones

- Los productos de AWS Service Catalog que desee copiar entre regiones o cuentas no pueden pertenecer a más de una cartera.

Arquitectura

En el siguiente diagrama se muestra la copia de los productos de AWS Service Catalog de una cuenta de origen a una cuenta de destino.

El siguiente diagrama muestra la copia de productos de AWS Service Catalog de una región de origen a una región de destino.

Pila de tecnología

- Amazon CloudWatch
- AWS Identity y Access Management (IAM)
- AWS Lambda
- AWS Service Catalog

Automatizar y escalar

Puede escalar el enfoque de este patrón mediante una función de Lambda que se puede escalar en función del número de solicitudes recibidas o del número de productos de AWS Service Catalog que necesite copiar. Para obtener más información al respecto, consulte el escalado de funciones de Lambda en la documentación de AWS Lambda.

Herramientas

- La Interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que permite interactuar con los servicios de AWS mediante comandos en el intérprete de comandos de línea de comandos.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Service Catalog le ayuda a administrar de forma centralizada los catálogos de servicios de TI aprobados para AWS. Los usuarios finales pueden implementar rápidamente solo los servicios de TI aprobados que necesitan, de acuerdo con las limitaciones establecidas por su organización.

Código

Puede usar el paquete (adjunto) `cross-account-copy` para copiar los productos de AWS Service Catalog entre cuentas o el paquete (adjunto) `cross-region-copy` para copiar productos entre regiones.

El paquete `cross-account-copy` contiene los siguientes archivos:

- `copyconf.properties`: el archivo de configuración que contiene los parámetros de región e ID de cuenta de AWS para copiar productos entre cuentas.
- `scProductCopyLambda.py`: la función de Python para copiar productos entre cuentas.
- `createDestAccountRole.sh`: el script para crear un rol de IAM en la cuenta de destino.
- `createSrcAccountRole.sh`: el script para crear un rol de IAM en la cuenta de origen.
- `copyProduct.sh`: el script para crear e invocar la función de Lambda para copiar productos entre cuentas.

El paquete `cross-region-copy` contiene los siguientes archivos:

- `copyconf.properties`: el archivo de configuración que contiene los parámetros de región e ID de cuenta de AWS para copiar productos entre regiones.
- `scProductCopyLambda.py`: la función Python para copiar productos entre regiones.
- `copyProduct.sh`: el script para crear un rol de IAM y crear e invocar la función de Lambda para copiar productos entre regiones.

Epics

Opción 1: copiar los productos de AWS Service Catalog en todas las cuentas

Tarea	Descripción	Habilidades requeridas
Actualizar el archivo de configuración.	1. Descargue el paquete (adjunto) `cross-account-copy` en su máquina local. 2. Actualice el archivo de `copyconf.properties` configuración con los siguientes valores: • `srcRegion` : proporcione la región de origen que contiene los productos. • `destRegion` : indique la región de destino de los productos. • `sourceAccountId` : proporcione el ID de cuenta de AWS de su cuenta de origen. • `destAccountId` : proporcione el ID de	Administrador de AWS, administrador de sistemas de AWS, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	cuenta de AWS de su cuenta de destino.	
Configure sus credenciales para la AWS CLI en la cuenta de destino.	Configure sus credencia les para acceder a la AWS CLI en su cuenta de destino ejecutando el `aws configure` comando y proporcionando los siguientes valores: `$aws configure` `AWS Access Key ID [None]: <your_access_key_id>` `AWS Secret Access Key [None]: <your_secret_access_key>` `Default region name [None]: Region` `Default output format [None]:` Para obtener más informaci ón al respecto, consulte Conceptos básicos de configuración en la interfaz de línea de comandos de AWS.	Administrador de AWS, administrador de sistemas de AWS, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Configure sus credenciales para la AWS CLI en la cuenta de origen.	Configure sus credencia les para acceder a la AWS CLI en su cuenta de origen ejecutando el comando `aws configure` y proporcio nando los siguientes valores: `$aws configure` `AWS Access Key ID [None]: <your_access_key_id>` `AWS Secret Access Key [None]: <your_secret_access_key>` `Default region name [None]: Region` `Default output format [None]:` Para obtener más informaci ón al respecto, consulte Conceptos básicos de configuración en la interfaz de línea de comandos de AWS.	Administrador de AWS, administrador de sistemas de AWS, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Cree un rol de ejecución para Lambda en su cuenta de destino.	Ejecute el script `createDestAccountRole.sh` en su cuenta de destino. El script implementa las siguientes acciones: • Crea un rol de ejecución para Lambda en la cuenta de destino • Crea y adjunta la política de IAM para la función de ejecución de Lambda	Administrador de AWS, administrador de sistemas de AWS, administrador de la nube
Cree el rol de IAM multicuenta en su cuenta de origen.	Ejecute el script `createSrcAccountRole.sh` en su cuenta de origen. El script implementa las siguientes acciones: • Crea una función de IAM multicuenta en la cuenta de origen que asume la función de ejecución de Lambda en la cuenta de destino para copiar productos • Crea y adjunta una política de IAM para la función multicuenta en su cuenta de origen	Administrador de AWS, administrador de sistemas de AWS, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Ejecute el script CopyProduct en la cuenta de destino.	Ejecute el script `copyProduct.sh` en su cuenta de destino. El script implementa las siguientes acciones: • Crea e invoca la función de Lambda para copiar productos de la cuenta de origen a la cuenta de destino	Administrador de AWS, administrador de sistemas de AWS, administrador de la nube

Opción 2: copiar los productos de AWS Service Catalog de una región de origen a una región de destino

Tarea	Descripción	Habilidades requeridas
Actualizar el archivo de configuración.	1. Descargue el paquete (adjunto) `cross-region-copy` en su máquina local. 2. Actualice el archivo de `copyconf.properties` configuración con los siguientes valores: • `srcRegion` : proporcione la región de origen que contiene los productos. • `destRegion` : indique la región de destino de los productos.	Administrador de sistemas de AWS, administrador de la nube, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	• `accountId` : proporcione su ID de cuenta de AWS.	
Configurar la CLI con sus credenciales de AWS.	Configure sus credenciales para acceder a la AWS CLI en su entorno ejecutando el comando `aws configure` y proporcionando los siguientes valores: `$aws configure` `AWS Access Key ID [None]: <your_access_key_id>` `AWS Secret Access Key [None]: <your_secret_access_key>` `Default region name [None]: Region` `Default output format [None]:` Para obtener más información al respecto, consulte Conceptos básicos de configuración en la interfaz de línea de comandos de AWS.	Administrador de AWS, administrador de sistemas de AWS, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Ejecute el script CopyProduct.	Ejecute el script `copyProduct.sh` en la región de destino. El script implementa las siguientes acciones: • Crear un rol de ejecución para Lambda • Crea y adjunta la política de IAM para la función de ejecución de Lambda • Crea e invoca la función de Lambda para copiar productos de la región de origen a la región de destino	Administrador de AWS, administrador de sistemas de AWS, administrador de la nube

Recursos relacionados

- Crear un rol de ejecución para Lambda (documentación de AWS Lambda)
- Crear una función de Lambda (documentación de AWS Lambda)
- AWS Service Catalog referencia API
- Documentación de AWS Service Catalog

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Cree alarmas para métricas personalizadas mediante la detección de CloudWatch anomalías de Amazon

Creado por Ram Kandaswamy (AWS) y Raheem Jiwani (AWS)

Entorno: producción	Tecnologías: gestión y gobierno; operaciones; DevOps nativas de la nube	Servicios de AWS: Amazon CloudWatch

Resumen

En la nube de Amazon Web Services (AWS), puede utilizar Amazon CloudWatch para crear alarmas que supervisen las métricas y envíen notificaciones o para realizar cambios automáticamente si se supera un umbral.

Para evitar verse limitado por umbrales estáticos, puede crear alarmas basadas en patrones anteriores y que lo notifiquen si determinadas métricas están fuera del intervalo operativo normal. Por ejemplo, puede supervisar los tiempos de respuesta de su API desde Amazon API Gateway y recibir notificaciones sobre anomalías que le impidan cumplir un acuerdo de nivel de servicio (SLA).

Este patrón describe cómo utilizar la detección de CloudWatch anomalías para las métricas personalizadas. El patrón le muestra cómo crear una métrica personalizada en Amazon CloudWatch Logs Insights o publicar una métrica personalizada con una función de AWS Lambda y, a continuación, configurar la detección de anomalías y crear notificaciones mediante Amazon Simple Notification Service (Amazon SNS).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Un tema de SNS existente, configurado para enviar notificaciones por correo electrónico. Para obtener más información al respecto, consulte Introducción a Amazon SNS en la documentación de Amazon SNS.
- Una aplicación existente, configurada con Logs. CloudWatch

Limitaciones

- CloudWatch las métricas no admiten intervalos de milisegundos. Para obtener más información sobre la granularidad de las métricas normales y personalizadas, consulta las CloudWatch preguntas frecuentes de Amazon.

Arquitectura

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Los registros que utilizan métricas creadas y actualizadas por CloudWatch Logs se transmiten a. CloudWatch
2. Se inicia una alarma en función de los umbrales y envía una alerta a un tema de SNS.
3. Amazon SNS le enviará una notificación por correo electrónico.

Pila de tecnología

- CloudWatch
- AWS Lambda
- Amazon SNS

Herramientas

- Amazon Cloudwatch: CloudWatch proporciona una solución de supervisión fiable, escalable y flexible.
- AWS Lambda: Lambda es un servicio informático que facilita poder ejecutar código sin aprovisionar ni administrar servidores.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) es un servicio administrado que proporciona la entrega de mensajes de los publicadores a los suscriptores.

Epics

Configurar la detección de anomalías para una métrica personalizada

Tarea	Descripción	Habilidades requeridas
Opción 1: Crear una métrica personalizada con una función de Lambda.	Descargue el `lambda_function.py` archivo (adjunto) y, a continuación, sustituya el `lambda_function.py` archivo de muestra del aws-lambda-developer-guiderepositorio en la documentación de AWS GitHub. Esto le proporciona un ejemplo de función Lambda que envía métricas personalizadas a CloudWatch Logs. La función Lambda utiliza la API Boto3 para integrarse con. CloudWatch Tras ejecutar la función Lambda, puede iniciar sesión en la consola de administración de AWS, abrir la CloudWatch consola y la métrica publicada estará disponible en su espacio de nombres publicado.	DevOps ingeniero, AWS DevOps
Opción 2: crear métricas personalizadas a partir de grupos de CloudWatch registros.	Inicie sesión en la consola de administración de AWS, abra la CloudWatch consola y, a continuación, seleccione Grupos de registro. Seleccion	DevOps ingeniero, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	e el grupo de registro para el que desea crear una métrica. Elija Acciones y, a continuac ión, seleccione Crear filtro de métrica. Para Patrón de filtro, introduzca el patrón de filtro que desea utilizar. Para obtener más información, consulte la sintaxis de filtros y patrones en la CloudWatch documentación. Para probar su patrón de filtro, ingrese uno o más eventos de registro en Probar patrón. Cada evento de registro debe estar dentro de una línea, ya que los saltos de línea se utilizan para separar los eventos de registro en el cuadro de Log event messages (Mensajes de eventos de registro). Tras probar el patrón, puede introducir un nombre y un valor para la métrica en Detalles de la métrica. Para obtener más informaci ón y los pasos para crear una métrica personalizada, consulte Crear un filtro de métrica para un grupo de	

Tarea	Descripción	Habilidades requeridas
	registros en la CloudWatch documentación.	
Cree una alarma para su métrica personalizada.	En la CloudWatch consola, selecciona Alarmas y, a continuación, selecciona Crear alarma. Seleccione Seleccionar métrica e introduzca el nombre de la métrica que creó anteriormente en el cuadro de búsqueda. Seleccione la pestaña Métricas graficadas y configure las opciones según sus necesidades. En Condiciones, seleccione Detección de anomalías en lugar de Umbrales estáticos. Esto le muestra una banda basada en dos desviaciones estándar predeterminadas. Puede configurar umbrales y ajustarlos según sus necesidades. Elija Siguiente. Nota: La banda es dinámica y depende de la calidad de los puntos de datos. Cuando comience a agregar más datos, la banda y los umbrales se actualizan automáticamente.	DevOps ingeniero, AWS DevOps

Tarea	Descripción	Habilidades requeridas
Configurar notificaciones de SNS.	En Notificación, elija el tema de SNS al que desee enviar la notificación cuando la alarma tenga el estado `ALARM`, `OK` o `INSUFFICIENT_DATA` . Para que la alarma envíe varias notificaciones para el mismo estado de alarma o para estados de alarma diferentes, seleccione Add notificación (Añadir notificac ión). Elija Siguiente. Escriba un nombre y la descripción de la alarma. El nombre solo debe contener caracteres ASCII. A continuación, elija Siguiente. En Obtener vista previa y crear, confirme que la información y las condiciones son las correctas y luego, elija Crear alarma.	DevOps ingeniero, AWS DevOps

Recursos relacionados

- Publicar métricas personalizadas en CloudWatch
- Uso de la detección de CloudWatch anomalías
- Eventos de alarma y Amazon EventBridge
- ¿Cuáles son las mejores prácticas que se deben seguir a la hora de introducir métricas personalizadas en Cloud Watch? (video)
- Introducción a CloudWatch Application Insights (vídeo)

- Detecte anomalías con CloudWatch (vídeo)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Documente el diseño de su zona de aterrizaje de AWS

Creado por Michael Daehnert (AWS), Florian Langer (AWS) y Michael Lodemann (AWS)

Entorno: producción	Tecnologías: administración y gobierno; infraestructura; seguridad, identidad y conformidad	Servicios de AWS: AWS Control Tower

Resumen

Una landing zone es un entorno de múltiples cuentas bien diseñado que se basa en las mejores prácticas de seguridad y cumplimiento. Es el contenedor para toda la empresa que contiene todas las unidades organizativas (OU) Cuentas de AWS, los usuarios y otros recursos. Una landing zone puede ampliarse para adaptarse a las necesidades de una empresa de cualquier tamaño. AWS tiene dos opciones para crear tu landing zone: una landing zone basada en servicios AWS Control Towero una landing zone personalizada que tú construyas. Cada opción requiere un nivel de AWS conocimiento diferente.

AWS creado AWS Control Tower para ayudarte a ahorrar tiempo mediante la automatización de la configuración de una landing zone. AWS Control Tower está gestionado por AWS las mejores prácticas y directrices, y las utiliza para ayudarle a crear su entorno fundamental. AWS Control Tower utiliza servicios integrados, como AWS Service Catalogy AWS Organizations, para aprovisionar cuentas en tu landing zone y gestionar el acceso a esas cuentas.

AWS Los proyectos de landing zone varían en cuanto a los requisitos, los detalles de implementación y los elementos de acción operativa. Hay aspectos de personalización que deben abordarse con cada implementación de landing zone. Esto incluye (pero no se limita a) cómo se gestiona la gestión del acceso, qué tecnología se utiliza y cuáles son los requisitos de supervisión para lograr la excelencia operativa. Este patrón proporciona una plantilla que te ayuda a documentar tu proyecto de landing zone. Al usar la plantilla, puedes documentar tu proyecto más rápidamente y ayudar a tus equipos de desarrollo y operaciones a entender tu landing zone.

Requisitos previos y limitaciones

Limitaciones

Este patrón no describe qué es una landing zone ni cómo implementarla. Para obtener más información sobre estos temas, consulte la sección de recursos relacionados.

Epics

Cree el documento de diseño

Tarea	Descripción	Habilidades requeridas
Identifique a las partes interesadas principales.	Identifica a los principales administradores de servicios y equipos que están vinculados a tu landing zone.	Administrador de proyectos
Personaliza la plantilla.	Descarga la plantilla en la sección de adjuntos y, a continuación, actualiza la plantilla de la siguiente manera: 1. Elimina todas las secciones que no se apliquen a la landing zone o a los procesos de tu organizac ión. 2. Agrega todas las secciones que sean exclusivas de tu organización.	Administrador de proyectos
Complete la plantilla.	En las reuniones con las partes interesadas o mediante un write-and-review proceso, complete la plantilla de la siguiente manera: 1. Utilice las instrucciones y la información de los	Administrador de proyectos

Tarea	Descripción	Habilidades requeridas
	recuadros azules para completar cada sección. 2. Sustituya o elimine los campos amarillos por valores personalizados para su organización. 3. Sustituya o elimine cualquier campo de imagen por su arquitectura o diagrama de flujo personalizados. 4. Complete la sección Historial de revisiones y colaboradores de la plantilla .	
Comparta el documento de diseño.	Cuando la documentación de diseño de tu landing zone esté completa, guárdala en un repositorio compartido o en una ubicación central donde todas las partes interesadas puedan acceder a ella. Le recomendamos que utilice procesos de control de documentos estándar para registrar y aprobar las revisiones del documento de diseño.	Administrador de proyectos

Recursos relacionados

- AWS Control Tower documentación
  - Planifica tu AWS Control Tower landing zone

  - AWS estrategia multicuenta para tu AWS Control Tower landing zone
  - Consejos administrativos para la configuración de la landing zone
  - Expectativas para la configuración de la zona de aterrizaje
- Personalizaciones para AWS Control Tower (biblioteca de AWS soluciones)
- Configuración de un entorno multicuenta seguro y escalable (AWS guíaAWS prescriptiva)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Configure la detección de CloudFormation desviaciones de AWS en una organización multirregional y multicuenta

Entorno: producción	Tecnologías: gestión y gobernanza; nativas en la nube; infraestructura; operaciones; modernización	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon SNS; AWS Config; AWS Lambda; AWS CloudFormation		

Resumen

Los clientes de Amazon Web Services (AWS) suelen buscar una forma eficaz de detectar los desajustes en la configuración de los recursos, incluida la desviación en las CloudFormation pilas de AWS, y solucionarlos lo antes posible. Este es especialmente el caso cuando se utilizan soluciones de AWS Control Tower o AWS Landing Zone.

Este patrón proporciona una solución prescriptiva que resuelve el problema de manera eficiente mediante el uso de cambios consolidados en la configuración de los recursos y la adopción de medidas en función de esos cambios para generar resultados. La solución está diseñada para situaciones en las que se crean varias CloudFormation pilas en más de una región, en más de una cuenta o en una combinación de ambas. Los objetivos de la solución son los siguientes:

- Simplificar el proceso de detección de desviaciones
- Configurar las notificaciones y las alertas
- Configurar los informes consolidados

Requisitos previos y limitaciones

Requisitos previos

- AWS Config está habilitado en todas las regiones y cuentas que deben supervisarse

Limitaciones

- El informe generado solo admite los formatos de salida .csv o .json.

Arquitectura

Pila de tecnología de destino

La guía actual ayudará a las organizaciones a alcanzar el objetivo mediante el uso de una combinación de los siguientes servicios:

- Regla de AWS Config
- CloudWatch Regla de Amazon
- AWS Identity y Access Management (IAM)
- AWS Lambda
- Amazon Simple Notification Service (Amazon SNS)

1. La regla AWS Config detecta desviaciones.
2. Los resultados de la detección de desviaciones en otras cuentas se envían a la cuenta de administración.
3. La CloudWatch regla llama Lambda.
4. Lambda consulta la regla de AWS Config para obtener resultados agregados.
5. Lambda notifica la desviación a Amazon SNS, que envía una notificación por correo electrónico.

Automatizar y escalar

La solución que se presenta aquí puede escalarse tanto para regiones como para cuentas adicionales.

Herramientas

AWS Config: AWS Config proporciona una visión detallada de la configuración de los recursos de AWS de su cuenta de AWS. Esto incluye cómo se relacionan los recursos entre sí y cómo se han configurado en el pasado, para que pueda ver cómo las configuraciones y las relaciones cambian

a lo largo del tiempo. Con AWS Config puede evaluar, auditar y evaluar las configuraciones de sus recursos de AWS.

Amazon CloudWatch: Amazon CloudWatch monitorea los recursos de AWS y las aplicaciones que ejecuta en AWS en tiempo real. Puede utilizarlas CloudWatch para recopilar y realizar un seguimiento de las métricas, que son variables que puede medir para sus recursos y aplicaciones.

AWS Lambda: AWS Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo. Solo pagará por el tiempo de computación que consuma, no se aplican cargos cuando el código no se está ejecutando.

Amazon SNS: Amazon Simple Notification Service (Amazon SNS) es un servicio administrado con el que se ofrece la entrega de mensajes de los publicadores a los suscriptores (también conocido como productores y consumidores).

Epics

Automatice la detección de desviaciones para CloudFormation

Tarea	Descripción	Habilidades requeridas
Cree el agregador.	En la consola de AWS Config, cree un agregador en la cuenta de administración. Asegúrese de que la replicación de datos esté activada para que AWS Config pueda obtener datos de las cuentas de origen. Además, seleccione todas las regiones y cuentas aplicables. Puede seleccionar cuentas en función de las organizaciones. Este es el enfoque recomendado porque las nuevas cuentas de la organización forman	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	parte automáticamente del agregador.	
Crear una regla gestionada por AWS.	Añada la regla `cloudformation-stack-drift-detection-check` gestionada por AWS. La regla necesita un valor de parámetro: `cloudformationArn` . Introduzca el nombre de recurso de Amazon (ARN) del rol de IAM que tiene los permisos de detectar la desviación de las pilas. Además, el rol debe tener una política de confianza que permita a AWS Config asumir el rol.	Arquitecto de la nube
Cree la sección de consultas avanzadas del agregador.	Para buscar pilas desviadas de varias fuentes, cree la siguiente consulta: `SELECT resourceId, configuration.driftInformation.stackDriftStatus WHERE resourceType = 'AWS::CloudFormation::Stack'  AND configuration.driftInformation.stackDriftStatus IN ('DRIFTED')`	Arquitecto de la nube, desarrollador

Tarea	Descripción	Habilidades requeridas
Automatice la ejecución de la consulta y la publicación.	Cree una función de Lambda utilizando el código que se adjunta. Lambda publicará los resultados en un tema de Amazon SNS que se proporciona como variable de entorno en la función de Lambda. Además, para recibir alertas, cree una suscripción por correo electrónico a un tema existente de Amazon SNS.	Arquitecto de la nube, desarrollador
Crea una CloudWatch regla.	Cree una CloudWatch regla basada en la programac ión para llamar a la función Lambda, que es responsable de las alertas.	Arquitecto de la nube

Recursos relacionados

Recursos

- ¿Qué es AWS Config?
- Conceptos: acumulación de datos de multicuentas y multiregiones
- Acumulación de datos de multicuentas y multiregiones
- Detección de cambios de configuración no administrados en pilas y recursos
- IAM: pasar un rol de IAM a un servicio de AWS específico
- ¿Qué es Amazon SNS?

Información adicional

Consideraciones

No es óptimo utilizar soluciones personalizadas que impliquen llamadas a la API en intervalos específicos para iniciar la detección de desviaciones en cada CloudFormation pila o conjunto de pilas. Genera un gran número de llamadas a la API y afecta al rendimiento. Debido a la cantidad de llamadas a la API, se pueden producir limitaciones. Otro posible problema es el retraso en la detección si los cambios en los recursos se identifican únicamente en función de la programación.

PREGUNTAS FRECUENTES

P: ¿Debo usar una solución basada en complementos con AWS Landing Zone?

R. Con la disponibilidad de la función de consultas avanzadas en AWS Config, junto con el agregador, se recomienda utilizar AWS Config en lugar de un complemento.

P: ¿Cómo aborda esta solución CloudFormation StackSets?

R: Como los conjuntos de pilas se componen de pilas, puede utilizar esta solución. Los detalles de las instancias de pilas también están disponibles como parte de la solución.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Mejore el rendimiento operativo al habilitar Amazon DevOps Guru en varias regiones, cuentas y unidades organizativas de AWS con la AWS CDK

Creado por el Dr. Rahul Gaikwad (AWS)

Repositorio de código: código de muestra de Amazon DevOps Guru	Entorno: PoC o piloto	Tecnologías: administración y gobierno; nativas de la nube DevOps; operaciones; seguridad, identidad y conformidad; sin servidor
Servicios de AWS: Amazon API Gateway; AWS CDK; Amazon DevOps Guru; Amazon DynamoDB; AWS Organizations		

Resumen

Este patrón muestra los pasos para habilitar el servicio Amazon DevOps Guru en varias regiones, cuentas y unidades organizativas (OU) de Amazon Web Services (AWS) mediante el kit de desarrollo en la nube de AWS (AWS CDK) en TypeScript. Puede usar las pilas de CDK de AWS para implementar AWS CloudFormation StackSets desde la cuenta de administrador (principal) de AWS para habilitar Amazon DevOps Guru en varias cuentas, en lugar de iniciar sesión en cada cuenta y habilitar DevOps Guru individualmente para cada una de ellas.

Amazon DevOps Guru ofrece funciones de operaciones de inteligencia artificial (AIOps) para ayudarlo a mejorar la disponibilidad de sus aplicaciones y resolver los problemas operativos con mayor rapidez. DevOps Guru reduce el esfuerzo manual al aplicar recomendaciones basadas en el aprendizaje automático (ML), sin necesidad de conocimientos de aprendizaje automático. DevOps Guru analiza sus recursos y datos operativos. Si detecta alguna anomalía, proporciona métricas, eventos y recomendaciones para ayudarle a solucionar el problema.

Este patrón describe tres opciones de implementación para habilitar Amazon DevOps Guru:

- Para todos, apile recursos en varias cuentas y regiones
- Para todos los recursos de pila en las OU
- Para recursos de pila específicos en varias cuentas y regiones

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada. (Consulte Instalación, actualización y desinstalación de la CLI de AWS en la documentación de la CLI de AWS).
- Kit de herramientas de AWS CDK, instalado y configurado. (Consulte el kit de herramientas de AWS CDK en la documentación de AWS CDK).
- Node Package Manager (npm), instalado y configurado para la AWS CDK en. TypeScript (Consulte Descarga e instalación de Node.js y npm en la documentación de npm).
- Python3 instalado y configurado para ejecutar un script de Python para inyectar tráfico en la aplicación sin servidor de muestra. (Consulte Configuración y uso de Python en la documentación de Python).
- Pip, instalado y configurado para instalar la biblioteca de solicitudes de Python. (Consulte las instrucciones de instalación de pip en el PyPI sitio web).

Versiones de producto

- Kit de herramientas de AWS CDK, versión 1.107.0 o posterior
- npm versión 7.9.0 o posterior
- Node.js: versión 15.3.0 o posterior

Arquitectura

Tecnologías

La arquitectura de este patrón incluye los siguientes servicios:

- El DevOps gurú de Amazon

- AWS CloudFormation
- Amazon API Gateway
- AWS Lambda
- Amazon DynamoDB
- Amazon CloudWatch
- AWS CloudTrail

Pilas de CDK de AWS

El patrón utiliza las siguientes pilas de CDK de AWS:

- `CdkStackSetAdminRole`: crea un rol de administrador de AWS Identity and Access Management (IAM) para establecer una relación de confianza entre las cuentas de administrador y de destino.
- `CdkStackSetExecRole`: crea un rol de IAM para confiar en la cuenta de administrador.
- `CdkDevopsGuruStackMultiAccReg`— Permite que DevOps Guru funcione en varias regiones y cuentas de AWS para todas las pilas, y configura las notificaciones del Amazon Simple Notification Service (Amazon SNS).
- `CdkDevopsGuruStackMultiAccRegSpecStacks`— Permite que DevOps Guru funcione en varias regiones y cuentas de AWS para pilas específicas, y configura las notificaciones de Amazon SNS.
- `CdkDevopsguruStackOrgUnit`— Habilita DevOps Guru en todas las unidades organizativas y configura las notificaciones de Amazon SNS.
- `CdkInfrastructureStack`: implementa ejemplos de componentes de aplicaciones sin servidor, como API Gateway, Lambda y DynamoDB, en la cuenta de administrador para demostrar la inyección de errores y la generación de información.

Arquitectura de aplicación de muestra

El siguiente diagrama ilustra la arquitectura de un ejemplo de aplicación sin servidor que se ha implementado en varias cuentas y regiones. El patrón utiliza la cuenta de administrador para implementar todas las pilas de CDK de AWS. También utiliza la cuenta de administrador como una de las cuentas de destino para configurar DevOps Guru.

1. Cuando DevOps Guru está activado, primero toma como base el comportamiento de cada recurso y, a continuación, ingiere los datos operativos de CloudWatch las métricas vendidas.

2. Si detecta una anomalía, la correlaciona con los eventos que se producen y genera información. CloudTrail
3. La información proporciona una secuencia correlacionada de eventos junto con recomendaciones prescritas para que el operador pueda identificar el recurso responsable.
4. Amazon SNS envía mensajes de notificación al operador.

Automatizar y escalar

El GitHub repositorio que se proporciona con este patrón utiliza la CDK de AWS como herramienta de infraestructura como código (IaC) para crear la configuración de esta arquitectura. AWS CDK le ayuda a organizar los recursos y a habilitar DevOps Guru en varias cuentas, regiones y unidades organizativas de AWS.

Herramientas

Servicios de AWS

- AWS CDK: el Kit de desarrollo en la nube de AWS (AWS CDK) le ayuda a definir su infraestructura de nube como código en uno de los cinco lenguajes de programación compatibles: JavaScript Python TypeScript, Java y C#.
- AWS CLI: Interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta unificada que proporciona una interfaz de la línea de comandos coherente para interactuar con los servicios y recursos de AWS.

Código

El código fuente de este patrón está disponible en el GitHub repositorio Amazon DevOps Guru CDK Samples. El código CDK de AWS está escrito TypeScript. Para clonar y utilizar el repositorio, siga las instrucciones de la siguiente sección.

Importante: algunas de las historias de este patrón incluyen ejemplos de comandos de AWS CDK y AWS CLI formateados para Unix, Linux y macOS. Para Windows, sustituya la barra diagonal invertida (\) utilizada como carácter de continuación de Unix al final de cada línea por el signo de intercalación (^).

Epics

Prepare los recursos de AWS para la implementación

Tarea	Descripción	Habilidades requeridas
Configure los perfiles con nombre de AWS.	Configure sus perfiles con nombre de AWS de la siguiente manera para implementar pilas en un entorno de varias cuentas. Para la cuenta de administrador: `$aws configure --profile administrator` `AWS Access Key ID [****]: <your-administrator-access-key-ID>` `AWS Secret Access Key [****]: <your-administrator-secret-access-key>` `Default region name [None]: <your-administrator-region>` `Default output format [None]: json` Para la cuenta de destino: `$aws configure --profile target` `AWS Access Key ID [****: <your-target-access-key-ID>` `AWS Secret Access Key [****]: <your-target-secret-access-key>`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`Default region name [None]: <your-target-region>` `Default output format [None]: json` Para obtener más información, consulte Uso de perfiles con nombre en la documentación de la CLI de AWS.	
Compruebe las configuraciones de los perfiles de AWS.	(Opcional) Puede verificar las configuraciones de su perfil de AWS en los archivos `credentials` y `config` siguiendo las instrucciones en Cómo establecer y ver los ajustes de configuración en la la documentación de la CLI de AWS.	DevOps ingeniero
Verifique la versión de AWS CDK.	Compruebe la versión del kit de herramientas de AWS CDK mediante el siguiente comando: `$cdk --version` Este patrón requiere la versión 1.107.0 o posterior. Si tiene una versión anterior de AWS CDK siga las instrucciones de la documentación de AWS CDK para actualizarla.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Clonar el código del proyecto.	Clona el GitHub repositorio de este patrón mediante el comando: `$git clone https://github.com/aws-samples/amazon-devopsguru-cdk-samples.git`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Instale las dependencias de los paquetes y compile los TypeScript archivos.	Instale las dependencias del paquete y compile los TypeScript archivos ejecutando los siguientes comandos: `$cd amazon-devopsguru-cdk-samples` `$npm install` `$npm fund` Estos comandos instalan todos los paquetes del repositorio de muestra. Importante: Si se muestra algún error acerca de paquetes que faltan, utilice uno de los siguientes comandos: `$npm ci` —o— `$npm install -g @aws-cdk/<package-name>` Puede encontrar la lista de nombres y versiones de los paquetes en la sección `Dependencies` del archivo `/amazon-devopsguru-cdk-samples/package.json`. Para obtener más información, consulte npm ci	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	y npm install en la documentación de npm.	

Crear (sintetizar) las pilas de CDK de AWS

Tarea	Descripción	Habilidades requeridas
Configure una dirección de correo electrónico para las notificaciones de Amazon SNS.	Siga estos pasos para proporcionar una dirección de correo electrónico para las notificaciones de Amazon SNS: 1. Edite los archivos `/amazon-devopsguru-cdk-samples/lib/cdk-devopsguru-multi-acc-reg-stack.ts` y `/amazon-devopsguru-cdk-samples/lib/cdk-devopsguru-org-uni-stack.ts` . 2. En la `DevOpsGuruTopic` , sección `Subscription` , actualice el parámetro `Endpoint` con su dirección de correo electrónico. 3. Guardar y cerrar los archivos.	DevOps ingeniero
Construya el código del proyecto.	Cree el código del proyecto y sintetice las pilas ejecutando el comando:	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`npm run build && cdk synth` Debería ver una salida similar a esta: `$npm run build && cdk synth` `> cdk-devopsguru@0.1.0 build` `> tsc` `Successfully synthesized to ~/amazon-devopsguru-cdk-samples/cdk.out` `Supply a stack id (CdkDevopsGuruStackMultiAccReg,CdkDevopsGuruStackMultiAccRegSpecStacks, CdkDevopsguruStackOrgUnit, CdkInfrastructureStack, CdkStackSetAdminRole, CdkStackSetExecRole) to display its template.` Para obtener más información y conocer los pasos, consulte Su primera aplicación de AWS CDK en la documentación de AWS CDK.	

Tarea	Descripción	Habilidades requeridas
Enumere las pilas de CDK de AWS.	Ejecute el siguiente comando para enumerar todas las pilas de AWS CDK: `$cdk list` El comando muestra la lista siguiente: `CdkDevopsGuruStack` `MultiAccReg` `CdkDevopsGuruSt` `ackMultiAccRegSpec` `Stacks` `CdkDevopsguruStackOr` `gUnit` `CdkInfrastructureStac` `k` `CdkStackSetAdminRole` `CdkStackSetExecRole`	DevOps ingeniero

Opción 1: Habilita DevOps Guru para todos los recursos acumulados en varias cuentas

Tarea	Descripción	Habilidades requeridas
Implemente las pilas de CDK de AWS para crear roles de IAM.	Este patrón utiliza AWS CloudFormation StackSets para realizar operaciones de apilamiento en varias cuentas. Si va a crear su primer conjunto de pilas, debe crear las siguientes funciones de IAM para configurar los permisos necesarios en sus cuentas de AWS:	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	• `AWSCloudFormationStackSetAdministrationRole` • `AWSCloudFormationStackSetExecutionRole` Nota: Los roles deben tener estos nombres exactos. 1. Cree el rol `AWSCloudFormationStackSetAdministrationRole` de IAM en la cuenta de administrador (principal) ejecutando el siguiente comando CLI: `$cdk deploy CdkStackSetAdminRole --profile administrator` 2. Cree el rol `AWSCloudFormationStackSetExecutionRole` de IAM en todas las cuentas de destino en las que desee ejecutar las instancias de la pila. Para crear este rol, ejecute estos comandos de CLI: `$cdk deploy CdkStackSetExecRole \ --parameters AdministratorAccou`	

Tarea	Descripción	Habilidades requeridas
	ntId=<administrato r-account-ID> \ --profile administr ator $cdk deploy CdkStackS etExecRole \ --parameters AdministratorAccou ntId=<administrato r-account-ID> \ --profile target Para obtener más informaci ón, consulte Otorgar permisos autogestionados en la CloudFormation documenta ción de AWS.	

Tarea	Descripción	Habilidades requeridas
Implemente la pila de CDK de AWS para habilitar DevOps Guru en varias cuentas.	La pila `CdkDevopsGuruStackMultiAccReg` de CDK de AWS crea conjuntos de pilas para implementar instancias de pila en varias cuentas y regiones. Para implementar la pila, ejecute el siguiente comando de la CLI con los parámetros especificados: `$cdk deploy CdkDevopsGuruStackMultiAccReg \ --profile administrator \ --parameters AdministratorAccountId=<administrator-account-ID> \ --parameters TargetAccountId=<target-account-ID> \ --parameters RegionIds="<region-1>,<region-2>"` Actualmente, Amazon DevOps Guru está disponible en las regiones de AWS que figuran en las preguntas frecuentes de DevOps Guru.	DevOps ingeniero

Opción 2: habilitar DevOps Guru para todos los recursos de pila en las unidades organizativas

Tarea	Descripción	Habilidades requeridas
Extraiga los ID de OU.	En la consola de AWS Organizations, identifique los ID de las unidades organizativas en las que quiere habilitar DevOps Guru.	DevOps ingeniero
Habilite los permisos administrados por servicios para las OU.	Si utiliza AWS Organizations para la administración de cuentas, debe conceder permisos gestionados por el servicio para activar DevOps Guru. En lugar de crear las funciones de IAM manualmente, utilice funciones de acceso confiable y vinculadas a servicios (SLR) basadas en la organización.	DevOps ingeniero
Implemente la pila de CDK de AWS para habilitar DevOps Guru en todas las unidades organizativas.	La `CdkDevopsguruStackOrgUnit` pila de CDK de AWS permite el servicio DevOps Guru en todas las unidades organizativas. Para implementar la pila, ejecute el siguiente comando con los parámetros especificados: `$cdk deploy CdkDevopsguruStackOrgUnit \ --profile administrator \ --parameters RegionIds="<region-1>,<region-2>" \`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`--parameters OrganizationalUnitIds="<OU-1>,<OU-2>"`	

Opción 3: Habilita DevOps Guru para almacenar recursos de pila específicos en varias cuentas

Tarea	Descripción	Habilidades requeridas
Implemente las pilas de CDK de AWS para crear roles de IAM.	Si aún no ha creado las funciones de IAM requeridas que se muestran en la primera opción, hágalo primero: 1. Cree el rol `AWSCloudFormationStackSetAdministrationRole` de IAM en la cuenta de administrador (principal) ejecutando el siguiente comando CLI: `$cdk deploy CdkStackSetAdminRole --profile administrator` 2. Cree el rol `AWSCloudFormationStackSetExecutionRole` de IAM en todas las cuentas de destino en las que desee ejecutar las instancias de la pila. Para crear este rol, ejecute los comandos CLI: `$cdk deploy CdkStackSetExecRole \`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	<pre>--parameters AdministratorAccountId=<administrator-account-ID> \ --profile administrator $cdk deploy CdkStackSetExecRole \ --parameters AdministratorAccountId=<administrator-account-ID> \ --profile target</pre> Para obtener más información, consulte Otorgar permisos autogestionados en la CloudFormation documentación de AWS.	

Tarea	Descripción	Habilidades requeridas
Eliminar las pilas existentes.	Si ya utilizaste la primera opción para habilitar DevOps Guru para todos los recursos de la pila, puedes eliminar la pila anterior mediante el siguiente comando: `$cdk destroy CdkDevops GuruStackMultiAccR eg --profile administr ator` O bien, puede cambiar el parámetro `RegionIds` al volver a implementar la pila para evitar el error Las pilas ya existen.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Actualizar la pila de CDK de AWS con una lista de pilas.	1. Edite el archivo `/amazon-devopsguru-cdk-samples/lib/cdk-devopsguru-multi-acc-reg-spec-stack.ts` . 2. En `Resources` , `CloudFormation` , `StackNames` , enumera las pilas para las que quieres activar DevOps Guru. A modo de demostración, el parámetro especifique la pila `CdkInfrastructureStack` , pero puede editar esta entrada en función de sus necesidades. 3. Guarde y cierre el archivo. 4. Para sintetizar y actualizar la plantilla de pila, ejecute: `$cdk synth`	Ingeniero de datos

Tarea	Descripción	Habilidades requeridas
Implemente la pila de CDK de AWS para habilitar a DevOps Guru para disponer de recursos de pila específicos en varias cuentas.	La `CdkDevopsGuruStackMultiAccRegSpecStacks` pila de CDK de AWS permite a DevOps Guru disponer de recursos de pila específicos en varias cuentas. Para implementar la pila, ejecute el siguiente comando: `$cdk deploy CdkDevopsGuruStackMultiAccRegSpecStacks \ --profile administrator \ --parameters AdministratorAccountId=<administrator-account-ID> \ --parameters TargetAccountId=<target-account-ID> \ --parameters RegionIds="<region-1>,<region-2>"` Nota: Si ya implementó esta pila para la opción 1, cambie el parámetro `RegionIds` (asegúrese de elegir entre las regiones disponibles) para evitar el error de que las pilas ya existen.	DevOps ingeniero

Implementar la pila de infraestructuras CDK de AWS

Tarea	Descripción	Habilidades requeridas
Implemente el ejemplo del paquete de infraestructura sin servidor.	La `CdkInfrastructureStack` pila de CDK de AWS implementa componentes sin servidor, como API Gateway, Lambda y una tabla de DynamoDB para mostrar las ideas de Guru. DevOps Para implementar la pila, ejecute el siguiente comando: `$cdk deploy CdkInfrastructureStack --profile administrator`	DevOps ingeniero
Introducir registros de ejemplo en DynamoDB.	Ejecute el siguiente comando para rellenar la tabla de DynamoDB con registros de ejemplo. Proporcione la ruta correcta para el script `populate-shops-dynamodb-table.json` . `$aws dynamodb batch-write-item \ --request-items file://scripts/populate-shops-dynamodb-table.json \ --profile administrator` El comando muestra el resultado siguiente:	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`{ "UnprocessedItems" : {} }`	

Tarea	Descripción	Habilidades requeridas
Compruebe los registros introducidos en DynamoDB.	Para comprobar que la tabla de DynamoDB incluye los registros de muestra del archivo `populate-shops-dynamodb-table.json` , acceda a a URL de la API `ListRestApiEndpointMonitorOperator` , que se publica como salida de la pila de CDK de AWS. También puede encontrar esta URL en la pestaña Salidas de la CloudFormation consola de AWS de la `CdkInfrastructureStack` pila. La salida de AWS CDK sería similar a la siguiente: `CdkInfrastructureStack.CreateRestApiMonitorOperatorEndpointD1D00045 = https://oure17c5vob.execute-api.<your-region>.amazonaws.com/prod/` `CdkInfrastructureStack.ListRestApiMonitorOperatorEndpointABBDB8D8 = https://cdff8icfrn4.execute-api.<your-region>.amazonaws.com/prod/`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Espere a que los recursos completen la línea de base.	Esta pila sin servidor tiene algunos recursos. Le recomendamos que espere 2 horas antes de realizar los siguientes pasos. Si implementó esta pila en un entorno de producción, es posible que se tarden hasta 24 horas en completar la línea base, según la cantidad de recursos que haya seleccion ado para monitorear en DevOps Guru.	DevOps ingeniero

Genera ideas de DevOps Guru

Tarea	Descripción	Habilidades requeridas
Actualizar la pila de infraestr ucturas CDK de AWS.	Para probar DevOps Guru Insights, puede realizar algunos cambios de configura ción para reproducir un problema operativo típico. 1. Edite el archivo `/amazon-devopsguru-cdk-samples/lib/infrastructure-stack.ts` . 2. En la sección `DDB Table`, cambie la capacidad de lectura de la tabla de DynamoDB de 5 a 1. 3. Guarde y cierre el archivo.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	4. Ejecute los siguientes comandos para sintetizar e implementar la pila de infraestructura CDK de AWS actualizada: `$cdk synth` `$cdk deploy CdkInfrastructureStack --profile administrator`	

Tarea	Descripción	Habilidades requeridas
Introduzca solicitudes HTTP en la API.	Inyecta tráfico de entrada en forma de solicitudes HTTP en la API `ListRestApiMonitorOperatorEndpointxxxx` : 1. Ejecute el script de Python `/amazon-devopsguru-cdk-samples/scripts/sendAPIRequest.py` . 2. Actualiza la variable `url` con el enlace de la API para `ListRestApiMonitorOperatorEndpointxxxx` . Puede encontrar esta URL en la salida del comando de implementación de AWS CDK o en la consola de AWS Cloudformation, en la pestaña Salidas de la pila. 3. Guarde y cierre el archivo. 4. Ejecute el script de Python mediante el comando siguiente: `$python sendAPIRequest.py` 5. Asegúrese de obtener un código de estado 200. 6. Puede que necesite ejecutar el script a través de varios terminales	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	(preferiblemente cuatro) para inyectar tráfico a una velocidad alta. 7. Una vez que el script se ejecute aproximadamente 10 minutos seguidos, podrá ver una visión operativa en la consola DevOps Guru.	
Revise las ideas de DevOps Guru.	En condiciones estándar, el panel de control de DevOps Guru muestra cero en el contador de información continua. Si detecta una anomalía, emite una alerta en forma de información. En el panel de navegación, selecciona Insights para ver los detalles de la anomalía, incluidos un resumen, métricas agregadas, eventos relevantes y recomenda ciones. Para obtener más información sobre la revisión de información, consulte la entrada del blog Cómo obtener información operativa con AIOps mediante Amazon DevOps Guru.	DevOps ingeniero

Limpieza

Tarea	Descripción	Habilidades requeridas
Limpie y elimine recursos.	Después de seguir este patrón, debe eliminar los recursos que ha creado para evitar incurrir en cargos adicionales. Ejecute estos comandos: `$cdk destroy CdkDevops GuruStackMultiAccReg --profile administrator` `$cdk destroy CdkDevops guruStackOrgUnit --profile administrator` `$cdk destroy CdkDevops GuruStackMultiAccRegSpecStacks --profile administrator` `$cdk destroy CdkInfrastructureStack --profile administrator` `$cdk destroy CdkStackSetAdminRole --profile administrator` `$cdk destroy CdkStackSetExecRole --profile administrator` `$cdk destroy CdkStackSetExecRole --profile target`	DevOps ingeniero

Recursos relacionados

- Obtenga información operativa con AIOps mediante Amazon Guru DevOps

- Configure Amazon DevOps Guru fácilmente en varias cuentas y regiones mediante AWS CloudFormation StackSets
- DevOps Taller de gurús

Implemente Account Factory for Terraform (AFT) mediante una canalización de arranque

Creado por Vinicius Elias (AWS) y Edgar Costa Filho (AWS)

Repositorio de código: aft-bootstrap-pipeline	Entorno: producción	Tecnologías: gestión y gobierno; infraestructura
Carga de trabajo: código abierto	Servicios de AWS: AWS CodeBuild CodeCommit; AWS CodePipeline; AWS Control Tower; AWS Organizations	

Resumen

Este patrón proporciona un método sencillo y seguro para implementar AWS Control Tower Account Factory for Terraform (AFT) desde la cuenta de administración de AWS Organizations. El núcleo de la solución es una AWS CloudFormation plantilla que automatiza la configuración de AFT mediante la creación de una canalización de Terraform, que está estructurada para adaptarse fácilmente a la implementación inicial o a las actualizaciones posteriores.

La seguridad y la integridad de los datos son las principales prioridades AWS, por lo que el archivo de estado de Terraform, que es un componente fundamental que rastrea el estado de la infraestructura y las configuraciones administradas, se almacena de forma segura en un depósito de Amazon Simple Storage Service (Amazon S3). Este depósito está configurado con varias medidas de seguridad, como el cifrado del lado del servidor y políticas para bloquear el acceso público, a fin de garantizar que el estado de Terraform esté protegido contra el acceso no autorizado y las filtraciones de datos.

La cuenta de administración organiza y supervisa todo el entorno, por lo que es un recurso fundamental en él. AWS Control Tower Este patrón sigue las AWS mejores prácticas y garantiza que el proceso de implementación no solo sea eficiente, sino que también se alinee con los estándares de seguridad y gobernanza, a fin de ofrecer una forma integral, segura y eficiente de implementar la AFT en su entorno. AWS

Para obtener más información sobre AFT, consulte la AWS Control Tower documentación.

Requisitos previos y limitaciones

Requisitos previos

- Un entorno básico de AWS múltiples cuentas con las siguientes cuentas como mínimo: cuenta de administración, cuenta de Log Archive, cuenta de auditoría y una cuenta adicional para la administración de AFT.
- Un AWS Control Tower entorno establecido. La cuenta de administración debe estar configurada correctamente, ya que la CloudFormation plantilla se implementará en ella.
- Los permisos necesarios en la cuenta AWS de administración. Necesitará permisos suficientes para crear y administrar recursos, como depósitos, AWS Lambda funciones AWS Identity and Access Management (IAM) y AWS CodePipeline proyectos de S3.
- Familiaridad con Terraform. Es importante comprender los conceptos básicos y el flujo de trabajo de Terraform porque la implementación implica generar y administrar las configuraciones de Terraform.

Limitaciones

- Tenga en cuenta las cuotas de AWS recursos de su cuenta. La implementación podría crear varios recursos y, si se produjeran cuotas de servicio, se podría impedir el proceso de implementación.
- La plantilla está diseñada para versiones específicas de Terraform y. Servicios de AWS La actualización o el cambio de versiones pueden requerir modificaciones en la plantilla.

Versiones de producto

- Terraform, versión 1.5.7 o posterior
- AFT versión 1.11.1 o posterior

Arquitectura

Pila de tecnología de destino

- AWS CloudFormation
- AWS CodeBuild
- AWS CodeCommit

- AWS CodePipeline
- Amazon EventBridge
- IAM
- AWS Lambda
- Amazon S3

Arquitectura de destino

El siguiente diagrama ilustra la implementación analizada en este patrón.

El flujo de trabajo consta de tres tareas principales: crear los recursos, generar el contenido y ejecutar la canalización.

Crear los recursos

La CloudFormation plantilla que se proporciona con este patrón crea y configura todos los recursos necesarios, en función de los parámetros que seleccione al implementar la plantilla. Como mínimo, la plantilla crea los siguientes recursos:

- Un CodeCommit repositorio para almacenar el código de arranque de AFT Terraform
- Un depósito de S3 para almacenar el archivo de estado de Terraform asociado a la implementación de AFT
- ¿ CodePipeline Una canalización
- Dos CodeBuild proyectos para implementar el plan Terraform y aplicar comandos en diferentes etapas del proceso
- Funciones y servicios de IAM CodeBuild CodePipeline
- Un segundo depósito de S3 para almacenar los artefactos relacionados con el tiempo de ejecución de la canalización
- Una EventBridge regla para capturar los cambios del CodeCommit repositorio en la `main` sucursal
- Otra función de IAM para la regla EventBridge

Además, si estableces el `Generate AFT Files` parámetro de la CloudFormation plantilla en`true`, la plantilla crea los siguientes recursos adicionales para generar el contenido:

- Un depósito de S3 para almacenar el contenido generado y utilizarlo como fuente del CodeCommit repositorio
- Una función Lambda para procesar los parámetros dados y generar el contenido apropiado
- Una función de IAM para ejecutar la función Lambda
- Un recurso CloudFormation personalizado que ejecuta la función Lambda cuando se implementa la plantilla

Generar el contenido

Para generar los archivos de arranque AFT y su contenido, la solución utiliza una función Lambda y un bucket S3. La función crea una carpeta en el depósito y, a continuación, crea dos archivos dentro de la carpeta: `main.tf` y. `backend.tf` La función también procesa los CloudFormation parámetros proporcionados y rellena estos archivos con código predefinido, sustituyendo los valores de los parámetros respectivos.

Para ver el código que se utiliza como plantilla para generar los archivos, consulte el GitHub repositorio de la solución. Básicamente, los archivos se generan de la siguiente manera.

main.tf

```
module "aft" {
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory?
ref=<aft_version>"

  # Required variables
  ct_management_account_id  = "<ct_management_account_id>"
  log_archive_account_id    = "<log_archive_account_id>"
  audit_account_id          = "<audit_account_id>"
  aft_management_account_id = "<aft_management_account_id>"
  ct_home_region            = "<ct_home_region>"

  # Optional variables
  tf_backend_secondary_region = "<tf_backend_secondary_region>"
  aft_metrics_reporting       = "<false|true>"

  # AFT Feature flags
  aft_feature_cloudtrail_data_events      = "<false|true>"
  aft_feature_enterprise_support          = "<false|true>"
  aft_feature_delete_default_vpcs_enabled = "<false|true>"
```

```
  # Terraform variables
  terraform_version      = "<terraform_version>"
  terraform_distribution = "<terraform_distribution>"

}
```

backend.tf

```
terraform {
  backend "s3" {
    region = "<aft-main-region>"
    bucket = "<s3-bucket-name>"
    key    = "aft-setup.tfstate"
  }
}
```

Durante la creación del CodeCommit repositorio, si estableces el `Generate AFT Files` parámetro en`true`, la plantilla utilizará el depósito de S3 con el contenido generado como fuente de la `main` rama para rellenar automáticamente el repositorio.

Ejecutando la canalización

Una vez creados los recursos y configurados los archivos de arranque, se ejecuta la canalización. La primera etapa (Fuente) busca el código fuente de la rama principal del repositorio, y la segunda etapa (Compilación) ejecuta el comando Terraform plan y genera los resultados para su revisión. En la tercera etapa (aprobación), el proceso espera a que se lleve a cabo una acción manual para aprobar o rechazar la última etapa (implementación). En la última etapa, la canalización ejecuta el `apply` comando Terraform utilizando como entrada el resultado del `plan` comando Terraform anterior. Por último, un rol multicuenta y los permisos de la cuenta de administración se utilizan para crear los recursos de AFT en la cuenta de administración de AFT.

Herramientas

Servicios de AWS

- AWS CloudFormationle ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- AWS CodeBuildes un servicio de compilación totalmente gestionado que le ayuda a compilar el código fuente, ejecutar pruebas unitarias y producir artefactos listos para su implementación.

- AWS CodeCommites un servicio de control de versiones que te ayuda a almacenar y gestionar de forma privada los repositorios de Git sin necesidad de gestionar tu propio sistema de control de código fuente.
- AWS CodePipelinete ayuda a modelar y configurar rápidamente las diferentes etapas de una versión de software y a automatizar los pasos necesarios para publicar los cambios de software de forma continua.
- AWS Lambdaes un servicio informático que ejecuta el código en respuesta a eventos y administra automáticamente los recursos informáticos, lo que proporciona una forma rápida de crear una aplicación moderna y sin servidor para la producción.
- AWS SDK for Python (Boto3)es un kit de desarrollo de software que le ayuda a integrar su aplicación, biblioteca o script de Python con los servicios de AWS.

Otras herramientas

- Terraform es una herramienta de infraestructura como código (IaC) que le permite crear, cambiar y versionar la infraestructura de forma segura y eficiente. Esto incluye componentes de bajo nivel, como instancias de procesamiento, almacenamiento y redes, y componentes de alto nivel, como entradas de DNS y funciones de SaaS.
- Python es un lenguaje de programación potente y fácil de aprender. Cuenta con estructuras de datos eficientes de alto nivel y proporciona un enfoque simple pero efectivo para la programación orientada a objetos.

Repositorio de código

El código de este patrón está disponible en el repositorio bootstrap Pipeline de GitHub AFT.

Para ver el repositorio AFT oficial, consulte AWS Control Tower Account Factory for Terraform en GitHub.

Prácticas recomendadas

Al implementar AFT mediante la CloudFormation plantilla proporcionada, le recomendamos que siga las mejores prácticas para garantizar una implementación segura, eficiente y exitosa. Las pautas y recomendaciones clave para implementar y operar la AFT incluyen las siguientes.

- Revisión exhaustiva de los parámetros: revise y comprenda cuidadosamente cada parámetro de la CloudFormation plantilla. La configuración precisa de los parámetros es crucial para la correcta configuración y funcionamiento de la AFT.
- Actualizaciones periódicas de la plantilla: mantenga la plantilla actualizada con las últimas AWS funciones y versiones de Terraform. Las actualizaciones periódicas le ayudan a aprovechar las nuevas funciones y a mantener la seguridad.
- Control de versiones: fije la versión de su módulo AFT y, si es posible, utilice una implementación AFT independiente para realizar las pruebas.
- Alcance: utilice AFT únicamente para implementar barandas y personalizaciones de infraestructura. No lo use para implementar su aplicación.
- Revestimiento y validación: la canalización AFT requiere una configuración de Terraform validada y revestida. Ejecute lint, valide y pruebe antes de enviar la configuración a los repositorios de AFT.
- Módulos de Terraform: cree código de Terraform reutilizable como módulos y especifique siempre las versiones de Terraform y del AWS proveedor para que se adapten a los requisitos de su organización.

Epics

Configure y configure el entorno AWS

Tarea	Descripción	Habilidades requeridas
Prepare el AWS Control Tower entorno.	Instálelo y AWS Control Tower configúrelo en su AWS entorno para garantiza r una administración y un gobierno centralizados para su Cuentas de AWS. Para obtener más información, consulte Primeros pasos AWS Control Tower en la AWS Control Tower documentación.	Administrador de la nube
Inicie la cuenta de administr ación de AFT.	Utilice AWS Control Tower Account Factory para lanzar	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	una nueva Cuenta de AWS que sirva como su cuenta de administración de AFT. Para obtener más información, consulte Aprovisionar cuentas con AWS Service Catalog Account Factory en la AWS Control Tower documentación.	

Implemente la CloudFormation plantilla en la cuenta de administración

Tarea	Descripción	Habilidades requeridas
Inicie la CloudFormation plantilla.	En esta epopeya, despliega la CloudFormation plantilla proporcionada con esta solución para configurar la canalización de arranque de AFT en su cuenta AWS de administración. The Pipeline implementa la solución AFT en la cuenta de administración de AFT que configuraste en la epopeya anterior. Paso 1: Abre la consola AWS CloudFormation • Inicie sesión en la AWS CloudFormation consola AWS Management Console y ábrala. Asegúrese de operar en la región AWS Control Tower principal correcta.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	Paso 2: Crea una pila nueva 1. Elige crear una pila nueva. 2. Selecciona la opción de cargar un archivo de plantilla y carga la CloudFormation plantilla que viene con este patrón. Paso 3: Configurar los parámetros de la pila • `Repository Name` : especifique el nombre del repositorio para almacenar el módulo de arranque AFT. • `Branch Name`: especifique la rama del repositorio de origen. • `CodeBuild Docker Image`: elija el archivo que se usará como imagen base de CodeBuild Docker. Paso 4: Decida la generación de archivos • El `Generate AFT Files` parámetro controla si se generan los archivos de despliegue AFT predeterm inados. Defina este parámetro en:	

Tarea	Descripción	Habilidades requeridas
	• `true`para crear y almacenar automátic amente los archivos de despliegue de AFT en el repositorio especificado. • `false`si desea gestionar manualmente la creación del archivo o si ya tiene los archivos en su lugar. Si lo ha seleccion ado`false`, vaya al paso 8; de lo contrario, siga primero los pasos 5-7. Paso 5: Rellena AWS Control Tower y AFT con los detalles de la cuenta • Información específica de la cuenta de entrada AWS Control Tower y AFT: • `Log Archive Account ID`: El ID de la cuenta de Log Archive es. AWS Control Tower • `Audit Account ID`: El ID de la cuenta de auditoría en AWS Control Tower. • `AFT Management Account ID`: El ID de la cuenta de administración	

Tarea	Descripción	Habilidades requeridas
	de la AFT que creaste en la primera epopeya. • `AFT Main Region`y`AFT Secondary Region`: El principal y el secundario Regiones de AWS para el despliegue de AFT. Paso 6: Configurar las opciones de AFT • Configure los informes de métricas: • `AFT Enable Metrics Reporting` : Habilite o deshabilite los informes de métricas de AFT. Para obtener más informaci ón, consulte las métricas operativas en la AWS Control Tower documenta ción. • Configure las opciones de las funciones de AFT: • `Enable AFT CloudTrail Data Events`: Habilite CloudTrail los eventos de datos en todas las cuentas administradas por AFT. Para obtener más información, consulte AWS CloudTrail los	

Tarea	Descripción	Habilidades requeridas
	eventos de datos en la AWS Control Tower documentación. • `Enable AFT Enterprise Support` : Habilite Enterprise Support en todas las cuentas administradas por AFT. Para obtener más información, consulte el plan AWS Enterprise Support en la AWS Control Tower documentación. • `Enable AFT Delete Default VPC`: Elimine únicamente todas las VPC de la cuenta de administración de AFT. Para obtener más información, consulte Eliminar la VPC AWS predeterminada en la AWS Control Tower documentación. Paso 7: Especificar las versiones • `AFT Terraform Version`: Elija la versión de Terraform para usarla en las tuberías AFT.	

Tarea	Descripción	Habilidades requeridas
	• `AFT Version`: Defina la versión AFT para el despliegue. Mantenga la configuración predeterm inada (`latest`) para usar la versión AFT más reciente. Paso 8: Revise y cree la pila • Revise todos los parámetro s y ajustes. Si todo está en orden, proceda a crear la pila. Paso 9: Supervise la creación de la pila • AWS CloudFormation aprovisiona y configura los recursos que ha definido. Supervise el proceso de creación de la pila en la CloudFormation consola. Este proceso puede tardar varios minutos. Paso 10: Verificar la implementación • Cuando el estado de la pila muestre CREATE_CO MPLETE, compruebe que todos los recursos se hayan creado correctamente.	

Tarea	Descripción	Habilidades requeridas
	• En la sección Salidas, anote el valor. `Terraform BackendBucketName`	

Complete y valide el repositorio y la canalización de arranque de AFT

Tarea	Descripción	Habilidades requeridas
Rellene el repositorio bootstrap de AFT.	(Opcional) Tras implementar la CloudFormation plantilla , puede rellenar o validar el contenido del repositor io bootstrap de AFT recién creado y comprobar si la canalización se ha ejecutado correctamente. Si establece el `Generate AFT Files` parámetro en`true`, pase a la siguiente historia (validando la canalizac ión). Paso 1: Rellene el repositorio 1. Abra la AWS CodeCommi t consola y seleccione el repositorio recién creado. Si ha mantenido el nombre predeterminado, se llamará al repositorio`aft-setup` . 2. Clona el repositorio en tu máquina local mediante SSH, HTTPS o HTTPS	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	(GRC) y ábrelo en un editor. 3. Crea una carpeta llamada `terraform` y dos archivos vacíos en su interior: `backend.tf` y. `main.tf` 4. Abre el `backend.tf` archivo y añade este fragmento de código: `terraform { backend "s3" { region = "<aft-main-region>" bucket = "<s3-bucket-name>" key = "aft-setup" } }` En el archivo: • `<aft-main-region>` Sustitúyala por la región AFT principal . Debe coincidir con la región AWS Control Tower principal. • `<s3-bucket-name>` Sustitúyalo por el nombre del depósito de backend de Terraform . Puedes encontrar lo en el `Terraform`	

Tarea	Descripción	Habilidades requeridas
	`BackendBucketName` resultado generado por la CloudFormation plantilla que implement aste anteriormente. 5. Abra el `main.tf` archivo y utilice uno de los ejemplos disponibles en el repositor io de AFT para implementar AFT. Por ejemplo, puedes trabajar con tu proveedor de sistema de control de versiones (VCS) preferido (CodeCommit GitHub, o Bitbucket) o personalizar la VPC de AFT. Para ver más opciones de entrada de AFT, consulta el archivo README del repositorio de AFT. Paso 2: Confirma y envía tus cambios • Una vez que haya creado y rellenado la carpeta y los archivos, confirme los cambios y suba el código al repositorio. La canalización se inicia automáticamente, pasa por las etapas de origen y compilación y, a continuación, espera a que se lleve a cabo una acción	

Tarea	Descripción	Habilidades requeridas
	de aprobación antes de la etapa de implementación.	

Tarea	Descripción	Habilidades requeridas
Valide la canalización de arranque de AFT.	Paso 1: Ver la canalización • Abre la CodePipeline consola y comprueba si la `aft-bootstrap-pipeline` canalización se inició correctamente. Debería estar ejecutando un plan Terraform o esperando una acción de aprobación manual. Paso 2: Aprobar los resultados del plan Terraform • Puede revisar los resultados del plan Terraform consultando los registros de ejecución de la fase de construcción y, a continuación, aprobar o rechazar la ejecución en la fase de aprobación. Si lo apruebas, la canalización empezará a implementar los recursos de AFT en la cuenta de administración de AFT proporcionada. Paso 3: espere a que se despliegue • Espere a que la canalización se ejecute correctamente. Esto debería tardar	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	unos 30 minutos. Los errores que puedas encontrar suelen deberse a las cuotas de la API. En estos casos, puedes volver a ejecutar la canalizac ión para continuar con la implementación. Paso 4: Compruebe los recursos creados • Acceda a la cuenta de administración de AFT y confirme que se hayan creado los recursos.	

Solución de problemas

Problema	Solución
La función Lambda personalizada incluida en la CloudFormation plantilla falla durante la implementación.	Compruebe la función Lambda en los CloudWatch registros de Amazon para identific ar el error. Los registros proporcionan informaci ón detallada y pueden ayudar a identificar el problema específico. Confirme que la función Lambda tiene los permisos necesarios y que las variables de entorno se han configurado correctamente.
Se producen errores en la creación o administr ación de los recursos debido a permisos inadecuados.	Revise las funciones y políticas de IAM asociadas a la función CodeBuild Lambda y otros servicios involucrados en la implement ación. Confirme que tienen los permisos

Problema	Solución
	necesarios. Si hay problemas con los permisos, ajuste las políticas de IAM para conceder el acceso necesario.
Estás utilizando una versión anticuada de la CloudFormation plantilla con versiones más recientes Servicios de AWS o de Terraform.	Actualiza la CloudFormation plantilla con regularidad para que sea compatible con las versiones más recientes AWS y las de Terraform. Consulte las notas de la versión o la documentación para ver si hay cambios o requisitos específicos de la versión.
Servicio de AWS Las cuotas se alcanzan durante la implementación.	Antes de implementar la canalización, compruebe Servicio de AWS las cuotas de recursos, como los buckets de S3, las funciones de IAM y las funciones de Lambda. Solicita aumentos si es necesario. Para obtener más información, consulte Servicio de AWS las cuotas en el AWS sitio web.
Se producen errores debido a parámetros de entrada incorrectos en la CloudFormation plantilla.	Compruebe todos los parámetros de entrada para ver si hay errores tipográficos o valores incorrectos. Confirme que los identificadores de recursos, como los identificadores de cuentas y los nombres de las regiones, sean correctos.

Recursos relacionados

Para implementar este patrón correctamente, revise los siguientes recursos. Estos recursos proporcionan información y orientación adicionales que pueden ser invaluables para configurar y administrar la AFT mediante el uso AWS CloudFormation.

AWSdocumentación:

- AWS Control Tower La guía del usuario ofrece información detallada sobre la configuración y la administración AWS Control Tower.

- AWS CloudFormation la documentación proporciona información sobre las CloudFormation plantillas, las pilas y la administración de recursos.

Políticas y mejores prácticas de IAM:

- Las prácticas recomendadas de seguridad en IAM explican cómo ayudar a proteger los AWS recursos mediante el uso de las funciones y políticas de IAM.

Terraform en: AWS

- La documentación de Terraform AWS Provider proporciona información completa sobre el uso de Terraform con. AWS

Servicio de AWS cuotas:

- Servicio de AWS cuotas proporciona información sobre cómo ver Servicio de AWS las cuotas y cómo solicitar aumentos.

Administre los productos de AWS Service Catalog en varias cuentas y regiones de AWS

Creado por Ram Kandaswamy (AWS)

Entorno: producción	Tecnologías: gestión y gobernanza; nativas en la nube; infraestructura; operaciones; modernización	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: AWS Service Catalog; AWS CloudFormation		

Resumen

Service Catalog, de Amazon Web Services (AWS), simplifica y acelera la gobernanza y la distribución de plantillas de infraestructura como código (IaC) para las empresas. Utiliza las CloudFormation plantillas de AWS para definir un conjunto de recursos de AWS (pilas) necesarios para un producto. AWS CloudFormation StackSets amplía esta funcionalidad al permitirle crear, actualizar o eliminar pilas en varias cuentas y regiones de AWS con una sola operación.

Los administradores de AWS Service Catalog crean productos mediante CloudFormation plantillas creadas por desarrolladores y las publican. A continuación, estos productos se asocian a una cartera y se imponen restricciones en materia de gobernanza. Para poner sus productos a disposición de usuarios de otras cuentas o unidades organizativas (OU) de AWS, normalmente comparte su cartera con ellos. Este patrón describe un enfoque alternativo para administrar las ofertas de productos de AWS Service Catalog que se basa en AWS CloudFormation StackSets. En lugar de compartir carteras, se usan restricciones de conjuntos de pilas para establecer las regiones y cuentas de AWS en las que se puede implementar y usar su producto. Con este enfoque puede aprovisionar sus productos de AWS Service Catalog en varias cuentas, unidades organizativas y regiones de AWS, y administrarlos desde una ubicación centralizada, a la vez que cumple con sus necesidades de gobernanza.

Ventajas de este enfoque:

- El producto se aprovisiona y administra desde la cuenta principal y no se comparte con otras cuentas.
- Este enfoque proporciona una vista consolidada de todos los productos aprovisionados (pilas) basados en un producto específico.
- La configuración con AWS Service Management Connector es más sencilla, ya que solo se dirige a una cuenta.
- Es más fácil consultar y usar los productos de AWS Service Catalog.

Requisitos previos y limitaciones

Requisitos previos

- CloudFormation Plantillas de AWS para iAC y control de versiones
- Configuración de múltiples cuentas y AWS Service Catalog para aprovisionar y administrar los recursos de AWS

Limitaciones

- Este enfoque utiliza AWS CloudFormation StackSets y se StackSets aplican las siguientes limitaciones:
  - StackSets no admite el despliegue CloudFormation de plantillas a través de macros. Si utiliza una macro para preprocesar la plantilla, no podrá utilizar una implementación StackSets basada.
  - StackSets ofrece la posibilidad de desasociar una pila del conjunto de pilas, de forma que puedas segmentar una pila específica para solucionar un problema. Sin embargo, una pila disociada no se puede volver a asociar al conjunto de pilas.
- AWS Service Catalog genera StackSet nombres automáticamente. Actualmente, la solución no es personalizable.

Arquitectura

Arquitectura de destino

1. El usuario crea una CloudFormation plantilla de AWS para aprovisionar los recursos de AWS, en formato JSON o YAML.
2. La CloudFormation plantilla crea un producto en AWS Service Catalog, que se añade a una cartera.
3. El usuario crea un producto aprovisionado, que crea CloudFormation pilas en las cuentas de destino.
4. Cada pila aprovisiona los recursos especificados en las CloudFormation plantillas.

Herramientas

Servicios de AWS

- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- La Interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que permite interactuar con los servicios de AWS mediante comandos en el intérprete de comandos de línea de comandos.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Service Catalog le ayuda a administrar de forma centralizada los catálogos de servicios de TI aprobados para AWS. Los usuarios finales pueden implementar rápidamente solo los servicios de TI aprobados que necesitan, de acuerdo con las limitaciones establecidas por su organización.

Epics

Aprovisione productos entre cuentas

Tarea	Descripción	Habilidades requeridas
Cree una cartera.	Una cartera es un contenedor que incluye uno o más productos agrupados en función de criterios específicos. El uso de una cartera para sus productos le ayuda	AWS Service Catalog, IAM

Tarea	Descripción	Habilidades requeridas
	a aplicar restricciones comunes a todo su conjunto de productos. Para crear una cartera, siga las instrucciones de la documentación de AWS Service Catalog. Si usa la CLI de AWS, aquí tiene un comando de ejemplo: `aws servicecatalog create-portfolio --provider-name my-provider --display-name my-portfolio` Para obtener más información, consulte la documentación de AWS CLI.	
Cree una CloudFormation plantilla.	Cree una CloudFormation plantilla que describa los recursos. Los valores de las propiedades de los recursos deben parametrizarse cuando proceda.	AWS CloudFormation, JSON/YAML

Tarea	Descripción	Habilidades requeridas
Cree un producto con información sobre la versión.	La CloudFormation plantilla se convierte en un producto cuando se publica en AWS Service Catalog. Proporcione valores para los parámetro s de detalle de versión opcionales, como el título de la versión y la descripción. Estos datos le resultarán útiles para realizar consultas sobre el producto más adelante. Para crear un producto, siga las instrucciones de la documentación de AWS Service Catalog. Si utiliza la CLI de AWS, aquí tiene un comando de ejemplo: `aws servicecatalog create-product --cli-input-json file://create-product-input.json` `create-product-input.json` es el archivo que transfiere los parámetros del producto. Para obtener un ejemplo de este archivo, consulte la sección Información adicional. Para obtener más información, consulte la documentación de AWS CLI.	AWS Service Catalog

Tarea	Descripción	Habilidades requeridas
Aplique restricciones.	Aplique restricciones de conjunto de paquetes a la cartera para configurar las opciones de implementación del producto, como múltiples permisos, cuentas y regiones de AWS. Para obtener instrucciones, consulte la documentación de AWS Service Catalog.	AWS Service Catalog
Añada permisos.	Conceda permisos a los usuarios para que lancen los productos de la cartera. Para obtener instrucciones sobre su consola, consulte la documentación de AWS Service Catalog. Si usa la CLI de AWS, aquí tiene un comando de ejemplo: `aws servicecatalog associate-principal-with-portfolio \ --portfolio-id port-2s6abcdefwdh4 \ --principal-arn arn:aws:iam::444455556666:role/Admin \ --principal-type IAM` Para obtener más información, consulte la documentación de AWS CLI.	AWS Service Catalog, IAM

Tarea	Descripción	Habilidades requeridas
Aprovisione el producto.	Un producto aprovisionado es una instancia con recursos de un producto. Al aprovisionar un producto a partir de una CloudFormation plantilla, se lanza una CloudFormation pila y sus recursos subyacentes. Aprovisione el producto definiendo las regiones y cuentas de AWS aplicables en función de las restricciones del conjunto de pilas. En el AWS de CLI, se muestra un ejemplo de comando: `aws servicecatalog provision-product \ --product-id prod-abcdfz3syn2rg \ --provisioning-artifact-id pa-abc347pcsccfm \ --provisioned-product-name "mytestppname3"` Para obtener más información, consulte la documentación de AWS CLI.	AWS Service Catalog

Recursos relacionados

Referencias

- Información general sobre AWS Service Catalog

- Uso de AWS CloudFormation StackSets

Tutoriales y vídeos

- AWS re:Invent 2019: Automatícelo todo: opciones y prácticas recomendadas (vídeo)

Información adicional

Al usar el `create-product` comando, el `cli-input-json` parámetro apunta a un archivo que especifica información como el propietario del producto, el correo electrónico de soporte y los detalles de la CloudFormation plantilla. A continuación se muestra un ejemplo de este archivo:

```
{
   "Owner": "Test admin",
      "SupportDescription": "Testing",
         "Name": "SNS",
            "SupportEmail": "example@example.com",
            "ProductType": "CLOUD_FORMATION_TEMPLATE",
               "AcceptLanguage": "en",
                  "ProvisioningArtifactParameters": {
                     "Description": "SNS product",
                        "DisableTemplateValidation": true,
                           "Info": {
                              "LoadTemplateFromURL": "<url>"
                     },
                           "Name": "version 1"
}
```

Migración de una cuenta de miembro de AWS de AWS Organizations a AWS Control Tower

Creado por Rodolfo Jr. Cerrada (AWS)

Entorno: producción	Tecnologías: gestión y gobernanza; modernización	Servicios de AWS: AWS Organizations; AWS Control Tower

Resumen

Este patrón describe cómo migrar una cuenta de Amazon Web Services (AWS) de AWS Organizations, donde la cuenta de miembro está regida por una cuenta de administración, a AWS Control Tower. Al incluir la cuenta en AWS Control Tower, puede aprovechar las funciones y barreras de protección y detección que simplifican la gobernanza de su cuenta. Es posible que también desee migrar su cuenta de miembro si su cuenta de administración de AWS Organizations se ha visto comprometida. En este caso, puede trasladar las cuentas de los miembros a una nueva organización gobernada por AWS Control Tower.

AWS Control Tower proporciona un marco que combina e integra las capacidades de varios servicios de AWS, incluido AWS Organizations, y garantiza un cumplimiento y gobernanza coherentes en su entorno de múltiples cuentas. Con AWS Control Tower, puede seguir un conjunto de reglas y definiciones prescritas que amplían las capacidades de AWS Organizations. Por ejemplo, puede implantar barreras de protección para asegurar la creación de los permisos de acceso entre cuentas y registros de seguridad necesarios evitando posibles alteraciones.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- AWS Control Tower configurado en la organización de destino en AWS Organizations (para obtener más instrucciones, consulte Configuración en la documentación de AWS Control Tower)
- Credenciales de administrador de AWS Control Tower (miembro del AWSControlTowerAdminsgrupo)
- Credenciales de administrador de la cuenta de AWS de origen

Limitaciones

- La cuenta de administración de origen de AWS Organizations debe ser diferente de la cuenta de administración de destino de AWS Control Tower.

Versiones de producto

- AWS Control Tower versión 2.3 (febrero de 2020) o posterior (consulte las notas de versión)

Arquitectura

En el diagrama siguiente se ilustra el proceso de migración y la arquitectura de referencia. Este patrón migra la cuenta de AWS de la organización de origen a una organización de destino gobernada por AWS Control Tower.

El proceso de inscripción consta de estos pasos:

1. La cuenta deja la organización de origen en AWS Organizations.
2. La cuenta se convierte en una cuenta independiente. Esto significa que no pertenece a ninguna organización, por lo que los administradores de cuentas gestionan la gobernanza y la facturación de forma independiente.
3. La organización de destino envía una invitación para unir la cuenta a la organización.
4. La cuenta independiente acepta la invitación y pasa a ser miembro de la organización de destino.
5. La cuenta se incluye en AWS Control Tower y se pasa a una unidad organizativa (OU) registrada. (Le recomendamos que consulte el panel de control de AWS Control Tower para confirmar la inclusión). En este momento entran en vigor todas las barreras de protección habilitadas en la OU registrada.

Herramientas

Servicios de AWS

- AWS Organizations es un servicio de administración de cuentas que le permite unificar varias cuentas de AWS en una única entidad (una organización) que haya creado y administrado de forma centralizada.

- AWS Control Tower integra capacidades de otros servicios, como AWS Organizations, AWS IAM Identity Center (sucesor de AWS Single Sign-On) y AWS Service Catalog, para ayudarle a aplicar y administrar las normas de gobernanza de seguridad, operaciones y conformidad a escala en todas sus organizaciones y cuentas en la nube de AWS.

Epics

Eliminar la cuenta miembro de la organización fuente

Tarea	Descripción	Habilidades requeridas
Compruebe que la cuenta de miembro pueda funcionar como una cuenta independiente.	Confirme que la cuenta de miembro que abandonará la organización de origen tenga la información necesaria para funcionar como una cuenta independiente. Por ejemplo, si la cuenta del miembro no tiene información de facturación, no podrá operar como una cuenta independiente, ya que AWS usa la información de pago para cargar cualquier actividad de AWS facturable que se produzca mientras la cuenta no esté vinculada a una organización. Generalmente, cuando crea una cuenta miembro en la consola AWS Organizations, la API o los comandos de la interfaz de la línea de comandos (CLI) de AWS, no se recopila toda la información necesaria para las cuentas independientes de manera	Cuenta de administrador

Tarea	Descripción	Habilidades requeridas
	automática. Para añadir esta información, inicie sesión en la cuenta y especifique un plan de soporte, información de contacto y un método de pago. Para obtener más informaci ón sobre lo que necesita saber antes de eliminar una cuenta de una organización, consulte Antes de eliminar una cuenta de la organización en la documentación de AWS Organizations.	

Tarea	Descripción	Habilidades requeridas
Elimine la cuenta de miembro de la organización de origen.	Siga las instrucciones de la documentación de AWS Organizations para eliminar una cuenta de miembro de una organización. Puede iniciar sesión en la cuenta de administración de la organización y eliminar la cuenta de miembro, o iniciar sesión en la cuenta de miembro y salir de la organización. Si no tiene credenciales de administrador para eliminar o abandonar la cuenta, solicite ayuda al administrador de su organización. Si a la cuenta de miembro le falta un plan de asistencia, información de contacto o información de pago, se le pedirá que proporcione y verifique esa información. Cuando deje la organización, se le redirigirá a la página Introducción de la consola de AWS Organizations, donde podrá ver las invitaciones pendientes de su cuenta para unirse a otras organizaciones. Importante: desde este momento, su cuenta es una cuenta independiente. Si	Administrador de cuentas de administración o administrador de cuentas

Tarea	Descripción	Habilidades requeridas
	ejecuta cargas de trabajo no cubiertas por el nivel gratuito de AWS, se le cobrará según la información de pago y facturación que haya proporcionado para la cuenta.	
Compruebe que la cuenta de miembro ya no forma parte de la organización de origen.	En la consola de AWS Organizations, ya no debería ver el botón Abandonar la organización. En su lugar, debería ver las invitaciones pendientes, si las hay, de otras organizaciones.	Cuenta de administrador

Tarea	Descripción	Habilidades requeridas
Elimine los roles de IAM que conceden acceso a su cuenta de la organización que ha dejado.	Al eliminar la cuenta de la organización de origen, las funciones de AWS Identity and Access Management (IAM) creadas por AWS Organizations o por los administradores no se eliminarán automáticamente. Si desea eliminar este acceso desde la cuenta de administración anterior de la organización, debe eliminar los roles de IAM manualmente. Para obtener más información, consulte Eliminación de roles o perfiles de instancia en la documentación de IAM. Cuando una cuenta miembro abandona una organización, se eliminan todas las etiquetas asociadas a la cuenta. Las cuentas independientes no admiten etiquetas.	Cuenta de administrador

Invite a la cuenta a unirse a la nueva organización con AWS Control Tower

Tarea	Descripción	Habilidades requeridas
Inicie sesión en AWS Control Tower.	Inicie sesión en la consola de AWS Control Tower como administrador. Actualmente, no existe una forma directa de pasar una cuenta de AWS de una	Administrador de AWS Control Tower

Tarea	Descripción	Habilidades requeridas
	organización de origen a una organización de una OU gobernada por AWS Control Tower. Sin embargo, puede ampliar la gobernanza de AWS Control Tower a una cuenta de AWS existente al inscribirla en una OU que ya esté gobernada por AWS Control Tower. Por ello, debe iniciar sesión en AWS Control Tower para realizar este paso.	

Tarea	Descripción	Habilidades requeridas
Invitar la cuenta miembro.	1. Inicie sesión en la consola de AWS Organizations y acceda a la página Cuentas de AWS. 2. En la página Agregar una cuenta AWS, seleccione Invitar una cuenta de AWS existente. 3. Complete la información de la cuenta, incluido el número de cuenta de 12 dígitos (sin guiones), la descripción y las etiquetas opcionales, y seleccione Enviar invitación. Importante: compruebe que la transferencia de la cuenta no afectará a ninguna aplicación ni a la conectividad de red. Esta acción envía un correo electrónico de invitación con un enlace a la cuenta de miembro. Cuando el administrador de la cuenta sigue el enlace y acepta la invitación, la cuenta del miembro aparece en la página de Cuentas de AWS. Para obtener más información, consulte Invitar una cuenta de AWS a unirse a su organizac	Administrador de AWS Control Tower

Tarea	Descripción	Habilidades requeridas
	ión. en la documentación de AWS Organizations.	

Tarea	Descripción	Habilidades requeridas
Pruebe las aplicaciones y la conectividad.	Cuando la cuenta del miembro se haya registrado en la nueva organización, aparecerá en la OU dentro de una raíz. También aparecerá en la consola de AWS Control Tower marcada como no incluida en ninguna cuenta, ya que aún no se ha inscrito en la OU registrada de AWS Control Tower. Compruebe lo siguiente: • Consulte el panel de control de AWS Control Tower para comprobar si hay alguna infracción de barreras de protección. • Compruebe la conectividad de la red (VPN o AWS Direct Connect) para asegurarse de que no se haya visto afectada por la transferencia. • (Propietarios de aplicación) Pruebe las aplicaciones asociadas a esta cuenta para comprobar que se ejecutan según lo previsto, y que la transferencia de la cuenta no ha afectado a las dependencias.	Administrador de AWS Control Tower, administrador de cuentas de miembros, propietarios de aplicación

Prepare la cuenta para la inclusión

Tarea	Descripción	Habilidades requeridas
Revise las barreras de protección y corrija cualquier infracción.	Revise las barreras de protección definidas en la OU de destino, especialmente las barreras preventivas, y corrija cualquier posible infracción. Al configurar la zona de aterrizaje de AWS Control Tower, se habilitan de forma predeterminada varias barreras de protección obligatorias y preventivas. Estas barreras no se pueden desactivar. Deberá revisarla s y reparar la cuenta de miembro (manualmente o mediante un script) antes de inscribirla. Nota: Las barreras de protección preventivas mantienen el cumplimiento de las cuentas registradas de AWS Control Tower y evitan el incumplimiento de las políticas. Cualquier infracción de las barreras de protección preventivas podría afectar a la inclusión. Si se detectan, las infracciones de las barreras de protección aparecerán en el panel de AWS Control Tower tras la correcta inclusión de	Administrador de AWS Control Tower, administrador de cuentas de miembros

Tarea	Descripción	Habilidades requeridas
	la cuenta. No afectarán al proceso de inscripción. Para obtener más información, consulte barrera de protección en AWS Control Tower en la documentación de AWS.	
Compruebe si hay problemas de conectividad después de corregir las infracciones de las barreras de protección.	En algunos casos, es posible que tenga que cerrar puertos específicos o desactivar servicios para corregir las infracciones de barreras de protección. Asegúrese de corregir las aplicaciones que usan esos puertos y servicios antes de inscribir la cuenta.	Propietario de la aplicación

Incluya la cuenta en AWS Control Tower

Tarea	Descripción	Habilidades requeridas
Inicie sesión en la consola de AWS Control Tower.	Use credenciales de inicio de sesión con permisos administrativos para AWS Control Tower. No use las credenciales del usuario raíz (cuenta de administración) para inscribir una cuenta de AWS Organizations. Aparecerá un mensaje de error.	Administrador de AWS Control Tower
Inscriba la cuenta.	1. En la página Account Factory de AWS Control Tower, elija Inscribir cuenta.	Administrador de AWS Control Tower

Tarea	Descripción	Habilidades requeridas
	2. Complete los detalles, incluida la dirección de correo electrónico asociada a la cuenta que desea inscribir, el nombre visible que aparecerá en AWS Control Tower, la dirección de correo electrónico de IAM Identity Center, el nombre y apellidos del propietario de la cuenta y la OU en la que desea incluir la cuenta. La dirección de correo electrónico de IAM Identity Center es su dirección de correo electrónico de usuario preferida. Puede usar la misma dirección de correo electrónico que la cuenta. 3. Seleccione Enroll account (Inscribir cuenta). Para obtener más información, consulte Inscribir una cuenta existente en la documentación de AWS Control Tower.	

Verifique la cuenta después de la inscripción

Tarea	Descripción	Habilidades requeridas
Verifique la cuenta.	En AWS Control Tower, elija Cuentas. La cuenta que acaba de inscribir tendrá el estado inicial Inscribiendo. Cuando se complete la inscripción, su estado cambiará a Inscrito.	Administrador de AWS Control Tower, administrador de cuentas de miembros
Compruebe si hay infraccio nes de barreras de protección.	Las barreras de protecció n definidas en la OU se aplicarán automáticamente a la cuenta del miembro inscrito. Supervise el panel de control de AWS Control Tower para detectar posibles infracciones y corríjalas en consecuencia. Para obtener más información, consulte barrera de protecció n en AWS Control Tower en la documentación de AWS.	Administrador de AWS Control Tower, administrador de cuentas de miembros

Solución de problemas

Problema	Solución
Recibe el mensaje de error: Se ha producido un error desconocido. Vuelva a intentarlo más tarde o póngase en contacto con AWS Support.	Este error se produce cuando usa las credenciales de usuario raíz (cuenta de administración) en AWS Control Tower para inscribir una cuenta nueva. AWS Service Catalog no puede asignar la cartera o el producto de Account Factory al usuario raíz, lo que genera un mensaje de error. Para corregir este error, introduzca credenciales de usuario

Problema	Solución
	(administrador) que no sean raíz y tengan acceso completo para inscribir la nueva cuenta. Para obtener más información sobre cómo asignar acceso administrativo a un usuario administrativo, consulte la Introducción en la documentación de AWS IAM Identity Center (sucesor de AWS Single Sign-On).
La página Actividades de AWS Control Tower muestra la acción Desviación catastrófica.	Esta acción refleja una comprobación de desviación del servicio, y no indica ningún problema con la configuración de AWS Control Tower. No hay que hacer nada más.

Recursos relacionados

Documentación

- Terminología y conceptos de AWS Organizations (Guía del usuario de AWS Organizations)
- ¿Qué es AWS Control Tower? (documentación de AWS Control Tower)
- Eliminar una cuenta de miembro de su organización (documentación de AWS Organizations)
- Crear una cuenta de administrador en AWS Control Tower (documentación de AWS Control Tower)

Tutoriales y videos

- Taller sobre AWS Control Tower (taller autogestionado)
- ¿Qué es AWS Control Tower? (video)
- Aprovisionamiento de usuarios en AWS Control Tower (video)
- Habilitar AWS Control Tower para organizaciones existentes (video)

Supervisar el uso de una imagen de máquina de Amazon compartida en varias cuentas de AWS

Creado por Naveen Suthar (AWS) y Sandeep Gawande (AWS)

Repositorio de código: - terraform-samples cross-account-ami-auditing	Entorno: PoC o piloto	Tecnologías: administración y gobierno; sin servidor; operaciones DevOps
Servicios de AWS: Amazon DynamoDB; AWS Lambda; Amazon EventBridge		

Resumen

Las Imágenes de máquina de Amazon (AMI) se utilizan para crear instancias de Amazon Elastic Compute Cloud (Amazon EC2) en su entorno de Amazon Web Services (AWS). Puede crear AMI en una cuenta de AWS independiente y centralizada, que en este patrón se denomina cuenta de creador. A continuación, puede compartir la AMI entre varias cuentas de AWS que estén en la misma región de AWS, que se denominan cuentas de consumidor en este patrón. La administración de las AMI desde una sola cuenta proporciona escalabilidad y simplifica la gobernanza. En las cuentas de consumidor, puede hacer referencia a la AMI compartida en las plantillas de lanzamiento de Amazon EC2 Auto Scaling y en los grupos de nodos de Amazon Elastic Kubernetes Service (Amazon EKS).

Cuando una AMI compartida queda obsoleta, se anula su registro o se deja de compartir, los servicios de AWS que hacen referencia a la AMI en las cuentas de consumidor no pueden usar esta AMI para lanzar nuevas instancias. Se produce un error en cualquier evento de escalado automático o en el relanzamiento de la misma instancia. Esto puede provocar problemas en el entorno de producción, como el tiempo de inactividad de las aplicaciones o la degradación del rendimiento. Cuando se producen eventos de uso compartido y de uso de la AMI en varias cuentas de AWS, puede ser difícil supervisar esta actividad.

Este patrón ayuda a supervisar el uso y el estado de la AMI compartida en cuentas de la misma región. Utiliza servicios de AWS sin servidor, como Amazon EventBridge, Amazon DynamoDB, AWS Lambda y Amazon Simple Email Service (Amazon SES). La infraestructura se aprovisiona como

código (IaC) mediante Terraform. HashiCorp Esta solución proporciona alertas cuando un servicio de una cuenta de consumidor hace referencia a una AMI que ya no está registrada o compartida.

Requisitos previos y limitaciones

Requisitos previos

- Dos o más cuentas de AWS activas: una cuenta de creador y una o más cuentas de consumidor
- Una o más AMI que se comparten desde la cuenta de creador a una cuenta de consumidor
- Terraform CLI, instalada (documentación de Terraform)
- Terraform AWS Provider, configurado (documentación de Terraform)
- (Opcional, pero recomendado) Backend de Terraform, configurado (documentación de Terraform)
- Git, instalado

Limitaciones

- Este patrón supervisa las AMI que se han compartido con cuentas específicas mediante el ID de la cuenta. Este patrón no supervisa las AMI que se han compartido con una organización mediante el ID de la organización.
- Las AMI solo se pueden compartir con cuentas que se encuentren dentro de la misma región de AWS. Este patrón supervisa las AMI dentro de una única región de destino. Para supervisar el uso de las AMI en varias regiones, implemente esta solución en cada región.
- Este patrón no supervisa ninguna AMI que se compartiera antes de implementar esta solución. Si desea supervisar las AMI compartidas anteriormente, puede dejar de compartir la AMI y, a continuación, volver a compartirla con las cuentas de consumidor.

Versiones de producto

- Versión de Terraform 1.2.0 o posterior
- Versión de Terraform AWS Provider 4.20 o posterior

Arquitectura

Pila de tecnología de destino

Los recursos siguientes se aprovisionan como IaC a través de Terraform:

- Tablas de Amazon DynamoDB
- EventBridge Reglas de Amazon
- Rol de AWS Identity and Access Management (IAM)
- Funciones de AWS Lambda
- Amazon SES

Arquitectura de destino

En el diagrama, se muestra el siguiente flujo de trabajo:

1. La AMI de la cuenta de creador se comparte con una cuenta de consumidor de la misma región de AWS.
2. Cuando se comparte la AMI, una EventBridge regla de Amazon en la cuenta del creador captura el `ModifyImageAttribute` evento e inicia una función Lambda en la cuenta del creador.
3. La función de Lambda almacena los datos relacionados con la AMI en una tabla de DynamoDB de la cuenta de creador.
4. Cuando un servicio de AWS de la cuenta del consumidor utiliza la AMI compartida para lanzar una instancia de Amazon EC2 o cuando la AMI compartida está asociada a una plantilla de lanzamiento, una EventBridge regla de la cuenta del consumidor captura el uso de la AMI compartida.
5. La EventBridge regla inicia una función Lambda en la cuenta del consumidor. La función de Lambda lleva a cabo lo siguiente:
   a. La función de Lambda actualiza los datos relacionados con la AMI en una tabla de DynamoDB de la cuenta de consumidor.
   b. La función de Lambda asume un rol de IAM en la cuenta de creador y actualiza la tabla de DynamoDB de la cuenta de creador. En la tabla `Mapping`, crea un elemento que asigna el ID de instancia o el ID de plantilla de lanzamiento a su ID de AMI correspondiente.
6. La AMI que se administra de forma centralizada en la cuenta de creador está obsoleta, se ha anulado su registro o ha dejado de compartirse.
7. La EventBridge regla de la cuenta del creador captura el `DeregisterImage` evento `ModifyImageAttribute` o con la `remove` acción e inicia la función Lambda.

8. La función de Lambda comprueba la tabla de DynamoDB para determinar si la AMI se utiliza en alguna de las cuentas de consumidor. Si en la tabla `Mapping` no hay ningún ID de instancia o ID de plantilla de lanzamiento asociado a la AMI, el proceso se ha completado.
9. Si hay algún ID de instancia o ID de plantilla de lanzamiento asociado a la AMI en la tabla `Mapping`, la función de Lambda utiliza Amazon SES para enviar una notificación por correo electrónico a los suscriptores configurados.

Herramientas

Servicios de AWS

- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, las funciones de Lambda de AWS, los puntos de conexión de invocación HTTP que utilizan destinos de API o los buses de eventos de otras cuentas de AWS.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Email Service (Amazon SES) facilita poder enviar y recibir correos electrónicos a través de los dominios y direcciones de correo electrónico propios.

Otras herramientas

- HashiCorp Terraform es una herramienta de código abierto de infraestructura como código (IaC) que le ayuda a usar el código para aprovisionar y administrar la infraestructura y los recursos de la nube.
- Python es un lenguaje de programación informático de uso general.

Repositorio de código

El código de este patrón está disponible en el repositorio -terraform-samples. GitHub cross-account-ami-monitoring

Prácticas recomendadas

- Siga las Prácticas recomendadas para trabajar con funciones de Lambda de AWS.
- Siga las Prácticas recomendadas para crear AMI.
- Al crear el rol de IAM, siga el principio del privilegio mínimo y conceda los permisos mínimos necesarios para llevar a cabo cada tarea. Para obtener más información, consulte Otorgar privilegio mínimo y Prácticas recomendadas de seguridad en la documentación de IAM.
- Configure la supervisión y las alertas para las funciones de Lambda de AWS. Para obtener más información, consulte Supervisión y solución de problemas de funciones de Lambda.

Epics

Personalizar los archivos de configuración de Terraform

Tarea	Descripción	Habilidades requeridas
Cree los perfiles con nombre de AWS CLI.	Para la cuenta de creador y para cada cuenta de consumidor, cree un perfil con nombre de Interfaz de la línea de comandos de AWS (AWS CLI). Si necesita instrucciones, consulte Configuración de AWS CLI en el Centro de recursos de introducción a AWS.	DevOps ingeniero
Clonar el repositorio.	Escriba el siguiente comando. Esto clona el repositorio cross-account-ami-monitoring-terraform-samples mediante SSH. GitHub	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`git clone git@github.com:aws-samples/cross-account-ami-monitoring-terraform-samples.git`	

Tarea	Descripción	Habilidades requeridas
Actualice el archivo provider.tf.	1. Ingrese el comando siguiente para acceder a la carpeta `terraform` del repositorio clonado. `cd cross-account-ami-monitoring/terraform` 2. Abra el archivo `provider.tf` . 3. Actualice las configuraciones de Terraform AWS Provider para la cuenta de creador y la cuenta de consumidor de la manera siguiente: • En `alias`, especifique un nombre para la configuración del proveedor. • En `region`, especifique la región de AWS de destino en la que desea implementar esta solución. • En `profile`, especifique el nombre de perfil de AWS CLI para acceder a la cuenta. 4. Si va a configurar más de una cuenta de consumidor, cree un perfil para cada cuenta de consumidor adicional.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	5. Guarde y cierre el archivo `provider.tf` . Para más información sobre la configuración de proveedor es, consulte Configuraciones de varios proveedores en la documentación de Terraform.	

Tarea	Descripción	Habilidades requeridas
Actualice el archivo terraform .tfvars.	1. Abra el archivo `terraform.tfvars` . 2. En el parámetro `account_email_mapping` , configure las alertas para la cuenta de creador y la cuenta de consumidor de la manera siguiente: • En `account`, especifique el ID de la cuenta. • En `email`, especifique la dirección de email a la que desea enviar alertas. Solo puede especificar una dirección de correo electrónico para cada cuenta. 3. Si va a configurar más de una cuenta de consumidor, especifique una cuenta y una dirección de correo electrónico para cada cuenta de consumidor adicional. 4. Guarde y cierre el archivo `terraform.tfvars` .	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Actualice el archivo main.tf.	Siga estos pasos solo si va a implementar esta solución en más de una cuenta de consumidor. Si va a implementar esta solución en una sola cuenta de consumidor, no es necesario modificar este archivo. 1. Abra el archivo `main.tf`. 2. Para cada cuenta de consumidor adicional, cree un módulo nuevo que se base en el módulo `consumer_account_A` de la plantilla. Para cada cuenta de consumidor, el valor de `provider` debe coincidir con el alias que especificó en el archivo `provider.tf` . 3. Guarde y cierre el archivo `main.tf`.	DevOps ingeniero

Implementar la solución mediante Terraform

Tarea	Descripción	Habilidades requeridas
Implemente la solución.	En la CLI de Terraform, ingrese los comandos siguientes para implementar los recursos de AWS en las cuentas de creador y de consumidor:	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	1. Ingrese el comando siguiente para inicializar Terraform. `terraform init` 2. Ingrese el comando siguiente para validar las configuraciones de Terraform. `terraform validate` 3. Ingrese el comando siguiente para crear un plan de ejecución de Terraform. `terraform plan` 4. Revise los cambios de configuración en el plan de Terraform y confirme que desea implementarlos. 5. Ingrese el comando siguiente para implementar los recursos. `terraform apply`	

Tarea	Descripción	Habilidades requeridas
Verificar la identidad de la dirección de correo electrónico.	Al implementar el plan Terraform, Terraform crea una identidad de dirección de correo electrónico para cada cuenta de consumidor en Amazon SES. Para poder enviar notificaciones a esa dirección de correo electrónico, es necesario verificarla. Para las instrucciones, consulte Verificación de la identidad de una dirección de correo electrónico en la documentación de Amazon SES.	AWS general

Validar la implementación de recursos

Tarea	Descripción	Habilidades requeridas
Valide la implementación en la cuenta de creador.	1. Inicie sesión en la cuenta de creador. 2. En la barra de navegación, confirme que ve la región de destino. Si se encuentra en una región diferente, seleccione el nombre de región que se muestra y la región de destino. 3. Abra la consola de DynamoDB en https://console.aws.amazon.com/dynamodb/.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	4. En el panel de navegación, elija Tablas. 5. En la lista de tablas, compruebe que la tabla `AmiShare` esté presente. 6. Abra la consola de Lambda en https://console.aws.amazon.com/lambda. 7. Seleccione Funciones en el panel de navegación. 8. En la lista de funciones, compruebe que la función `ami-share` esté presente. 9. Abra la consola de IAM en https://console.aws.amazon.com/iamv2/. 10. Seleccione Roles en el panel de navegación. 11. En la lista de roles, compruebe que el rol `external-ddb-role` esté presente. 12. Abra la EventBridge consola en https://console.aws.amazon.com/events/. 13. En el panel de navegación, seleccione Reglas. 14. En la lista de reglas, compruebe que la regla `modify_image_attribute_event` esté presente.	

Tarea	Descripción	Habilidades requeridas
	15 Abra la consola de Amazon SES en https:/console.aws.amazon.com/ses/. 16 En el panel de navegación, seleccione Verified identities (Identidades verificadas). 17 En la lista de identidades, compruebe que se haya registrado y verificado la identidad de una dirección de correo electrónico para cada cuenta de consumidor.	

Tarea	Descripción	Habilidades requeridas
Valide la implementación en la cuenta de consumidor.	1. Inicie sesión en la cuenta de consumidor. 2. En la barra de navegación, confirme que ve la región de destino. Si se encuentra en una región diferente, seleccione el nombre de región que se muestra y la región de destino. 3. Abra la consola de DynamoDB en https://console.aws.amazon.com/dynamodb/. 4. En el panel de navegación, elija Tablas. 5. En la lista de tablas, compruebe que la tabla `Mapping` esté presente. 6. Abra la consola de Lambda en https://console.aws.amazon.com/lambda. 7. Seleccione Funciones en el panel de navegación. 8. En la lista de funciones, compruebe que las funciones `ami-usage-function` y `ami-deregister-function` estén presentes. 9. Abra la EventBridge consola en https://console.aws.amazon.com/events/.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	10 En el panel de navegación, seleccione Reglas. 11 En la lista de reglas, compruebe que las reglas `ami_usage_events` y `ami_deregister_events` estén presentes.	

Validar la supervisión

Tarea	Descripción	Habilidades requeridas
Cree una AMI en la cuenta de creador.	1. Cree una AMI privada en la cuenta de creador. Para obtener instrucciones, consulte Crear una AMI a partir de una instancia de Amazon EC2. 2. Comparta la nueva AMI con una de las cuentas de consumidor. Para obtener instrucciones, consulte Compartir una AMI con cuentas de AWS específicas.	DevOps ingeniero
Use la AMI en la cuenta de consumidor.	En la cuenta de consumidor, utilice la AMI compartida para crear una instancia de EC2 o una plantilla de lanzamiento. Para obtener instrucciones, consulte Cómo puedo lanzar una instancia de EC2 desde una AMI personalizada (AWS	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Re:post Knowledge Center) o Cómo crear una plantilla de lanzamiento (document ación de Amazon EC2 Auto Scaling).	
Valide la supervisión y las alertas.	1. Inicie sesión en la cuenta de creador. 2. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/. 3. En el panel de navegación, seleccione AMIs. 4. Seleccione la AMI en la lista y, a continuación, Actions (Acciones), Edit AMI permissions (Editar permisos de la AMI). 5. En la sección Shared accounts (Cuentas compartidas), seleccione la cuenta de consumidor y, a continuación, Remove selected (Eliminar lo seleccionado). 6. Seleccione Save changes (Guardar cambios). 7. Valide que la dirección de correo electrónico de destino que definió para la cuenta de consumidor reciba una notificación de cancelación del uso compartido de la AMI.	DevOps ingeniero

(Opcional) Dejar de supervisar las AMI compartidas

Tarea	Descripción	Habilidades requeridas
Elimine los recursos.	1. Ingrese el comando siguiente para eliminar los recursos implement ados por este patrón y dejar de supervisar las AMI compartidas. `terraform destroy` 2. Confirme el comando `destroy`; para hacerlo, especifique `yes`.	DevOps ingeniero

Solución de problemas

Problema	Solución
No he recibido ninguna alerta por correo electrónico.	Puede haber varios motivos por los que no se envió el correo electrónico de Amazon SES. Compruebe lo siguiente: 1. En la sección Epics, utilice el resumen Validar la implementación de recursos para confirmar que la infraestructura se aprovisio nó correctamente en todas las cuentas de AWS. 2. Valide los eventos de la función Lambda en Amazon CloudWatch Logs. Para obtener instrucciones, consulte Uso de la CloudWatc h consola en la documentación de Lambda. Confirme que los permisos no tengan ningún problema, como una denegación explícita

Problema	Solución
	en una política basada en la identidad o en los recursos. Para obtener más información, consulte Lógica de evaluación de políticas en la documentación de IAM. 3. En Amazon SES, compruebe que el estado de la identidad de la dirección de correo electrónico sea Verified (Verificado). Para obtener más información, consulte Verificación de identidades de correo electrónico.

Recursos relacionados

Documentación de AWS

- Creación de funciones de Lambda con Python (documentación de Lambda)
- Creación de una AMI (documentación de Amazon EC2)
- Compartir una AMI con cuentas de AWS específicas (documentación de Amazon EC2)
- Anular el registro de la AMI (documentación de Amazon EC2)

Documentación de Terraform

- Instalar Terraform
- Configuración del backend de Terraform
- Proveedor de AWS para Terraform
- Descarga binaria de Terraform

Configure alertas para el cierre programático de cuentas en AWS Organizations

Creado por Richard Milner-Watts (AWS), Debojit Bhadra (AWS) y Manav Yadav (AWS)

Repositorio de código: Notificador de cierre de cuentas de AWS	Entorno: producción	Tecnologías: administración y gobierno
Servicios de AWS: AWS CloudTrail; Amazon EventBridge; AWS Lambda; AWS Organizations; Amazon SNS		

Resumen

La CloseAccount API para AWS Organizations le permite cerrar las cuentas de los miembros de una organización mediante programación, sin tener que iniciar sesión en la cuenta con las credenciales raíz. La RemoveAccountFromOrganization API extrae una cuenta de una organización en AWS Organizations, por lo que pasa a ser una cuenta independiente.

Estas API pueden aumentar el número de operadores que pueden cerrar o eliminar una cuenta de AWS. Todos los usuarios que tengan acceso a la organización a través de AWS Identity and Access Management (IAM) en la cuenta de administración de AWS Organizations pueden llamar a estas API, por lo que el acceso no se limita al propietario del correo raíz de la cuenta con ningún dispositivo de autenticación multifactor (MFA) asociado.

Este patrón implementa alertas cuando se llama a las API `CloseAccount` y `RemoveAccountFromOrganization`, de este modo usted puede supervisar estas actividades. Para alertas, utiliza un tema de Amazon Simple Notification Service (Amazon SNS) También puede configurar las notificaciones de Slack mediante un webhook.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa

- Una organización en AWS Organizations
- Acceso a la cuenta de administración de la organización, ubicada en la raíz de la organización, para crear los recursos necesarios

Limitaciones

- Como se describe en la referencia de la API de AWS Organizations, la API `CloseAccount` permite cerrar solo el 10 % de las cuentas de los miembros activos en un período continuo de 30 días.
- Cuando se cierra una cuenta de AWS, su estado cambia a SUSPENDIDA. Durante 90 días después de esta transición de estado, AWS Support puede volver a abrir la cuenta. La cuenta se elimina permanentemente después de 90 días.
- Los usuarios que tienen acceso a la cuenta de administración y a las API de AWS Organizations también pueden tener permisos para deshabilitar estas alertas. Si lo que más preocupa es un comportamiento malicioso en lugar de una eliminación accidental, considere la posibilidad de proteger los recursos creados por este patrón con un límite de permisos de IAM.
- La API llama a `CloseAccount` y `RemoveAccountFromOrganization` procesa mediante la región Este de EE. UU. (Norte de Virginia) (`us-east-1`). Por lo tanto, usted debe implementar esta solución en `us-east-1` para poder observar los eventos.

Arquitectura

Pila de tecnología de destino

- AWS Organizations
- AWS CloudTrail
- Amazon EventBridge
- AWS Lambda
- Amazon SNS

Arquitectura de destino

El siguiente diagrama muestra la arquitectura de soluciones para este patrón.

1. AWS Organizations procesa una solicitud `CloseAccount` o `RemoveAccountFromOrganization`.
2. Amazon EventBridge está integrado con AWS CloudTrail para enviar estos eventos al bus de eventos predeterminado.
3. Una EventBridge regla de Amazon personalizada coincide con las solicitudes de AWS Organizations y llama a una función de AWS Lambda.
4. La función de Lambda envía un mensaje a un tema de SNS, al que los usuarios pueden suscribirse para recibir alertas por correo electrónico o para su posterior procesamiento.
5. Si las notificaciones de Slack están habilitadas, la función de Lambda envía un mensaje a un webhook de Slack.

Herramientas

Servicios de AWS

- AWS CloudFormation proporciona una forma de modelar un conjunto de recursos relacionados de AWS y de terceros, aprovisionarlos de forma rápida y coherente y gestionarlos a lo largo de sus ciclos de vida, tratando la infraestructura como código.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que puede utilizar para conectar sus aplicaciones con datos de diversas fuentes. EventBridge recibe un evento, un indicador de un cambio en el entorno, y aplica una regla para enrutar el evento a un objetivo. Las reglas hacen coincidir los eventos con los objetivos o bien en función de la estructura del evento, llamado un patrón de evento, o bien de una programación.
- AWS Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo. Solo paga por el tiempo de proceso que consume. No se aplican cargos cuando su código no se está ejecutando.
- AWS Organizations le ayuda a administrar y gobernar su entorno de forma centralizada a medida que hace crecer y escalar sus recursos de AWS. Con AWS Organizations, puede crear nuevas cuentas de AWS y asignar recursos mediante programación, agrupar cuentas para organizar sus flujos de trabajo, aplicar políticas a cuentas o grupos para el control y simplificar la facturación mediante un único método de pago para todas sus cuentas.
- AWS CloudTrail monitorea y registra la actividad de las cuentas en toda su infraestructura de AWS y le permite controlar las acciones de almacenamiento, análisis y corrección.

- Amazon Simple Notification Service (Amazon SNS) es un servicio de mensajería totalmente gestionado para application-to-application la comunicación (A2A) application-to-person y (A2P).

Otras herramientas

- La biblioteca AWS Lambda Powertools para Python es un conjunto de utilidades que proporcionan funciones de seguimiento, registro, métricas y gestión de eventos para las funciones de Lambda.

Code

El código de este patrón se encuentra en el repositorio GitHub AWS Account Closer Notifier.

La solución incluye una CloudFormation plantilla que implementa la arquitectura de este patrón. Utilice la biblioteca AWS Lambda Powertools para Python para proporcionar registro y seguimiento.

Epics

Implementación de la arquitectura

Tarea	Descripción	Habilidades requeridas
Lance la CloudFormation plantilla para la pila de soluciones.	La CloudFormation plantilla para este patrón se encuentra en la rama principal del GitHub repositorio. Implement a las funciones de IAM, EventBridge las reglas, las funciones de Lambda y el tema SNS. Para iniciar la plantilla: 1. Clone el GitHub repositorio para obtener una copia del código de la solución. 2. Abra la consola de administración de AWS para la cuenta de administr	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	ación de AWS Organizations. 3. Elija la región EE.UU. Este (Norte de Virginia) (`us-east-1`) y, a continuación, abra la CloudFormation consola. 4. Cree la pila utilizando la plantilla `account-closure-notifier.yml` y especificando los siguientes valores: • Nombre de pila: `aws-account-closure-notifier-stack` • Parámetro `ResourcePrefix`: `aws-account-closure-notifier` • Parámetro `SlackNotification`: si se requieren notificaciones de Slack, cambie esta configuración a `true`. • Parámetro `SlackWebhookEndpoint`: si se requieren notificaciones de Slack, especifique la URL del webhook. Para obtener más información sobre el lanzamiento de una	

Tarea	Descripción	Habilidades requeridas
	CloudFormation pila, consulte la documentación de AWS.	
Compruebe que la solución se haya lanzado correctamente.	1. Espere a que la CloudFormation pila alcance el estado CREATE_COMPLETE. 2. Abre la consola. EventBridge `us-east-1` 3. Compruebe que se haya creado una nueva regla con ese nombre `aws-account-closure-notifier-event-rule` .	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Suscríbase al tema de SNS.	(Opcional) Si quiere suscribir se al tema de SNS: 1. Abra la consola de Amazon SNS en `us-east-1` y busque el tema denominado `aws-account-closure-notifier-sns-topic`. 2. Elija el nombre del tema y, a continuación, elija Create subscription (Crear suscripción). 3. En Protocol (Protocolo), elija Email (Correo electrónico). 4. En Endpoint (Punto de conexión), escriba una dirección de correo electrónico que puede utilizar para recibir la notificación y, a continuación, elija Create subscription (Crear suscripción). 5. Revise su bandeja de entrada de correo electrónico para ver si hay algún mensaje de AWS Notifications. Utilice el enlace del correo electrónico para confirmar la suscripción. Para obtener más información acerca de la configuración	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	de notificaciones de SNS, consulte la documentación de Amazon SNS.	

Verificación de la solución

Tarea	Descripción	Habilidades requeridas
Envíe un evento de prueba al bus de eventos predeterminado.	El GitHub repositorio proporciona un ejemplo de evento que puede enviar al bus de eventos EventBridge predeterminado para probarlo. La EventBridge regla también reacciona ante los eventos que utilizan la fuente de eventos personalizada `aws.accountclosure.notifier`. Nota: No puede usar la fuente del CloudTrail evento para enviar este evento, ya que no es posible enviar un evento como un servicio de AWS. Para enviar un evento de prueba: 1. Abre la EventBridge consola en `us-east-1`. 2. En el panel de navegación, en Buses, elija Event buses (Buses de eventos) y, a continuación, seleccione el	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	bus de eventos predeterminado. 3. Seleccione Send events (Enviar eventos). 4. En Event source (Origen del evento), introduzca `account.closure.notifier` . 5. En Detail type (Tipo de detalle), introduzca `AWS API Call via CloudTrail` . 6. Para ver los detalles del evento, copia y pega el contenido `tests/dummy-event.json` del GitHub repositorio en el cuadro de texto. 7. Seleccione Send (Enviar) para iniciar el flujo de trabajo de notificaciones.	
Compruebe que se ha recibido la notificación por correo electrónico.	Compruebe si hay notificaciones en el buzón de correo que se suscribió al tema de SNS. Usted debería recibir un correo electrónico con la información sobre la cuenta que se cerró y la entidad principal que realizó la llamada a la API.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Verifique que se haya recibido la notificación de Slack.	(Opcional) Si especificaste una URL de webhook para el `SlackWebhookEndpoint` parámetro al implementar la CloudFormation plantilla, comprueba el canal de Slack que está asignado al webhook. Debería mostrar un mensaje con la información de la cuenta que se cerró y de la entidad principal que realizó la llamada a la API.	Administrador de AWS

Recursos relacionados

- CloseAccount acción (referencia de la API de AWS Organizations)
- RemoveAccountFromOrganization acción (referencia de la API de AWS Organizations)
- AWS Lambda Powertools para Python

Más patrones

- Automatice la evaluación de recursos de AWS
- Automatice la implementación de productos y la cartera de AWS Service Catalog mediante AWS CDK
- Adjunte automáticamente una política administrada de AWS para Systems Manager a los perfiles de instancia de EC2 mediante Cloud Custodian y AWS CDK
- Cifrar automáticamente los volúmenes de Amazon EBS nuevos y existentes
- Registro centralizado y barrera de protección para varias cuentas
- Compruebe las instancias EC2 para ver si hay etiquetas obligatorias en el lanzamiento
- Crear una matriz RACI o RASCI para un modelo operativo en la nube
- Crear una definición de tareas de Amazon ECS y montar un sistema de archivos en instancias EC2 mediante Amazon EFS
- Cree reglas personalizadas de AWS Config mediante las políticas de AWS CloudFormation Guard
- Crea automáticamente CloudWatch paneles de Amazon basados en etiquetas
- Eliminar volúmenes de Amazon Elastic Block Store (Amazon EBS) no utilizados con AWS Config y AWS Systems Manager
- Implemente y gestione los controles de la Torre de Control de AWS mediante AWS CDK y AWS CloudFormation
- Implementación y administración de los controles de AWS Control Tower mediante Terraform
- Implemente código en varias regiones de AWS mediante AWS CodePipeline CodeCommit, AWS y AWS CodeBuild
- Exporte un informe de las identidades del centro de identidad de IAM de AWS y sus asignaciones mediante PowerShell
- Genere una CloudFormation plantilla de AWS que contenga las reglas administradas por AWS Config mediante Troposphere
- Otorgue a las instancias de SageMaker notebook acceso temporal a un CodeCommit repositorio de otra cuenta de AWS
- Lance un CodeBuild proyecto en todas las cuentas de AWS mediante Step Functions y una función de proxy Lambda
- Migración de los certificados SSL de Windows a un equilibrador de carga de aplicación mediante ACM
- Supervisar la actividad del usuario raíz de IAM

- ???
- Preserve el espacio IP enrutable en los diseños de VPC de varias cuentas para subredes que no son de carga de trabajo
- Registre varias cuentas de AWS con una sola dirección de correo electrónico mediante Amazon SES
- Rotar las credenciales de la base de datos sin reiniciar los contenedores
- Envíe notificaciones para una instancia de base de datos de Amazon RDS para SQL Server mediante un servidor SMTP en las instalaciones y el Correo de base de datos
- Configurar un panel de monitoreo de Grafana para AWS ParallelCluster
- Etiquete automáticamente las conexiones de puerta de enlace de tránsito con AWS Organizations
- Utilice las consultas de BMC Discovery para extraer datos de migración para planificar la migración
- Visualice los informes de credenciales de IAM para todas las cuentas de AWS que utilizan Amazon QuickSight

Mensajería y comunicaciones

Temas

Automatizar la configuración de RabbitMQ en Amazon MQ

Creado por Yogesh Bhatia (AWS) y Afroz Khan (AWS)

Entorno: PoC o piloto	Tecnologías: mensajería y comunicaciones; Infraestructura DevOps	Servicios de AWS: Amazon MQ; AWS CloudFormation

Resumen

Amazon MQ es un servicio de agente de mensajes administrado que proporciona compatibilidad con muchos de los agentes de mensajes más populares. El uso de Amazon MQ con RabbitMQ proporciona un sólido clúster de RabbitMQ gestionado en la nube de Amazon Web Services (AWS) con varios agentes y opciones de configuración. Amazon MQ proporciona una infraestructura escalable, segura y de alta disponibilidad, y puede procesar una gran cantidad de mensajes por segundo con facilidad. Varias aplicaciones pueden utilizar la infraestructura con distintos hosts virtuales, colas e intercambios. Sin embargo, administrar estas opciones de configuración o crear la infraestructura manualmente puede requerir tiempo y esfuerzo. Este patrón describe una forma de administrar las configuraciones de RabbitMQ en un solo paso, a través de un único archivo. Puede incrustar el código proporcionado con este patrón en cualquier herramienta de integración continua (CI), como Jenkins o Bamboo.

Puede utilizar este patrón para configurar cualquier clúster de RabbitMQ. Lo único que necesita es conectividad con el clúster. Aunque hay muchas otras maneras de administrar las configuraciones de RabbitMQ, esta solución crea configuraciones de aplicaciones completas en un solo paso, para poder administrar las colas y otros detalles con facilidad.

Requisitos previos y limitaciones

Requisitos previos

- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada para que apunte a su cuenta de AWS (para obtener instrucciones, consulte la documentación de la AWS CLI)
- Ansible instalado, para poder ejecutar guías para crear la configuración
- rabbitmqadmin instalado (para obtener instrucciones, consulte la documentación de RabbitMQ)
- Un clúster de RabbitMQ en Amazon MQ, creado con métricas de Amazon saludables CloudWatch

Requisitos adicionales

- Asegúrese de crear las configuraciones para los hosts virtuales y los usuarios por separado y no como parte de JSON.
- Asegúrese de que el JSON de configuración forme parte del repositorio y esté controlado por versiones.
- La versión de la CLI de rabbitmqadmin debe ser la misma que la versión del servidor de RabbitMQ, por lo que la mejor opción es descargar la CLI desde la consola de RabbitMQ.
- Como parte de la canalización, asegúrese de que la sintaxis JSON esté validada antes de cada ejecución.

Versiones de producto

- CLI de AWS versión 2.0
- Ansible versión 2.9.13
- rabbitmqadmin versión 3.9.13 (debe ser la misma que la versión del servidor RabbitMQ)

Arquitectura

Pila de tecnología de origen

- Un clúster de RabbitMQ que se ejecute en una máquina virtual (VM) existente en las instalaciones o en un clúster de Kubernetes (en las instalaciones o en la nube)

Pila de tecnología de destino

- Configuraciones de RabbitMQ automatizadas en Amazon MQ para RabbitMQ

Arquitectura de destino

Existen muchas formas de configurar RabbitMQ. Este patrón utiliza la funcionalidad de configuración de importación, en la que un único archivo JSON contiene todas las configuraciones. Este archivo aplica todos los ajustes y se puede administrar mediante un sistema de control de versiones como Bitbucket o Git. Este patrón utiliza Ansible para implementar la configuración a través de la CLI rabbitmqadmin.

Herramientas

Herramientas

- rabbitmqadmin es una herramienta de línea de comandos para la API basada en HTTP de RabbitMQ. Se usa para administrar y supervisar los nodos y clústeres de RabbitMQ.
- Ansible es una herramienta de código abierto para automatizar las aplicaciones y la infraestructura de TI.
- AWS CLI permite interactuar con los servicios de AWS mediante el uso de comandos en el intérprete de comandos de la línea de comandos.

Servicios de AWS

- Amazon MQ es un servicio de agente de mensajes administrado que facilita la configuración y el funcionamiento de los agentes de mensajes en la nube.
- AWS le CloudFormation ayuda a configurar su infraestructura de AWS y a acelerar el aprovisionamiento en la nube con la infraestructura como código.

Código

El archivo de configuración JSON utilizado en este patrón y un ejemplo del manual de estrategias de Ansible se incluyen en el archivo adjunto.

Epics

Crear la infraestructura de AWS

Tarea	Descripción	Habilidades requeridas
Cree un clúster de RabbitMQ en AWS.	Si aún no tiene un clúster de RabbitMQ, puede usar AWS CloudFormation para crear la pila en AWS. O bien, puede usar el módulo de Cloudformation de Ansible	AWS CloudFormation, Ansible

Tarea	Descripción	Habilidades requeridas
	para crear la pila. Con este último enfoque, puede usar Ansible para ambas tareas: crear la infraestructura de RabbitMQ y administrar las configuraciones.	

Crear la configuración de Amazon MQ para RabbitMQ

Tarea	Descripción	Habilidades requeridas
Cree un archivo de propiedades.	Descargue el archivo de configuración JSON (`rabbitmqconfig.json`) del archivo adjunto o expórtelo desde la consola RabbitMQ. Modifíquelo para configurar colas, intercambios y enlaces. En el diagrama siguiente, se muestra esta configuración: - Crea dos colas: `sample-queue1` y `sample-queue2` - Crea dos intercambios: `sample-exchange1` y `sample-exchange2` - Implementa el enlace entre las colas y los intercambios Estas configuraciones se realizan en el host virtual raíz (/), según lo exige rabbitmqadmin.	JSON

Tarea	Descripción	Habilidades requeridas
Obtenga los detalles de la infraestructura de Amazon MQ para RabbitMQ.	Obtenga los detalles de la infraestructura de RabbitMQ en AWS: • Nombre del agente • Host de RabbitMQ • Nombre de usuario de RabbitMQ (el usuario administrador creado durante la creación del clúster) • Contraseña de RabbitMQ Puede utilizar la opción Consola de administración de AWS o la AWS CLI para recuperar esta información. Estos detalles permiten que el manual de Ansible se conecte a su cuenta de AWS y utilice el clúster de RabbitMQ para ejecutar comandos. Importante: La computadora que ejecuta el manual de Ansible debe poder acceder a su cuenta de AWS, y la AWS CLI debe estar ya configurada, tal y como se describe en la sección Requisitos previos.	AWS CLI, Amazon MQ

Tarea	Descripción	Habilidades requeridas
Cree el archivo hosts_var.	Cree el archivo `hosts_var` para Ansible y asegúrese de que todas las variables estén definidas en el archivo. Considere la posibilidad de utilizar Ansible Vault para almacenar la contraseña. Puede configurar el archivo `hosts_var` de la siguiente manera (sustituya los asteriscos por su información): `RABBITMQ_HOST: "**********.mq.us-east-2.amazonaws.com"` `RABBITMQ_VHOST: "/"` `RABBITMQ_USERNAME: "admin"` `RABBITMQ_PASSWORD: "*******"`	Ansible

Tarea	Descripción	Habilidades requeridas
Cree un manual de Ansible.	Para ver un ejemplo de manual, consulte `ansible-rabbit-config.yaml` en el archivo adjunto. Descargue y guarde este archivo. El manual de Ansible importa y administra todas las configuraciones de RabbitMQ, como las colas, los intercambios y los enlaces, que requieren las aplicaciones. Siga las prácticas recomendadas de los manuales de Ansible, como proteger las contraseñas. Utilice Ansible Vault para cifrar las contraseñas y recupere la contraseña de RabbitMQ del archivo cifrado.	Ansible

Implementación de la configuración

Tarea	Descripción	Habilidades requeridas
Ejecute el manual.	Ejecute el manual de Ansible que creó en la Epics anterior. `ansible-playbook ansible-rabbit-config.yaml`	RabbitMQ, Amazon MQ, Ansible

Tarea	Descripción	Habilidades requeridas
	Puede verificar las nuevas configuraciones en la consola RabbitMQ.	

Recursos relacionados

- Migrating from RabbitMQ to Amazon MQ (Migración de RabbitMQ a Amazon MQ) (entrada del blog de AWS)
- Management Command Line Tool (Herramienta de línea de comandos de administración) (Documentación de RabbitMQ)
- Crear o eliminar una CloudFormation pila de AWS (documentación de Ansible)
- Migrating message driven applications to Amazon MQ for RabbitMQ (Migración de aplicaciones basadas en mensajes a Amazon MQ para RabbitMQ) (Entrada de blog de AWS)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Mejorar la calidad de las llamadas en las estaciones de trabajo de los agentes en los centros de contacto de Amazon Connect

Creado por Ernest Ozdoba (AWS)

Entorno: producción	Tecnologías: mensajería y comunicaciones; informática para el usuario final	Servicios de AWS: Amazon Connect

Resumen

Los problemas de calidad de las llamadas son algunos de las cuestiones más difíciles de solucionar en los centros de contacto. Para evitar problemas de calidad de voz y procedimientos de solución de problemas complejos, debe optimizar el entorno de trabajo y la configuración de la estación de trabajo de sus agentes. Este patrón describe las técnicas de optimización de la calidad de voz para las estaciones de trabajo de los agentes en los centros de contacto de Amazon Connect. Proporciona recomendaciones en las siguientes áreas:

- Ajustes del entorno de trabajo. El entorno de los agentes no afecta a la forma en que se transmite la voz a través de la red, pero sí afecta a la calidad de las llamadas.
- Configuración de la estación de trabajo del agente. Las configuraciones de hardware y red de las estaciones de trabajo de los centros de contacto tienen efectos significativos en la calidad de las llamadas.
- Configuración del navegador. Los agentes utilizan un navegador web para acceder al sitio web del Panel de control de contactos (CCP) de Amazon Connect y comunicarse con los clientes, por lo que la configuración del navegador puede afectar a la calidad de las llamadas.

Los siguientes componentes también pueden afectar a la calidad de las llamadas, pero quedan fuera del ámbito de la estación de trabajo y no están incluidos en este patrón:

- El tráfico fluye a la nube de Amazon Web Services (AWS) a través de AWS Direct Connect, una VPN de túnel completo o una VPN de túnel dividido
- Condiciones de la red cuando se trabaja dentro o fuera de la oficina corporativa
- Conectividad a una red telefónica pública conmutada (PSTN)

- El dispositivo y el operador de telefonía del cliente
- Infraestructura de escritorio virtual (VDI)

Para obtener más información relacionada con estas áreas, consulte Problemas comunes del panel de control de contactos (CCP) y Utilice la utilidad de prueba de punto de conexión en la documentación de Amazon Connect.

Requisitos previos y limitaciones

Requisitos previos

- Los auriculares y las estaciones de trabajo deben cumplir los requisitos especificados en la Guía del administrador de Amazon Connect.

Limitaciones

- Las técnicas de optimización de este patrón se aplican a la calidad de la voz suave de los teléfonos. No se aplican al configurar el CCP de Amazon Connect en el modo de teléfono de escritorio. Sin embargo, puede usar el modo de teléfono de escritorio si la configuración de su teléfono virtual no proporciona una calidad de voz aceptable para la llamada.

Versiones de producto

- Para ver los navegadores y las versiones compatibles, consulte la Guía del administrador de Amazon Connect.

Arquitectura

Este patrón es independiente de la arquitectura porque se centra en la configuración de la estación de trabajo del agente. Como se muestra en el siguiente diagrama, la ruta de voz del agente al cliente depende de los auriculares, el navegador, el sistema operativo, el hardware de la estación de trabajo y la red del agente.

En los centros de contacto de Amazon Connect, la conectividad de audio del usuario se establece con WebRTC. La voz se codifica con el códec de audio interactivo Opus y se cifra con el Protocolo

de transporte seguro en tiempo real (SRTP) en tránsito. Son posibles otras arquitecturas de red, incluidas las redes VPN, WAN/LAN privadas e ISP.

Herramientas

- Utilidad de prueba de punto de conexión de Amazon Connect: esta utilidad comprueba la conectividad de la red y la configuración del navegador.
- Editores de configuración del navegador para los ajustes de WebRTC:
  - Para Firefox: about:config
  - Para Chrome: chrome: //flags
- Analizador de registros de CCP: esta herramienta le ayuda a analizar los registros de CCP para solucionar problemas.

Epics

Ajusta el entorno de trabajo

Tarea	Descripción	Habilidades requeridas
Reducir el ruido de fondo.	Evitar los entornos ruidosos. Si esto no es posible, optimice el entorno con estos consejos de insonorización: • Absorba el ruido utilizando superficies que disipen el sonido, como cortinas, alfombras y muebles blandos. • Bloquee el ruido colocando barreras entre los escritorios. • Considera la posibilidad de utilizar una solución de cancelación activa del ruido (ANC), como un	Agente, administrador

Tarea	Descripción	Habilidades requeridas
	generador de ruido blanco, para ayudarte a concentrarte y garantizar la privacidad, o bien utiliza auriculares con cancelación de ruido. • Evita el eco en tus llamadas. Los espacios grandes y vacíos pueden crear efectos de eco o amplificar los ruidos. Cubrir las superficies que pueden hacer rebotar los sonidos ayudará a reducir los ecos.	

Optimice la configuración de la estación de trabajo del agente

Tarea	Descripción	Habilidades requeridas
Elegir los auriculares adecuados.	• Si el entorno es ruidoso, elija unos auriculares estéreo. Dirigir el sonido a ambos oídos ayuda a los agentes a concentrarse y a escuchar mejor al cliente, y reduce el ruido general al reducir las probabilidades de que los agentes alcen la voz. • Evite utilizar altavoces o audio de ordenador incorporado. Para obtener la mejor calidad, usa unos auriculares con cable diseñados específicamente	Agente, administrador

Tarea	Descripción	Habilidades requeridas
	para el uso en centros de contacto. Los auriculares inalámbricos son prácticos , pero pueden provocar un retraso adicional en el audio y reducir la calidad del audio debido a las interferencias de radio y a la transcodi ficación.	

Tarea	Descripción	Habilidades requeridas
Utilice los auriculares según lo previsto.	• Active las funciones de reducción activa de ruido y mejora de la voz de los auriculares, si están disponibles. Busque ajustes como ANC o ANR. Para obtener instrucciones sobre cómo activar estos ajustes, consulta el manual del usuario de los auriculares. • Ajuste el micrófono para que pueda hablar directamente con él. La mejor posición para colocar el micrófono es justo debajo de la barbilla. La colocación correcta puede marcar una diferencia de 10 decibelios (dB) en el nivel de sonido. La mayoría de los auriculares permiten girar o doblar el brazo del micrófono (brazo), por lo que es importante mantenerlo en el lugar correcto cuando se habla. • Algunos auriculares están equipados con varios micrófonos y funciones avanzadas, como la formación de haces de voz, que ayuda a capturar la voz sin que se produzca un boom. Para asegurarte de que utilizas el micrófono	Agente

Tarea	Descripción	Habilidades requeridas
	principal según lo previsto por el fabricante, consulta el manual del usuario del dispositivo.	
Compruebe los recursos de la estación de trabajo.	Asegúrese de que las computadoras de sus agentes funcionen correctamente. Si utilizan aplicaciones de terceros que consumen recursos, es posible que sus equipos no cumplan con los requisitos mínimos de hardware para ejecutar CCP. Si los agentes tienen problemas con la calidad de las llamadas, asegúrese de que disponen de suficiente potencia de procesamiento (CPU), espacio en disco, ancho de banda de red y memoria suficientes para el CCP. Los agentes deben cerrar todas las aplicacio nes y pestañas innecesarias para mejorar el rendimiento del CCP y la calidad de las llamadas.	Administrador

Tarea	Descripción	Habilidades requeridas
Configure los ajustes de sonido del sistema operativo.	Los ajustes predeterminados para el nivel y el aumento del micrófono suelen funcionar bien. Si descubre que la voz saliente es baja o que el micrófono capta demasiado , puede que le ayude ajustar estos ajustes. Los ajustes del micrófono se encuentran en la configuración de sonido del sistema del ordenador (sonido, entrada en macOS, propiedades del micrófono en Windows). Puede acceder a los ajustes avanzados que pueden afectar a la calidad de la voz a través de las herramientas del sistema o de aplicaciones de terceros. Estos son algunos de los ajustes que puede comprobar: • Frecuencia de muestreo: este valor determina cuántas veces se sondea el sonido por segundo. La configuración predeterm inada suele ser de 44 o 48 kilohercios (kHz). El valor óptimo para Amazon Connect es de 48 kHz. Puede usar la configura ción de su navegador para anular el valor predeterm inado. Para obtener más	Agente, administrador

Tarea	Descripción	Habilidades requeridas
	información, consulte la sección de solución de problemas de la Guía del administrador de Amazon Connect. • Ganancia: este valor determina en qué medida el micrófono amplifica el sonido. Si aumenta la ganancia, es posible que el micrófono capte más ruido de fondo. • Profundidad de bits: este valor de resolución digital describe cuántos niveles de amplitud de sonido se reconocen. Cuanto mayor sea la profundidad de bits, más suave será el sonido de la voz. Sin embargo, muchas redes de telefonía tradicionales utilizan el estándar de modulació n por pulsos codificados (PCM), que solo admite una resolución de 8 bits. • Umbral abierto: es la amplitud de sonido mínima que capta un micrófono. Si tiene problemas con la calidad de la voz, intente restablecer estos valores a su	

Tarea	Descripción	Habilidades requeridas
	configuración predeterminada antes de seguir investigando. Para obtener más informaci ón acerca de estos ajustes y otros ajustes, consulte el manual del dispositivo.	

Tarea	Descripción	Habilidades requeridas
Utilice una red cableada.	Por lo general, la Ethernet cableada tiene una latencia más baja, por lo que es más fácil proporcionar la calidad de transmisión uniforme requerida para la transmisión de datos de voz. Recomenda mos un ancho de banda mínimo de 100 KB por llamada. • Si los agentes trabajan desde casa, recomenda mos conexiones cableadas antes que conexiones inalámbricas. Escuchar al cliente no debería tardar más de 150 milisegundos. Puede acceder a la prueba de latencia de Amazon Connect desde la utilidad Amazon Connect Endpoint Test Utility. Sin embargo, esta utilidad mide el retraso desde el navegador hasta las regiones de Amazon Connect, no hasta los clientes. La recomendación de demora unidireccional de 150 milisegundos impide que el agente y el cliente hablen entre sí. El valor se mide de un extremo a otro y cada elemento añade un retraso, incluida la parte de	Administrador de red, agente

Tarea	Descripción	Habilidades requeridas
	la llamada entre la región de Amazon Connect y el cliente. • Si los agentes trabajan desde la oficina, el Wi-Fi corporativo es aceptable siempre que los parámetros estén dentro del rango recomendado y se dé prioridad al tráfico del Protocolo de transporte en tiempo real (RTP).	

Tarea	Descripción	Habilidades requeridas
Actualice los controladores de hardware.	Si utiliza auriculares USB o de otro tipo que tengan su propio firmware, le recomendamos que los mantenga actualizados con la última versión. Los auriculares sencillos que utilizan un puerto auxiliar utilizan el dispositivo de audio integrado en el ordenador, así que asegúrese de que el controlador de hardware del sistema operativo esté actualizado. En raras ocasiones, una actualización del controlador de audio puede provocar problemas de audio y es posible que tenga que revertirla. Para obtener más información sobre cómo cambiar las versiones del firmware y del controlador, consulte el manual del dispositivo.	Administrador

Tarea	Descripción	Habilidades requeridas
Evite los concentradores y dongles USB.	Cuando conecte los auriculares, evite usar dispositivos adicionales, como dongles, convertidores de tipo de puerto, concentradores y cables de extensión. Estos dispositivos pueden afectar a la calidad de las llamadas. En su lugar, conecte el dispositivo directamente al puerto del ordenador.	Agente

Tarea	Descripción	Habilidades requeridas
Compruebe los registros del CCP.	El analizador de registros CCP proporciona una forma sencilla de comprobar los registros de las aplicaciones. 1. Descargue los registros del CCP después de una llamada. 2. Abra el analizador de Registros del CCP. 3. Arrastre y suelte el archivo de registro para cargarlo y analizarlo. 4. Cuando se haya analizado el registro, se seleccion ará la pestaña Instantán eas y registros de forma predeterminada. Seleccione la pestaña Métricas situada junto a ella para consultar la información. 5. En la sección Métricas de WebRTC: audio_input, compruebe lo siguiente: • El gráfico del nivel de audio, para ver si el nivel de audio recibido es superior a 0. Esto indica que se ha recibido el audio de la persona que llama. • El gráfico de Paquetes para ver los paquetes perdidos. Si este gráfico	Agente (habilidades avanzadas)

Tarea	Descripción	Habilidades requeridas
	muestra aumentos significativos, póngase en contacto con su equipo de soporte de TI. 6. En la sección Métricas de WebRTC: audio_output, compruebe lo siguiente: • El gráfico del Nivel de audio, para confirmar que el audio se envió desde su dispositivo. • El gráfico de Paquetes. Si observa un aumento en la pérdida de paquetes, infórmelo a su equipo de soporte de TI. • El gráfico Jitter Buffer y RTT. Los valores del tiempo de ida y vuelta (RTT) superiores a 300 afectarán a la experienc ia de llamada. Informe de ello a su equipo de soporte de TI.	

Optimizar la configuración del navegador

Tarea	Descripción	Habilidades requeridas
Restaurar la configuración predeterminada de WebRTC.	La WebRTC debe estar habilitada para realizar llamadas telefónicas flexibles con CCP. Le recomenda	Administrador

Tarea	Descripción	Habilidades requeridas
	mos que utilice la configura ción predeterminada de las funciones relacionadas con WebRTC. • En Chrome, puede configurar banderas navegando hasta la URL chrome: //flags. Escriba WebRTC en el cuadro de búsqueda para encontrar configuraciones que puedan interferir con el CCP y establézcalas como Predeterminadas. • En Firefox, escriba about:config en la barra de direcciones y, a continuac ión, escriba WebRTC en el cuadro de búsqueda de la página de configuración. Los ajustes no predeterm inados aparecen en negrita y se pueden cambiar a Predeterminados.	

Tarea	Descripción	Habilidades requeridas
Deshabilite las extensiones del navegador al solucionar problemas.	Algunas extensiones del navegador pueden afectar a la calidad de las llamadas o incluso impedir que las llamadas se conecten correctamente. Use la ventana de incógnito o el modo privado de tu navegador y desactiva todas las extensiones. Si eso soluciona el problema, revise las extensiones de tu navegador y busque complementos sospechos os, o desactívalos de forma individual.	Agente, administrador
Compruebe la frecuencia de muestreo del navegador.	Confirme que la entrada del micrófono esté configura da en la frecuencia de muestreo óptima de 48 kHz. Para obtener instrucciones, consulte la Guía del administr ador de Amazon Connect.	Agente, administrador

Recursos relacionados

Si ha seguido los pasos de este patrón pero sigue teniendo problemas con la calidad de las llamadas, consulte los siguientes recursos para obtener consejos de solución de problemas.

- Revise los problemas más comunes del Panel de control de contactos (CCP).
- Compruebe la conexión con la utilidad de prueba de terminales.
- Siga la guía de solución de problemas para cualquier otro problema.

Si la solución de problemas y los ajustes no resuelven el problema de calidad de las llamadas, es posible que la causa principal sea externa a la estación de trabajo. Para obtener más información sobre la solución de problemas, póngase en contacto con tu equipo de soporte de TI.

Más patrones

- Descomponga monolitos en microservicios mediante CQRS y abastecimiento de eventos
- Integre Amazon API Gateway con Amazon SQS para gestionar las API REST asíncronas
- Registre varias cuentas de AWS con una sola dirección de correo electrónico mediante Amazon SES
- Ejecute cargas de trabajo basadas en mensajes a escala con AWS Fargate

Migración

Temas

Automatice la identificación y planificación de la estrategia de migración mediante AppScore

Entorno: producción	Origen: Todas las cargas de trabajo	Destino: nube de AWS
Tipo R: N/D	Carga de trabajo: todas las demás cargas de trabajo	Tecnologías: migración; modernización; aplicaciones web y móviles; SaaS
Servicios de AWS: AWS Application Discovery Service; AWS Migration Hub		

Resumen

Las aplicaciones en las instalaciones requieren un enfoque de transformación para poder aprovechar los beneficios de la nube de Amazon Web Services (AWS). Las siete estrategias de migración más comunes (las 7 R) le ofrecen opciones de transformación, que van desde realizar cambios tecnológicos en los servidores de bases de datos en las instalaciones hasta reconstruir una aplicación mediante una arquitectura de microservicios nativa en la nube.

Si opta por utilizar el modelo completo de las 7 R, tendrá que trabajar a nivel empresarial y de aplicación, en lugar de limitarse a evaluar y preparar los servidores para la migración. Si bien puede obtener los datos del servidor mediante herramientas como el Evaluador de la migración de AWS, a menudo no se registra otra información de la aplicación (por ejemplo, el estado de la hoja de ruta, el objetivo de tiempo de recuperación (RTO) y el objetivo de punto de recuperación (RPO) requeridos, o los requisitos de privacidad de los datos).

Este patrón describe cómo AppScoreevitar estos desafíos mediante una visión de su cartera centrada en las aplicaciones. Esto incluye una ruta de transformación recomendada a la nube de AWS para cada aplicación según el modelo completo de las 7 R. AppScore le ayuda a recopilar información sobre las aplicaciones, determinar la ruta de transformación ideal, identificar el riesgo, la complejidad y las ventajas de la adopción de la nube y definir rápidamente los ámbitos de migración, los grupos de movimientos y los cronogramas.

Este patrón lo crearon AWS y AppScore Technology Limited, un socio de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Aplicaciones existentes que desea migrar a la nube de AWS.
- Información de inventario de servidores existente de una herramienta como el Evaluador de la migración de AWS. También puede importar estos datos en una fase posterior de la migración.
- Una AppScore cuenta existente con privilegios de usuario avanzado. Para obtener más información sobre las cuentas de AppScore usuario, consulte ¿Cómo se asigna el control de acceso basado en roles (RBAC) a los usuarios? en la documentación AppScore
- Comprensión de cómo asignar funciones de RBAC en. AppScore AppScore proporciona tres funciones de experto en la materia (SME) que se alinean con las preguntas que se formulan en la etapa de puntuación. Esto significa que un SME solo responde a las preguntas relacionadas con su experiencia y su función. Para obtener más información al respecto, consulte ¿Cómo se asigna el control de acceso basado en roles (RBAC) a los usuarios? en la documentación. AppScore
- Una comprensión AppScore de las recomendaciones, que se basan en las tres categorías siguientes de atributos de la aplicación:
  - Riesgo: la importancia empresarial de la aplicación, si contiene datos confidenciales, los requisitos de soberanía de los datos y el número de usuarios o interfaces de la aplicación
  - Complejidad: el lenguaje, la antigüedad, la interfaz de usuario o el número de interfaces de desarrollo de la aplicación (por ejemplo, COBOL tiene una puntuación más alta que .NET o PHP)
  - Ventaja: la demanda de procesamiento por lotes, el perfil de la aplicación, el modelo de recuperación de desastres y el uso del entorno de desarrollo y prueba
- Una comprensión de las AppScore cuatro fases de la captura iterativa de datos:
  - Señalización: preguntas que se combinan con los datos del servidor para producir las evaluaciones de las 7 R. Para obtener más información, consulte Cómo señalizar y puntuar las aplicaciones en la AppScore documentación.
  - Puntuación: preguntas que generan puntuaciones en función del riesgo, el beneficio y la complejidad.
  - Evaluación del estado actual: preguntas que proporcionan una evaluación del estado actual de la aplicación.

- Transformación: preguntas que evalúan de manera integral la aplicación para el diseño del futuro estado.

Importante: solo se requieren las etapas de señalización y puntuación para recibir las calificaciones de las solicitudes, las evaluaciones de 7 R y permitir la planificación grupal. Después de agrupar las solicitudes y los campos de los formularios, puede completar las etapas de evaluación y transformación del estado actual para obtener una visión general más detallada de su aplicación.

Arquitectura

El siguiente diagrama muestra el AppScore flujo de trabajo que utiliza datos de aplicaciones y servidores para crear una recomendación para su estrategia de migración y su plan de transformación.

Herramientas

- AppScore— le AppScore ayuda a cerrar la brecha entre el descubrimiento y la implementación de la migración, ya que proporciona una visión de su cartera centrada en las aplicaciones, con una ruta recomendada hacia la nube para cada aplicación en comparación con el modelo completo de las 7 R.
- Evaluador de la migración de AWS: el Evaluador de la migración de AWS es un servicio de evaluación de la migración que le ayuda a crear un modelo de negocio orientado a la planificación y la migración.

Epics

Cree y cargue la lista inicial de aplicaciones

Tarea	Descripción	Habilidades requeridas
Prepare la lista de aplicacio nes.	Inicie sesión en el AppScore portal con sus credenciales de usuario. Descargue la `Import Template` desde la página de la página de la Aplicació	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	n y, a continuación, actualice la `Import Template` con los atributos no técnicos de la aplicación (por ejemplo, una clasificación de datos o una lista de atributos que se puedan personalizar). Para obtener más informaci ón al respecto, consulte Cómo modificar los cuestionarios empresariales y de AppScore solicitud en la AppScore documentación. Nota: También puede añadir una aplicación manualmen te seleccionando Nueva aplicación en la página de la aplicación. A continuación, puede introducir los atributos no técnicos de la aplicación.	
Importe los datos de la aplicación.	En la página de la aplicación, seleccione Importar aplicacio nes para importar los datos de la aplicación.	Ingeniero de migraciones

Capture los datos empresariales y de la aplicación

Tarea	Descripción	Habilidades requeridas
Revise y responda las preguntas sobre señalización y puntuación.	Abra la página Servidores y elija Importar servidores. Elija	Propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	el archivo .csv que contiene los datos del servidor. El archivo puede incluir atributos como el nombre, el centro de datos, el sistema operativo, virtual o físico, el nombre de la aplicación, el rol, la tecnología de la base de datos, el entorno, el número y la utilización de los núcleos de la CPU, el tamaño y la utilizaci ón de la RAM, el tamaño y la utilización del disco, el tipo de equipo correspondiente y los costos mensuales actuales y proyectados. Confirme la asignación de columnas y seleccion e Confirmar e importar. La información que falta en los datos importados aparece resaltada en la página del servidor. Puede resolver estas brechas en esta página o mediante la opción de edición masiva. Los servidores están asociados a la aplicación pertinente. Sin embargo, si las aplicaciones no existen en AppScore, se crean automátic amente y, a continuación, se asocian los servidores.	

Tarea	Descripción	Habilidades requeridas
	También puede utilizar una conexión de API de para recuperar los datos con AWS Migration Hub. Para obtener más información al respecto, consulte ¿Cómo puedo importar servidores desde AWS Migration Hub mediante la API? En la AppScore documentación. Nota: Si utilizó una herramien ta de detección (por ejemplo, AWS Migration Evaluator) para capturar el rendimien to a lo largo del tiempo, debe cargar una extracció n temprana de los datos del servidor lo antes posible y actualizarlos cuando las métricas de rendimiento estén completamente capturada s. AppScore utiliza los nombres de los servidore s, las versiones del sistema operativo y de las bases de datos, los centros de datos y los entornos para ofrecer puntuaciones y recomenda ciones de 7 rupias.	

Tarea	Descripción	Habilidades requeridas
Compruebe las puntuaciones de las aplicaciones.	Abra la página Aplicaciones para ver la puntuación y la evaluación de las 7 R de sus aplicaciones. También se calculan sus costos de ejecución actuales. Estos cálculos se actualizan cuando se importa nueva información a las páginas de aplicaciones o servidores.	Propietario de la aplicación
Analice las aplicaciones individuales.	Elija una aplicación en la página de aplicaciones para consultar las recomenda ciones detalladas. Puede seleccionar informe de evaluación de la aplicación para generar un archivo .pdf o .docx con los datos de evaluación detallados de las aplicaciones específicas.	Propietario de la aplicación

Cree el cronograma de migración

Tarea	Descripción	Habilidades requeridas
Elija las aplicaciones para el grupo de movimiento.	Abra la página planificación, elija creador de grupo y, a continuación, cree grupos de movimientos de aplicaciones según sus necesidades. Puede añadir o eliminar atributos de la lista de aplicaciones en la sección	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	Columnas. También puede usar los atributos de la aplicación en la sección Filtros para elegir aplicacio nes específicas, lo que incluye filtrar todas las aplicacio nes que ya forman parte de los grupos de movimientos existentes.	
Cree el grupo de movimientos.	Elija Grupo seleccionado, especifique un nombre para el grupo de movimientos, elija las aplicaciones que desee incluir en el grupo de movimientos y, a continuación, seleccione Añadir al grupo.	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
Programe la migración.	En la página de cronogramas de transformación, AppScore proporciona una estimación de la duración, el esfuerzo y el coste de la transformación para su grupo de mudanzas. El grupo de movimiento se agrega automáticamente al programa de transformación general. Nota: Puede personalizar las suposiciones en las que se basa la estimación del esfuerzo en la página Configuración de planificación. Esto ayuda a alinearlas con los requisitos de su organización. Para obtener más información al respecto, consulte Cómo configurar los ajustes de planificación en la AppScore documentación.	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
Genere el informe de transformación completo.	Abra la página Administrador de grupos y elija Crear documento de informe de transformación de aplicaciones. Elija los grupos de movimiento y, a continuación, elija Exportar. Esto genera un archivo .docx que resume la transformación, incluidos los detalles de cada grupo de movimientos. Para ver un ejemplo de informe de transformación de aplicaciones, consulte un ejemplo de informe de transformación de aplicaciones del AppScore sitio web.	Ingeniero de migraciones

Recursos relacionados

- ¿Cuáles son las 7 R de la migración de una aplicación?
- Un análisis más detallado de AppScore
- AppScore en AWS Marketplace

Cree CloudFormation plantillas de AWS para las tareas de AWS DMS con Microsoft Excel y Python

Creado por Venkata Naveen Koppula (AWS)

Entorno: PoC o piloto	Origen: Automatización	Destino: Base de datos en la nube de AWS
Tipo R: N/D	Carga de trabajo: Microsoft	Tecnologías: Migración; bases de datos

Resumen

Este patrón describe los pasos para crear automáticamente CloudFormation plantillas de AWS para AWS Database Migration Service (AWS DMS) mediante Microsoft Excel y Python.

La migración de bases de datos mediante AWS DMS suele implicar la creación de CloudFormation plantillas de AWS para aprovisionar las tareas de AWS DMS. Anteriormente, la creación de CloudFormation plantillas de AWS requería conocimientos del lenguaje de programación JSON o YAML. Con esta herramienta, solo necesita conocimientos básicos de Excel y de cómo ejecutar un script de Python mediante una terminal o una ventana de comandos.

Como entrada, la herramienta utiliza un libro de trabajo de Excel que incluye los nombres de las tablas que se van a migrar, los nombres de recursos de Amazon (ARN) de los puntos de conexión de AWS DMS y las instancias de replicación de AWS DMS. A continuación, la herramienta genera CloudFormation plantillas de AWS para las tareas de AWS DMS necesarias.

Para ver los pasos detallados y la información básica, consulte la entrada del blog Crear CloudFormation plantillas de AWS para tareas de AWS DMS con Microsoft Excel en el blog AWS Database.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa

- Microsoft Excel versión 2016 o posterior
- Python versión 2.7 o posterior
- El módulo Python xlrd (instalado en una línea de comandos con el comando: pip install xlrd)
- Puntos de conexión de origen y destino de AWS DMS e instancia de replicación de AWS DMS

Limitaciones

- Los nombres de los esquemas, las tablas y las columnas asociadas se transforman en minúsculas en los puntos de conexión de destino.
- Esta herramienta no aborda la creación de instancias de replicación y puntos de conexión de AWS DMS.
- Actualmente, la herramienta solo admite un esquema para cada tarea de AWS DMS.

Arquitectura

Pila de tecnología de origen

- Base de datos en las instalaciones
- Microsoft Excel

Pila de tecnología de destino

- CloudFormation Plantillas de AWS
- Una base de datos en la nube de AWS

Arquitectura

Herramientas

- Pycharm IDE o cualquier entorno de desarrollo integrado (IDE) compatible con Python versión 3.6
- Microsoft Office 2016 (para Microsoft Excel)

Epics

Configurar la red, la instancia de replicación de AWS DMS y los puntos de conexión

Tarea	Descripción	Habilidades requeridas
Si es necesario, solicite un aumento de cuota de servicio.	Solicite un aumento de cuota de servicio para las tareas de AWS DMS si es necesario.	AWS general
Configure la región de AWS, las nubes privadas virtuales (VPC), los rangos de CIDR, las zonas de disponibilidad y las subredes.		AWS general
Configure la instancia de replicación de AWS DMS.	La instancia de replicación de AWS DMS puede conectarse tanto a bases de datos en las instalaciones como de AWS.	AWS general
Configure los puntos de conexión de AWS DMS.	Configure los puntos de conexión para las bases de datos de origen y de destino.	AWS general

Preparar las hojas de trabajo para las tareas y etiquetas de AWS DMS

Tarea	Descripción	Habilidades requeridas
Configure la lista de tablas.	Enumere todas las tablas implicadas en la migración.	Database
Prepare la hoja de trabajo de tareas.	Prepare la hoja de cálculo de Excel con la lista de tablas que configuró.	AWS general, Microsoft Excel
Prepare la hoja de trabajo sobre las etiquetas.	Detalle las etiquetas de recursos de AWS que se	AWS general, Microsoft Excel

Tarea	Descripción	Habilidades requeridas
	deben adjuntar a las tareas de AWS DMS.	

Descargar y ejecutar la herramienta

Tarea	Descripción	Habilidades requeridas
Descargue y extraiga la herramienta de generación de plantillas del GitHub repositorio.	GitHub repositorio: https://github.com/aws-samples/dms-cloudformation-templates-generator/	
Ejecute la herramienta.	Siga las instrucciones detalladas de la entrada del blog que aparece en la sección "Referencias y ayuda".	

Recursos relacionados

- Cree CloudFormation plantillas de AWS para las tareas de AWS DMS con Microsoft Excel (entrada del blog)
- Generador de CloudFormation plantillas de DMS (repositorio) GitHub
- Documentación de Python
- Descripción y descarga en xlrd
- Documentación de AWS DMS
- CloudFormation Documentación de AWS

Introducción a la detección automática de cartera

Creado por Pratik Chunawala (AWS) y Rodolfo Jr. Cerrada (AWS)

Entorno: producción	Origen: en las instalaciones	Destino: en las instalaciones
Tipo R: N/D	Carga de trabajo: todas las demás cargas de trabajo	Tecnologías: migración

Resumen

Evaluar la cartera y recopilar metadatos es un desafío fundamental al migrar aplicaciones y servidores a la nube de Amazon Web Services (AWS), especialmente en el caso de migraciones grandes con más de 300 servidores. El uso de una herramienta automatizada de detección de cartera puede ayudarle a recopilar información sobre sus aplicaciones, como la cantidad de usuarios, la frecuencia de uso, las dependencias y la información sobre la infraestructura de la aplicación. Esta información es esencial a la hora de planificar oleadas de migración, ya que le permite priorizar y agrupar adecuadamente las aplicaciones con características similares. El uso de una herramienta de detección agiliza la comunicación entre el equipo de cartera y los propietarios de las aplicaciones, ya que el equipo de cartera puede validar los resultados de la herramienta de detección en lugar de recopilar los metadatos manualmente. En este patrón se analizan las consideraciones clave a la hora de seleccionar una herramienta de detección automatizada, y se ofrece información sobre cómo implementar y probar una en su entorno.

Este patrón incluye una plantilla que le servirá como punto de partida para crear su propia lista de verificación de actividades de alto nivel. Junto a la lista de verificación encontrará una plantilla para crear una matriz responsable, fiable, consultada y fundamentada (RACI). Puede usar esta matriz RACI para determinar quién es responsable de cada tarea de su lista de verificación.

Epics

Selección una herramienta de detección

Tarea	Descripción	Habilidades requeridas
Determine si una herramien ta de detección es apropiada para su caso de uso.	Es posible que una herramien ta de detección no sea la mejor solución para su caso de uso. Tenga en cuenta la cantidad de tiempo que necesitará para seleccion ar, adquirir, preparar e implementar una herramienta de detección. La configuración del dispositivo de escaneo para una herramienta de detección sin agente en su entorno, o la instalación de agentes en todas las cargas de trabajo incluidas en el ámbito de aplicación, puede llevar de 4 a 8 semanas. Una vez implementada, la herramienta de detección tardará de 4 a 12 semanas en recopilar los metadatos escaneando las cargas de trabajo de las aplicaciones y realizar un análisis del conjunto de aplicaciones. Si va a migrar menos de 100 servidores, es posible que pueda recopilar los metadatos manualmente y analizar las dependencias en menos tiempo del que tardaría en	Responsable de migraciones, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	implementar y recopilar los metadatos con una herramien ta de detección automatizada.	
Selección una herramientas de detección.	Consulte las Considera ciones para seleccionar una herramienta de detección automática en la sección Información adicional. Determine los criterios adecuados para seleccionar una herramienta de detección para su caso de uso y, a continuación, evalúe cada herramienta en función de dichos criterios. Para obtener una lista completa de herramientas de detección automatizadas, consulte Herramientas de detección , planificación y migración recomendadas.	Responsable de migraciones, ingeniero de migraciones

Para preparar la instalación

Tarea	Descripción	Habilidades requeridas
Prepare la lista de verificación previa a la implementación.	Cree una lista de verificac ión con las tareas que debe completar antes de implement ar la herramienta. Para ver un ejemplo, consulte la Lista de verificación previa a la	Responsable de compilaci ón, ingeniero de migraciones, responsable de migraciones, administrador de red

Tarea	Descripción	Habilidades requeridas
	implementación en el sitio web de documentación de Flexera.	
Prepare los requisitos de la red.	Aprovisione los puertos, protocolos, direcciones IP y enrutamiento necesarios para que la herramienta se ejecute y acceda a los servidores de destino. Para obtener más información, consulte la guía de instalación de su herramienta de detección. Para ver un ejemplo, consulte la Requisitos para la implementación en el sitio web de documentación de Flexera.	Ingeniero migraciones, administrador de redes, arquitecto de la nube
Prepare los requisitos de cuenta y credenciales.	Identifique las credenciales que necesita para acceder a los servidores de destino e instalar todos los componentes de la herramienta.	Administrador de la nube, AWS general, ingeniero de migraciones, responsable de migraciones, administrador de redes, administrador de AWS
Prepare los dispositivos en los que va a instalar la herramienta.	Asegúrese de que los dispositivos en los que va a instalar los componentes de la herramienta cumplen las especificaciones y los requisitos de plataforma de la herramienta.	Ingeniero de migraciones, ingeniero de migraciones, líder de migraciones, administrador de red
Prepare las órdenes de cambio.	Siguiendo el proceso de gestión de cambios de su organización, prepare las órdenes de cambio necesarias y asegúrese de que se aprueben.	Responsable de compilación, líder de migración

Tarea	Descripción	Habilidades requeridas
Envíe los requisitos a las partes interesadas.	Envíe la lista de verificación previa a la implementación y los requisitos de red a las partes interesadas. Las partes interesadas deben revisar, evaluar y preparar los requisitos necesarios antes de proceder con la implementación.	Responsable de compilación, líder de migración

Implemente la herramienta

Tarea	Descripción	Habilidades requeridas
Descargue el instalador.	Descargue el instalador o la imagen de máquina virtual. Las imágenes de máquinas virtuales suelen estar en formato de virtualización abierta (OVF).	Responsable de compilación, líder de migración
Extraiga los archivos.	Si usa un instalador, debe descargarlo y ejecutarlo en un servidor en las instalaciones.	Responsable de compilación, líder de migración
Implemente la herramienta en los servidores.	Implemente la herramienta de detección en los servidores de destino en las instalaciones de la siguiente manera: • Si el archivo de origen es una imagen de máquina virtual, impleméntela en su entorno de máquina virtual, como VMware.	Responsable de compilación, líder de migración, administrador de red

Tarea	Descripción	Habilidades requeridas
	• Si el archivo de origen es un instalador, ejecútelo para instalar y configurar la herramienta.	
Inicie sesión en la herramienta de detección.	Siga las indicaciones que aparecen en pantalla e inicie sesión para usar la herramienta.	Líder de migración, responsable de compilación
Active el producto.	Introduzca su clave de licencia.	Responsable de compilación, líder de migración
Configure la herramienta.	Introduzca las credenciales necesarias para acceder a los servidores de destino, como credenciales de Windows, VMware, Simple Network Management Protocol (SNMP), Secure Shell Protocol (SSH) o bases de datos.	Responsable de compilación, líder de migración

Pruebe la herramienta

Tarea	Descripción	Habilidades requeridas
Seleccione los servidores de prueba.	Identifique un conjunto pequeño de subredes o direcciones IP que no sean de producción y que pueda usar para probar la herramienta de detección. Esto le ayudará a validar los escaneos rápidamente, identificar y	Responsable de compilación, líder de migración, administrador de red

Tarea	Descripción	Habilidades requeridas
	solucionar cualquier error con prontitud y aislar las pruebas de los entornos de producción.	
Comience a escanear los servidores de prueba seleccionados.	Si usa una herramienta de detección sin agente, introduzca las subredes o direcciones IP de los servidores de prueba seleccionados en la consola de la herramienta de detección e inicie el escaneo. Si usa una herramienta de detección basada en agente, instale el agente en los servidores de prueba seleccionados.	Responsable de compilación, líder de migración, administrador de red
Revise los resultados escaneados.	Revise los resultados del escaneo de los servidores de prueba. Si encuentra algún error, corríjalo. Documente los errores y las soluciones. Puede hacer referencia a esta información en el futuro y añadirla al manual de procedimientos de su cartera.	Responsable de compilación, líder de migración, administrador de red
Vuelva a escanear los servidores de prueba.	Una vez completado el rescaneo, repítalo hasta que no surjan errores.	Responsable de compilación, líder de migración, administrador de red

Recursos relacionados

Recursos de AWS

- Guía de evaluación de la cartera de aplicaciones para la migración a la nube de AWS
- Herramientas de detección, planificación y migración recomendadas

Guías de implementación para las herramientas de detección más comunes

- Implemente el dispositivo virtual RN150 (documentación de Flexera)
- Instalación de Gatherer (documentación de ModelizeIT)
- Instalación de On-Prem Analysis Server (documentación de ModelizeIt)

Información adicional

Consideraciones para seleccionar una herramienta de detección automatizada

Cada herramienta de detección tiene sus ventajas y limitaciones. A la hora de seleccionar la herramienta adecuada para su caso de uso, tenga en cuenta lo siguiente:

- Seleccione una herramienta de detección que pueda recopilar la mayoría, si no todos, de los metadatos que necesita para alcanzar el objetivo de evaluación de su cartera.
- Identifique los metadatos incompatibles con la herramienta que necesite recopilar manualmente.
- Comunique los requisitos de la herramienta de detección a las partes interesadas para que puedan revisarla y evaluarla en función de sus necesidades internas de seguridad y conformidad, como los requisitos de servidor, red y credenciales.
  - ¿Es necesario que la herramienta instale un agente en la carga de trabajo prevista?
  - ¿Es necesario que la herramienta configure un dispositivo virtual en su entorno?
- Determine sus requisitos de residencia de datos. Algunas organizaciones no desean almacenar sus datos fuera de su entorno. Para abordar este aspecto, es posible que deba instalar algunos componentes de la herramienta en el entorno en las instalaciones.
- Asegúrese de que la herramienta sea compatible con el sistema operativo (SO) y la versión del sistema operativo de la carga de trabajo pertinente.
- Determine si su cartera incluye servidores mainframe, de gama media y heredados. La mayoría de las herramientas de detección pueden detectar estas cargas de trabajo como dependencias,

pero es posible que algunas herramientas no puedan obtener detalles del dispositivo, como la utilización y las dependencias del servidor. Las herramientas de detección Device42 y ModernizeIT son compatibles con servidores de mainframe y de gama media.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Migración de cargas de trabajo de Cloudera en las instalaciones a la plataforma de datos de Cloudera en AWS

Entorno: PoC o piloto	Origen: Cargas de trabajo de Cloudera	Destino: nube pública de Cloudera Data Platform (CDP)
Tipo R: N/D	Carga de trabajo: todas las demás cargas de trabajo	Tecnologías: migración; macrodatos; bases de datos; análisis
Servicios de AWS: Amazon EC2; Amazon EKS; AWS Identity and Access Management; Amazon S3; Amazon RDS		

Resumen

Este patrón describe los pasos de alto nivel para migrar sus cargas de trabajo en las instalaciones Cloudera Distributed Hadoop (CDH), Hortonworks Data Platform (HDP) y Cloudera Data Platform (CDP) a la nube pública de CDP en AWS. Le recomendamos que se asocie con los servicios profesionales de Cloudera y con un integrador de sistemas (SI) para implementar estos pasos.

Hay muchos motivos por los que los clientes de Cloudera quieren trasladar sus cargas de trabajo en las instalaciones de CDH, HDP y CDP a la nube. Algunas de las razones más habituales son las siguientes:

- Optimizar la adopción de nuevos paradigmas de plataformas de datos, como Data Lakehouse o Data Mesh
- Aumentar la agilidad empresarial, democratice el acceso y la inferencia sobre los activos de datos existentes
- Reducir el costo total de propiedad (TCO)
- Mejorar la elasticidad de la carga
- Permitir una mayor escalabilidad; reducir drásticamente el tiempo de aprovisionamiento de los servicios de datos en comparación con la base de instalación en las instalaciones heredada

- Eliminar el hardware heredado y reducir significativamente los ciclos de actualización del hardware
- Aproveche los pay-as-you-go precios, que se extienden a las cargas de trabajo de Cloudera en AWS con el modelo de licencias (CCU) de Cloudera
- Aprovechar una implementación más rápida y una mejor integración con las plataformas de integración continua y entrega continua (CI/CD)
- Utilizar una única plataforma unificada (CDP) para múltiples cargas de trabajo

Cloudera es compatible con las principales cargas de trabajo, incluidas Machine Learning, Data Engineering, Data Warehouse, Operational Database, Stream Processing (CSP) y seguridad y gobierno de datos. Cloudera lleva muchos años ofreciendo estas cargas de trabajo en las instalaciones, y puede migrarlas a la nube de AWS mediante la nube pública de CDP con Workload Manager y Replication Manager.

Cloudera Shared Data Experience (SDX) proporciona un catálogo de metadatos compartido entre estas cargas de trabajo para facilitar la gestión y las operaciones de datos coherentes. SDX también incluye seguridad integral y granular para proteger contra las amenazas y una gobernanza unificada para las capacidades de auditoría y búsqueda a fin de cumplir con estándares como el Estándar de Seguridad de Datos del Sector de Tarjetas de Pago (PCI DSS) y el GDPR.

La migración a CDP de un vistazo

Carga de trabajo	Carga de trabajo de origen	Nube privada de CDH, HDP y CDP
	Entorno de origen	• Windows, Linux • En las instalaciones, coubicación o en cualquier entorno que no sea de AWS
	Carga de trabajo del destino	Nube pública de CDP en AWS
	Entorno de destino	• Modelo de implementación: cuenta de cliente • Modelo operativo: plano de control cliente/Cloudera

	Estrategia de migración (7Rs)	Volver a alojar, redefinir la plataforma o refactorizar
Migración	¿Se trata de una actualización de la versión de carga de trabajo?	Sí
	Duración de la migración	• Implementación: aproximadamente 1 semana para crear una cuenta de cliente, una nube privada virtual (VPC) y un entorno de nube pública de CDP administrado por el cliente. • Duración de la migración: de 1 a 4 meses, según la complejidad y el tamaño de la carga de trabajo.

Costo	Costo de ejecutar la carga de trabajo en AWS	• A un alto nivel, el costo de una migración de cargas de trabajo CDH a AWS asume que establecerá un nuevo entorno en AWS. Incluye el cálculo de tiempo y esfuerzo del personal, así como el aprovisionamiento de los recursos informáticos y las licencias de software para el nuevo entorno. • El modelo de precios de Cloudera basado en el consumo de la nube le ofrece la flexibilidad necesaria para aprovecha r las amplias capacidades de escalado automático. Para obtener más informaci ón, consulte las tarifas del servicio de nube pública de CDP en el sitio web de Cloudera. • Cloudera Enterprise Data Hub se basa en Amazon Elastic Compute Cloud (Amazon EC2) y modela de forma precisa los clústeres tradicionales. Data Hub se puede personalizar, pero esto repercutirá en los costos. • CDP Public Cloud Data Warehouse, Cloudera Machine Learning y Cloudera Data Engineeri

		ng (CDE) están basados en contenedores y se pueden configurar para que se escalen automáticamente.
Marco y acuerdos de infraestructura	Requisitos del sistema	Consulte la sección Requisitos previos.
	SLA	Consulte el Acuerdo de nivel de servicio de Cloudera para la nube pública de CDP.
	DR	Consulte la recuperación de desastres en la documentación de Cloudera.
	Licencia y modelo operativo (para la cuenta de AWS objetivo)	Modelo Traiga su propia licencia (BYOL)
Conformidad	Requisitos de seguridad	Consulte la descripción general de seguridad de Cloudera en la documentación de Cloudera.
	Otras certificaciones de conformidad	Consulte la información en el sitio web de Cloudera sobre el cumplimiento del Reglamento General de Protección de Datos (GDPR) y el CDP Trust Center.

Requisitos previos y limitaciones

Requisitos previos

- Requisitos de las cuentas de AWS, incluidas las cuentas, los recursos, los servicios y los permisos, como la configuración de las políticas y los roles de AWS Identity and Access Management (IAM)

- Requisitos previos para la implementación de CDP desde el sitio web de Cloudera

La migración requiere los siguientes roles y experiencia:

Rol	Habilidades y responsabilidades
Líder de migración	Garantiza el apoyo ejecutivo, la colaboración en equipo, la planificación, la implementación y la evaluación
Cloudera SME	Conocimientos especializados en administración, administración de sistemas y arquitectura de CDH, HDP y CDP
Arquitecto de AWS	Habilidades en servicios, redes, seguridad y arquitecturas de AWS

Arquitectura

Construir según la arquitectura adecuada es un paso fundamental para garantizar que la migración y el rendimiento satisfagan sus expectativas. Para que su esfuerzo de migración cumpla con las suposiciones de este manual, su entorno de datos de destino en la nube de AWS, ya sea en instancias alojadas en la nube privada virtual (VPC) o en CDP, debe coincidir de manera equivalente con su entorno de origen en términos de versiones del sistema operativo y software, así como de las principales especificaciones de las máquinas.

El siguiente diagrama (reproducido con el permiso de la hoja de datos de Cloudera Shared Data Experience) muestra los componentes de infraestructura del entorno CDP y la forma en que interactúan los niveles o los componentes de la infraestructura.

La arquitectura incluye los siguientes componentes del CDP:

- Data Hub es un servicio para lanzar y gestionar clústeres de cargas de trabajo con tecnología Cloudera Runtime. Puede usar las definiciones de clústeres de Data Hub para aprovisionar clústeres de carga de trabajo y acceder a ellos para casos de uso personalizados y definir

configuraciones de clústeres personalizadas. Para obtener más información, consulte el sitio web de Cloudera.

- El flujo y la transmisión de datos abordan los principales desafíos a los que se enfrentan las empresas con los datos en movimiento. Gestiona lo siguiente:
  - Procesamiento del flujo de datos en tiempo real a gran volumen y a gran escala
  - Seguimiento de la procedencia de los datos y del linaje de los datos de streaming
  - Gestión y supervisión de las aplicaciones periféricas y las fuentes de streaming

  Para obtener más información, consulte Cloudera DataFlow y CSP en el sitio web de Cloudera.
- La ingeniería de datos incluye la integración, la calidad y el gobierno de los datos, lo que ayuda a las organizaciones a crear y mantener flujos de trabajo y flujos de datos. Para obtener más información, consulte el sitio web de Cloudera. Aprenda sobre la compatibilidad con instancias de spot para facilitar el ahorro de costos en las cargas de trabajo de ingeniería de datos de AWS for Cloudera.
- Data Warehouse le permite crear data warehouses y data marts independientes que se escalan automáticamente para satisfacer las demandas de carga de trabajo. Este servicio proporciona instancias informáticas aisladas y una optimización automatizada para cada data warehouse y data mart, y le ayuda a ahorrar costos a la vez que cumple los SLA. Para obtener más información, consulte el sitio web de Cloudera. Aprenda sobre la administración de costos y el autoscalamiento de Cloudera Data Warehouse en AWS.
- La base de datos operativa de CDP proporciona una base fiable y flexible para aplicaciones escalables y de alto rendimiento. Ofrece una base de datos escalable, siempre disponible y en tiempo real que proporciona datos estructurados tradicionales junto con datos nuevos y no estructurados dentro de una plataforma operativa y de almacenamiento unificada. Para obtener más información, consulte el sitio web de Cloudera.
- Machine Learning es una plataforma de machine learning nativa de la nube que combina las capacidades de autoservicio de ciencia de datos e ingeniería de datos en un único servicio portátil dentro de una nube de datos empresarial. Permite la implementación escalable del machine learning y la inteligencia artificial (IA) en los datos en cualquier lugar. Para obtener más información, consulte el sitio web de Cloudera.

CDP en AWS

El siguiente diagrama (adaptado con permiso del sitio web de Cloudera) muestra la arquitectura de alto nivel de CDP en AWS. CDP implementa su propio modelo de seguridad para administrar tanto las cuentas como el flujo de datos. Se integran con la IAM mediante el uso de roles entre cuentas.

El plano de control del CDP reside en una cuenta maestra de Cloudera en su propia VPC. Cada cuenta de cliente tiene su propia subcuenta y una VPC única. Los roles de IAM entre cuentas y las tecnologías SSL redirigen el tráfico de administración hacia y desde el plano de control a los servicios de atención al cliente que residen en las subredes públicas enrutables por Internet dentro de cada VPC del cliente. En la VPC del cliente, la experiencia de datos compartidos (SDX) de Cloudera proporciona una seguridad empresarial sólida con una gobernanza y un cumplimiento unificados para que pueda obtener información a partir de sus datos con mayor rapidez. La SDX es una filosofía de diseño que se incorpora a todos los productos de Cloudera. Para obtener más información sobre SDX y la arquitectura de red de nube pública CDP para AWS, consulte la documentación de Cloudera.

Herramientas

Servicios de AWS

- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon Elastic Kubernetes Service (Amazon EKS) le ayuda a ejecutar Kubernetes en AWS sin necesidad de instalar ni mantener su propio plano de control o nodos de Kubernetes.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- Amazon Relational Database Service (Amazon RDS) le ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Automatizar y herramientas

- Para obtener herramientas adicionales, puede usar Cloudera Backup Data Recovery (BDR), AWS Snowball y AWS Snowmobile para ayudar a migrar los datos del CDH, HDP y CDP en las instalaciones al CDP alojado en AWS.

- Para las nuevas implementaciones, le recomendamos que utilice la solución para socios de AWS para CDP.

Epics

Preparación para la migración

Tarea	Descripción	Habilidades requeridas
Involucre al equipo de Cloudera.	Cloudera sigue un modelo de interacción estandarizado con sus clientes y puede trabajar con su integrador de sistemas (SI) para promover el mismo enfoque. Póngase en contacto con el equipo de atención al cliente de Cloudera para que le brinden orientación y los recursos técnicos necesarios para iniciar el proyecto. Ponerse en contacto con el equipo de Cloudera garantiza que todos los equipos necesario s puedan prepararse para la migración a medida que se acerque su fecha. Puede ponerse en contacto con los servicios profesion ales de Cloudera para que su implementación de Cloudera pase de la fase piloto a la fase de producción rápidamente, a un costo menor y con el máximo rendimiento. Para obtener una lista completa de	Líder de migración

Tarea	Descripción	Habilidades requeridas
	ofertas, consulte el sitio web de Cloudera.	
Cree un entorno de nube pública de CDP en AWS para su VPC.	Trabaje con Cloudera Professional Services o su SI para planificar e implement ar la nube pública de CDP en una VPC en AWS.	Arquitecto de la nube, Cloudera SME

Tarea	Descripción	Habilidades requeridas
Priorice y evalúe las cargas de trabajo para la migración.	Evalúe todas sus cargas de trabajo en las instalaciones para determinar cuáles son las más fáciles de migrar. Es mejor migrar primero a las aplicaciones que no son esenciales para la misión, ya que tendrán un impacto mínimo en sus clientes. Guarde las cargas de trabajo esenciales para el final, después de migrar correctam ente otras cargas de trabajo. Nota: Las cargas de trabajo transitorias (CDP Data Engineering) son más fáciles de migrar que las cargas de trabajo persistentes (CDP Data Warehouse). También es importante tener en cuenta el volumen y las ubicacion es de los datos al migrar. Los desafíos pueden incluir replicar los datos de forma continua desde un entorno en las instalaciones a la nube y cambiar los procesos de ingesta de datos para importarlos directamente a la nube.	Líder de migración

Tarea	Descripción	Habilidades requeridas
Analice las actividades de migración de CDH, HDP, CDP y aplicaciones antiguas.	Considere y comience a planificar las siguientes actividades con Cloudera Workload Manager: • Datos y cargas de trabajo para copiar a su entorno de AWS • Datos listos para la nube • Vecinos ruidosos, que consumen recursos y crean problemas a otros inquilinos • Cargas de trabajo elásticas • Clústeres pequeños con una elevada sobrecarga operativa	Líder de migración

Tarea	Descripción	Habilidades requeridas
Complete los requisitos y recomendaciones de Cloudera Replication Manager.	Trabaje con Cloudera Professional Services y su SI para prepararse para migrar las cargas de trabajo a su entorno de nube pública de CDP en AWS. Comprender los siguientes requisitos y recomendaciones puede ayudarle a evitar problemas comunes durante y después de instalar el servicio Replication Manager. • Revise los documentos de respaldo de Replication Manager para confirmar que cumple con los requisitos del entorno y del sistema. Para obtener más información, consulte la matriz de soporte para CDP Public Cloud Replication Manager en el sitio web de Cloudera. • No necesita acceso root a los nodos en los que se instalarán la aplicación Replication Manager y el motor Data Lifecycle Manager (DLM). • Instale Apache Hive durante la instalación inicial de Replication Manager, a menos que esté seguro de que no utilizará la	Líder de migración

Tarea	Descripción	Habilidades requeridas
	replicación de Hive en el futuro. Si decide instalar Hive después de crear las políticas de replicación de HDFS en Replication Manager, tendrá que eliminar y volver a crear todas las políticas de replicación de HDFS después de agregar Hive. • Los clústeres utilizados en Replication Manager deben tener configuraciones simétricas. Cada clúster de una relación de replicación debe estar configurado exactamente de la misma manera en cuanto a seguridad (Kerberos), administración de usuarios (LDAP/AD) y Knox Proxy. Los servicios de clúster, como el Sistema de archivos distribuido de Hadoop (HDFS), Apache Hive, Apache Knox, Apache Ranger y Apache Atlas, pueden tener diferentes configuraciones para una alta disponibilidad (HA). Por ejemplo, los clústeres de origen y de destino pueden tener configuraciones de	

Tarea	Descripción	Habilidades requeridas
	alta y de baja disponibilidad independientes.	

Migración de CDP a AWS

Tarea	Descripción	Habilidades requeridas
Migre la primera carga de trabajo para entornos de desarrollo/pruebas con Cloudera Workload Manager.	Su SI puede ayudarlo a migrar su primera carga de trabajo a la nube de AWS. Debe ser una aplicación que no esté orientada al cliente ni sea esencial para la misión. Las aplicaciones que tienen datos que la nube puede ingerir fácilmente, como las cargas de trabajo de ingeniería de datos de CDP, son candidatas ideales para la migración de desarrollo y pruebas. Se trata de una carga de trabajo transitoria a la que, por lo general, acceden menos usuarios, en comparación con una carga de trabajo persistente, como una carga de trabajo de CDP Data Warehouse, que podría tener muchos usuarios que necesitan un acceso ininterrumpido. Las cargas de trabajo de ingeniería de datos no son persistentes, lo que minimiza el impacto empresarial en caso de que algo vaya	Líder de migración

Tarea	Descripción	Habilidades requeridas
	mal. Sin embargo, estas tareas pueden ser fundament ales para los informes de producción, así que priorice primero las cargas de trabajo de ingeniería de datos de bajo impacto.	

Tarea	Descripción	Habilidades requeridas
Repita los pasos de migración según sea necesario.	Cloudera Workload Manager ayuda a identificar las cargas de trabajo que mejor se adaptan a la nube. Proporciona métricas como las calificaciones de rendimiento de la nube, los planes de tamaño y capacidad para el entorno objetivo y los planes de replicación. Los mejores candidatos para la migración son las cargas de trabajo estacionales, los informes ad hoc y los trabajos intermitentes que no consumen muchos recursos. Cloudera Replication Manager mueve los datos en las instalaciones a la nube y de la nube a las instalaciones. Optimice de forma proactiva las cargas de trabajo, las aplicaciones, el rendimiento y la capacidad de la infraestructura para el almacenamiento de datos, la ingeniería de datos y el machine learning mediante Workload Manager. Para obtener una guía completa sobre cómo modernizar un data warehouse, consulte el sitio web de Cloudera.	Cloudera SME

Recursos relacionados

Documentación de Cloudera:

- Registro de clústeres clásicos con CDP, Cloudera Manager y Replication Manager:
  - Consola de administración
  - Replication en Hive de Replication Manager
- Replicación de Sentry
- Permisos de Sentry
- Lista de verificación para la planificación de clústeres de Data Hub
- Arquitectura de Workload Manager
- Requisitos de Replication Manager
- Observabilidad de la plataforma de datos de Cloudera
- Requisitos de AWS

Documentación de AWS:

- Migración de datos a la nube

Reinicie el agente de replicación de AWS automáticamente sin deshabilitar SELinux después de reiniciar un servidor fuente de RHEL

Creado por Anil Kunapareddy (AWS), Shanmugam Shanker (AWS) y Venkatramana Chintha (AWS)

Entorno: producción	Tecnologías: migración; sistemas operativos	Carga de trabajo: código abierto
Servicios de AWS: servicio de migración de aplicaciones de AWS		

Resumen

El servicio de migración de aplicaciones de AWS ayuda a simplificar, acelerar y automatizar la migración de la carga de trabajo de Red Hat Enterprise Linux (RHEL) a la nube de Amazon Web Services (AWS). Para añadir servidores de origen al Servicio de migración de aplicaciones, instale el agente de replicación de AWS en los servidores.

El servicio de migración de aplicaciones proporciona una replicación asíncrona a nivel de bloques en tiempo real. Esto significa que puede continuar con las operaciones de TI normales durante todo el proceso de replicación. Estas operaciones de TI pueden requerir que reinicie o reinicie el servidor de origen de RHEL durante la migración. Si esto ocurre, el agente de replicación de AWS no se reiniciará automáticamente y la replicación de datos se detendrá. Normalmente, puede configurar Security-Enhanced Linux (SELinux) en modo deshabilitado o permisivo para reiniciar automáticamente AWS Replication Agent. Sin embargo, es posible que las políticas de seguridad de su organización prohíban la desactivación de SELinux y que también tenga que volver a etiquetar sus archivos.

Este patrón describe cómo reiniciar automáticamente el agente de replicación de AWS sin apagar SELinux cuando el servidor de origen de RHEL se reinicia o se reinicia durante una migración.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una carga de trabajo de RHEL en las instalaciones que desee migrar a la nube de AWS.
- El servicio de migración de aplicaciones se inicializó desde la consola del Servicio de migración de aplicaciones. La inicialización solo es necesaria la primera vez que utilice este servicio. Para obtener instrucciones, consulte la documentación de Application Migration Service.
- Política de AWS Identity and Access Management (IAM) vigente para el Servicio de migración de aplicaciones. Para obtener más información, consulte la documentación de Application Migration Service.

Versiones

- RHEL versión 7 o posterior

Herramientas

Servicios de AWS

- AWS Application Migration Service es una solución lift-and-shift (rehospedaje) altamente automatizada que simplifica, agiliza y reduce el costo de la migración de aplicaciones a AWS.

Comandos de Linux

La siguiente tabla proporciona una lista de los comandos de Linux que se ejecutarán en el servidor fuente de RHEL. Estos también se describen en las epics y las historias de este patrón.

Comando	Descripción
`#systemctl –version`	Identifica la versión del sistema.
`#systemctl list-units --type=service`	Muestra todos los servicios activos que están disponibles en el servidor RHEL.
`#systemctl list-units --type=service | grep running`	Muestra todos los servicios que se están ejecutando actualmente en el servidor RHEL.

`#systemctl list-units --type=service | grep failed`	Muestra todos los servicios que no se pudieron cargar después de que el servidor RHEL se reiniciara o se reiniciara.
`restorecon -Rv /etc/rc.d/init.d/aws-replication-service`	Cambia el contexto a `aws-replication-service` .
`yum install policycoreutils*`	Instala las utilidades principales de la política necesarias para el funcionamiento del sistema SELinux.
`ausearch -c "insmod" --raw | audit2allow -M my-modprobe`	Busca en el registro de auditoría y crea un módulo para las políticas.
`semodule -i my-modprobe.pp`	Activa la política.
`cat my-modprobe.te`	Se muestra el contenido del archivo `my-modprobe.te` .
`semodule -l | grep my-modprobe`	Comprueba si la política se ha cargado en el módulo SELinux.

Epics

Instale el agente de replicación de AWS y reinicie el servidor de origen de RHEL

Tarea	Descripción	Habilidades requeridas
Cree un usuario de Application Migration Service con una clave de acceso y una clave de acceso secreta.	Para instalar el agente de replicación de AWS, debe crear un usuario del Servicio de migración de aplicaciones con las credenciales de AWS requeridas. Para obtener instrucciones, consulte la documentación del servicio de migración aplicación.	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
Instale el agente de replicación de AWS.	1. Inicie sesión en la consola de administración de AWS y abra la consola de AWS Lambda en https://console.aws.amazon.com/lambda/. 2. Configure los ajustes de replicación siguiendo las instrucciones de la documentación de Application Migration Service. 3. Instale el agente de replicación de AWS siguiendo las instrucciones de la documentación de Application Migration Service. 4. En la página Servidores de origen, elija el servidor de origen de RHEL y, a continuación, elija Replicación para iniciar la replicación inicial. Para obtener más información, consulte la documentación de Application Migration Service.	Ingeniero de migraciones
Reinicie o resetee el servidor de origen de RHEL.	Reinicie o resetee el servidor de origen de RHEL cuando su Estado de replicación de datos aparezca Correcto en el Panel de migración.	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
Compruebe el estado de la replicación de los datos.	Espere una hora y, a continuación, vuelva a comprobar el estado de la Replicación de los datos en el panel de migración. Debería estar en estado Parado.	Ingeniero de migraciones

Compruebe el estado del agente de replicación de AWS en el servidor de origen de RHEL

Tarea	Descripción	Habilidades requeridas
Identifica la versión del sistema.	Abra la interfaz de línea de comandos del servidor fuente de RHEL y ejecute el siguiente comando para identificar la versión del sistema: `#systemctl –version`	Ingeniero de migraciones
Enumere todos los servicios activos.	Para ver todos los servicios activos disponibles en el servidor RHEL, ejecute el comando: `#systemctl list-units --type=service`	Ingeniero de migraciones
Enumere todos los servicios en ejecución.	Para mostrar todos los servicios que se están ejecutando actualmente en el servidor RHEL, use el comando:	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	`#systemctl list-units --type=service | grep running`	
Enumere todos los servicios que no se pudieron cargar.	Para mostrar todos los servicios que no se pudieron cargar después de que el servidor RHEL se reiniciar a o se reiniciara, ejecute el comando: `#systemctl list-units --type=service | grep failed`	Ingeniero de migraciones

Cree y ejecute el módulo SELinux

Tarea	Descripción	Habilidades requeridas
Cambie el contexto de seguridad.	En la interfaz de línea de comandos del servidor de origen de RHEL, ejecute el siguiente comando para cambiar el contexto de seguridad al servicio de replicación de AWS: `restorecon -Rv /etc/rc.d/init.d/aws-replication-service`	Ingeniero de migraciones
Instale las utilidades principal es.	Para instalar las utilidades principales necesarias para el funcionamiento del sistema	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	SELinux y sus políticas, ejecute el comando: `yum install policycoreutils*`	
Busca el registro de auditoría y crea un módulo para las políticas.	Ejecute el comando: `ausearch -c "insmod" --raw | audit2allow -M my-modprobe`	Ingeniero de migraciones
Muestre el contenido del archivo. my-modprobe-te	El archivo **`my-modprobe.te`** se genera mediante el comando audit2allow. Incluye los dominios de SELinux, el directorio de fuentes de políticas y los subdirectorios, y especifica las reglas y transiciones de los vectores de acceso asociadas a los dominios. Para mostrar el contenido del archivo, ejecute el comando: `cat my modprobe.te`	Ingeniero de migraciones
Activa la política.	Para insertar el módulo y activar el paquete de políticas, ejecute el comando: `semodule -i my-modprobe.pp`	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
Compruebe si el módulo se ha cargado.	Ejecute el comando: `semodule -l | grep my-modprobe` Una vez cargado el módulo SELinux, ya no tendrá que configurar SELinux en modo desactivado o permisivo durante la migración.	Ingeniero de migraciones
Reinicie o resetee el servidor de origen de RHEL y compruebe el estado de la replicación de los datos.	Abra la consola de AWS Migration Service, vaya a Progreso de la replicación de datos y, a continuación, reinicie o resetee el servidor de origen de RHEL. La replicación de datos ahora debería reanudarse automáticamente después de que se reinicie el servidor de origen de RHEL.	Ingeniero de migraciones

Recursos relacionados

- Documentación de Application Migration Service
- Materiales de formación técnica
- Solución de problemas con AWS Replication Agent
- Políticas de Application Migration Service

Rediseñar

Temas

- Convierta el tipo de datos VARCHAR2 (1) para Oracle en un tipo de datos booleano para Amazon Aurora PostgreSQL
- Crear usuarios y roles de aplicaciones en Aurora compatible con PostgreSQL
- Emule Oracle DR mediante una base de datos global de Aurora compatible con PostgreSQL
- Migre gradualmente de Amazon RDS para Oracle a Amazon RDS para PostgreSQL con Oracle SQL Developer y AWS SCT
- Cargar archivos BLOB en TEXT mediante la codificación de archivos en Aurora compatible con PostgreSQL
- Migrar Amazon RDS para Oracle a Amazon RDS para PostgreSQL en modo SSL mediante AWS DMS
- Migre Amazon RDS para Oracle a Amazon RDS para PostgreSQL con AWS SCT y AWS DMS mediante AWS CLI y AWS CloudFormation
- Migre los paquetes pragma SERIALLY_REUTILIZABLE de Oracle a PostgreSQL
- Migre tablas externas de Oracle a Amazon Aurora compatible con PostgreSQL
- Migre índices basados en funciones de Oracle a PostgreSQL
- Migrar las funciones nativas de Oracle a PostgreSQL mediante extensiones
- Migrar una base de datos de Db2 de Amazon EC2 a Aurora compatible con MySQL mediante AWS DMS
- Migración de una base de datos de Microsoft SQL Server de Amazon EC2 a Amazon DocumentDB mediante AWS DMS
- Migre una base de datos ThoughtSpot Falcon local a Amazon Redshift
- Migrar una base de datos de Oracle a Amazon DynamoDB mediante AWS DMS
- Migre una tabla particionada de Oracle a PostgreSQL mediante AWS DMS
- Migrar de Amazon RDS para Oracle a Amazon RDS para MySQL
- Migrar de IBM Db2 en Amazon EC2 a compatible con Aurora PostgreSQL mediante AWS DMS y AWS SCT
- Migre de Oracle 8i o 9i a Amazon RDS para PostgreSQL mediante AWS DMS SharePlex
- Migre de Oracle 8i o 9i a Amazon RDS para PostgreSQL mediante la vista materializada y AWS DMS

- Migración de Oracle en Amazon EC2 a Amazon RDS para MySQL con AWS DMS y AWS SCT
- Migración de Oracle a Amazon DocumentDB con AWS DMS
- Migrar una base de datos Oracle de Amazon EC2 a Amazon RDS para MariaDB mediante AWS DMS y AWS SCT
- Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para MySQL con AWS DMS y AWS SCT
- Migre una base de datos Oracle en las instalaciones a Amazon RDS para PostgreSQL mediante Oracle Bystander y AWS DMS
- Migre de Oracle Database a Amazon RDS for PostgreSQL mediante Oracle GoldenGate
- Migración de una base de datos de Oracle a Amazon Redshift con AWS DMS y AWS SCT
- Migrar una base de datos de Oracle a Aurora PostgreSQL con AWS DMS y AWS SCT
- Migre datos de una base de datos Oracle en las instalaciones a Aurora PostgreSQL
- Migración de SAP ASE a Amazon RDS para SQL Server utilizando AWS DMS
- Migre una base de datos de Microsoft SQL Server en las instalaciones a Amazon Redshift mediante AWS DMS
- Migre una base de datos en las instalaciones de Microsoft SQL Server a Amazon Redshift mediante agentes de extracción de datos de AWS SCT
- Migración de una base de datos de Teradata a Amazon Redshift con los agentes de extracción de datos de AWS SCT
- Migración de una base de datos Vertica en las instalaciones a Amazon Redshift con los agentes de extracción de datos de AWS SCT
- Migre aplicaciones heredadas de Oracle Pro*C a ECPG
- Migre columnas generadas de forma virtual de Oracle a PostgreSQL
- Configure la funcionalidad UTL_FILE de Oracle en Aurora compatible con PostgreSQL
- Validar los objetos de la base de datos después de migrar de Oracle a Amazon Aurora PostgreSQL

Convierta el tipo de datos VARCHAR2 (1) para Oracle en un tipo de datos booleano para Amazon Aurora PostgreSQL

Creado por Naresh Damera (AWS)

Entorno: PoC o piloto	Origen: Oracle	Destino: Amazon Aurora PostgreSQL
Tipo R: renovar arquitectura	Carga de trabajo: Oracle	Tecnologías: migración ; desarrollo y pruebas de software; almacenamiento y respaldo; bases de datos
Servicios de AWS: Amazon Aurora; AWS DMS; Amazon RDS; AWS SCT		

Resumen

Durante una migración de Amazon Relational Database Service (Amazon RDS) para Oracle a Amazon Aurora PostgreSQL Compatible Edition, es posible que se produzca una discrepancia de datos al validar la migración en Amazon Web Services (AWS) Database Migration Service (AWS) Database Migration Service (AWS DMS). Para evitar esta discrepancia, puede convertir el tipo de datos VARCHAR2 (1) en un tipo de datos booleano.

El tipo de datos VARCHAR2 almacena cadenas de texto de longitud variable y VARCHAR2 (1) indica que la cadena tiene una longitud de 1 carácter o 1 byte. Para obtener más información sobre VARCHAR2, consulte Tipos de datos integrados de Oracle (documentación de Oracle).

En este patrón, en la columna de la tabla de datos fuente de ejemplo, los datos de VARCHAR2 (1) son una Y, para Sí, o N, para No. Este patrón incluye instrucciones para usar AWS DMS y Herramienta de conversión de esquemas de AWS (AWS SCT) para convertir este tipo de datos de los valores Y y N de VARCHAR2 (1) a valores true o false en booleano.

Público objetivo

Este patrón se recomienda para quienes tengan experiencia en la migración de bases de datos de Oracle a una versión compatible con Aurora PostgreSQL mediante AWS DMS. A medida

que complete la migración, siga las recomendaciones de Convertir Oracle a Amazon RDS para PostgreSQL o Amazon Aurora PostgreSQL (documentación de AWS SCT).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Confirme que su entorno esté preparado para Aurora, incluida la configuración de credenciales, permisos y un grupo de seguridad. Para obtener más información, consulte Configuración del entorno para Amazon Aurora (documentación de Aurora).
- Base de datos Amazon RDS para Oracle de origen que contiene una columna de tabla con datos de VARCHAR2 (1).
- Instancia de base de datos compatible con Amazon Aurora PostgreSQL. Para obtener más información, consulte Creación de un clúster de base de datos y cómo conectarse a una base de datos en un clúster de base de datos de Aurora PostgreSQL (documentación de Aurora).

Versiones de producto

- Opciones de Amazon RDS para Oracle Versión 12.1.0.2 o posterior.
- AWS DMS versión 3.1.4 o posterior. Para obtener más información, consulte Uso de una base de datos Oracle como fuente para AWS DMS y Uso de una base de datos PostgreSQL como destino para AWS DMS (documentación de AWS DMS). Le recomendamos utilizar la versión más reciente de AWS DMS para obtener el soporte más completo de versiones y características.
- Herramienta de conversión de esquemas de AWS (AWS SCT) versión 1.0.632 o posterior. Le recomendamos utilizar la última versión de AWS SCT para obtener el soporte más completo de versiones y características.
- Aurora es compatible con las versiones de PostgreSQL que figuran en Versiones del motor de base de datos para Aurora compatibles con PostgreSQL (documentación de Aurora).

Arquitectura

Pila de tecnología de origen

Recurso de instancia de base de datos de Amazon RDS para Oracle

Pila de tecnología de destino

Instancia de base de datos compatible con Amazon Aurora PostgreSQL

Arquitectura de origen y destino

Herramientas

Servicios de AWS

- La edición de Amazon Aurora compatible con PostgreSQL es un motor de base de datos relacional completamente administrado y compatible con ACID que le permite configurar, administrar y escalar implementaciones de PostgreSQL.
- AWS Database Migration Service (AWS DMS) le permite migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones.
- Amazon Relational Database Service (Amazon RDS) para Oracle ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS.
- Herramienta de conversión de esquemas de AWS (AWS SCT) simplifica las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado a un formato compatible con la base de datos de destino.

Otros servicios

- Oracle SQL Developer es un entorno de desarrollo integrado que simplifica el desarrollo y la administración de bases de datos de Oracle, tanto en implementaciones tradicionales como en implementaciones basadas en la nube. En este patrón, utilice esta herramienta para conectarse a la instancia de base de datos Amazon RDS para Oracle y consultar los datos.
- pgAdmin es una herramienta de gestión de código abierto para PostgreSQL. Proporciona una interfaz gráfica que permite crear, mantener y utilizar objetos de bases de datos. En este patrón, utilice esta herramienta para conectarse a la instancia de base de datos Aurora y consultar los datos.

Epics

Preparar la migración

Tarea	Descripción	Habilidades requeridas
Crear un informe de migración de bases de datos.	1. Crear un informe de evaluación de la migración de la base de datos en AWS SCT. Para obtener más información, consulte Creación de informes de evaluación de la migración. 2. Revise y lleve a cabo las acciones del informe de evaluación de la migración. Para obtener más información, consulte el informe de evaluación, consulte Elementos de acción del informe de evaluación.	Administrador de base de datos, desarrollador
Elimine las restricciones de clave externa en la base de datos de destino.	En PostgreSQL, las claves foráneas se implementan mediante activadores. Durante la fase de carga completa, AWS DMS carga cada tabla de una en una. Recomendamos encarecidamente que deshabilite las restricciones de clave externa durante una carga completa, utilizando uno de los siguientes métodos: • Deshabilite temporalmente todos los disparadores de la	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
	instancia y finalice la carga completa. • Utilice el parámetro `session_replicatio n_role` en PostgreSQL. Si no es posible deshabili tar las restricciones de clave externa, cree una tarea de migración a AWS DMS para los datos principales que sea específica de la tabla principal y la tabla secundaria.	
Deshabilite las claves principal es y únicas en la base de datos de destino.	Con los siguientes comandos, deshabilite las claves y restricciones principales de la base de datos de destino. Esto ayuda a mejorar el rendimiento de la tarea de carga inicial. `ALTER TABLE <table> DISABLE PRIMARY KEY;` `ALTER TABLE <table> DISABLE CONSTRAINT <constraint_name>;`	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
Cree la tarea de carga inicial.	En AWS DMS, cree la tarea de migración para la carga inicial. Para obtener instrucciones, consulte Creación de tareas. En Migration type (Tipo de migración), elija Migrate existing data (Migrar datos existentes). Este método de migración se llama `Full Load` en la API. No inicie esta tarea todavía.	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
Edite la configuración de la tarea de carga inicial.	Edite la configuración de la tarea para añadir la validación de datos. Estos ajustes de validación se deben crear en un archivo JSON. Para obtener instrucciones y ejemplos, consulte Especificar la configuración de las tareas. Añada las siguientes validaciones: • Para validar que los datos de VARCHAR2 (1) se han convertido correctamente a booleanos en la base de datos de destino, añada el código en el Script de validación de datos de la sección Información adicional de este patrón. El script de validación convierte los valores booleanos de 1 en Y y de 0 en N de la tabla de destino y, a continuación, compara los valores de la tabla de destino con la tabla de origen. Para validar el resto de la migración de datos, habilite la validación de datos en la tarea. Para obtener más información consulte	Administrador de AWS, Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Configuración de tareas de validación de datos.	
Creación de una tarea de replicación continua.	En AWS DMS, cree la tarea de migración que mantenga la base de datos de destino sincronizada con la base de datos de origen. Para obtener instrucciones, consulte Creación de tareas. Para el método de migración, elija Replicar solo los cambios de datos. No inicie esta tarea todavía.	Administrador de base de datos

Probar las tareas de migración

Tarea	Descripción	Habilidades requeridas
Cree datos de muestra para realizar pruebas.	En la base de datos de origen, cree una tabla de muestra con datos para realizar pruebas.	Desarrollador
Confirme que no haya actividades conflictivas.	Utilice `pg_stat_activity` para comprobar si hay alguna actividad en el servidor que pueda afectar a la migración . Para obtener más informaci ón, consulte Recopilador de estadísticas (documentación de PostgreSQL).	Administrador de AWS
Inicie las tareas de migración de AWS DMS.	En la consola de AWS DMS, en la página del Panel de control, inicie la carga inicial	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	y las tareas de replicación en curso que creó en la epopeya anterior.	
Supervise las tareas y los estados de carga de la tabla.	Durante la migración, supervise el estado de las tareas y los estados de la tabla. Cuando se complete la tarea de carga inicial, en la pestaña Estadísticas de la tabla: • El Estado de carga debe ser Tabla completada. • El Estado de validación debe estar Validado.	Administrador de AWS
Compruebe los resultados de la migración.	Con pgAdmin, consulte la tabla en la base de datos de destino. Una consulta correcta indica que los datos se migraron correctamente.	Desarrollador
Agregue claves principales y claves externas a la base de datos de destino.	Cree la clave principal y la clave externa en la base de datos de destino. Para obtener más información, consulte ALTER TABLE (sitio web de PostgreSQL).	Administrador de base de datos
Elimine los datos de la prueba.	En las bases de datos de origen y destino, limpie los datos que se crearon para las pruebas unitarias.	Desarrollador

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Completar la migración.	Repita la epopeya anterior, pruebe las tareas de migración utilizando los datos de origen reales. De este modo, se migran los datos desde la base de datos de origen a la base de datos de destino.	Desarrollador
Valide que las bases de datos de origen y destino estén sincronizadas.	Valide que las bases de datos de origen y destino estén sincronizadas. Para obtener más información e instrucciones, consulte Validación de datos de AWS DMS.	Desarrollador
Detenga la base de datos de origen.	Detenga la base de datos de Amazon RDS para Oracle. Para obtener instrucciones, consulte Detener temporalmente una instancia de base de datos de Amazon RDS. Al detener la base de datos de origen, la carga inicial y las tareas de replicación en curso en AWS DMS se detienen automáticamente. No es necesario realizar ninguna acción adicional para detener estas tareas.	Desarrollador

Recursos relacionados

Referencias de AWS

- Migre una base de datos de Oracle a Aurora PostgreSQL con AWS DMS y AWS SCT (Recomendaciones de AWS)
- Conversión de Oracle a Amazon RDS para PostgreSQL o Amazon Aurora PostgreSQL (documentación de AWS SCT)
- Cómo funciona AWS DMS (documentación de AWS DMS)

Otras referencias

- Tipo de datos booleano (documentación de PostgreSQL)
- Tipos de datos integrados de Oracle (documentación de Oracle)
- pgAdmin (sitio web de pgAdmin)
- SQL Developer (sitio web de Oracle)

Tutoriales y vídeos

- Introducción a AWS DMS
- Introducción a Amazon RDS
- Introducción a AWS DMS (vídeo)
- Descripción de Amazon RDS (vídeo)

Información adicional

Script de validación de datos

El siguiente script de validación de datos convierte 1 en Y y 0 en N. Esto ayuda a que la tarea de AWS DMS complete y supere correctamente la validación de la tabla.

```
{
"rule-type": "validation",
"rule-id": "5",
"rule-name": "5",
"rule-target": "column",
"object-locator": {
```

```
"schema-name": "ADMIN",
"table-name": "TEMP_CHRA_BOOL",
"column-name": "GRADE"
},
"rule-action": "override-validation-function",
"target-function": "case grade when '1' then 'Y' else 'N' end"
        }
```

La sentencia `case` del script realiza la validación. Si se produce un error en la validación, AWS DMS inserta un registro en la tabla public.awsdms_validation_failures_v1 de la instancia de base de datos de destino. Este registro incluye el nombre de la tabla, el tiempo de error y detalles sobre los valores que no coinciden en las tablas de origen y destino.

Si no añade este script de validación de datos a la tarea de AWS DMS y los datos se insertan en la tabla de destino, la tarea de AWS DMS mostrará el estado de validación como Registros no coincidentes.

Durante la conversión a SCT de AWS, la tarea de migración de AWS DMS cambia el tipo de datos del tipo de datos VARCHAR2 (1) a booleano y añade una restricción de clave principal en la columna `"NO"`.

Crear usuarios y roles de aplicaciones en Aurora compatible con PostgreSQL

Creado por Abhishek Verma (AWS)

Entorno: PoC o piloto	Origen: Cualquier base de datos	Destino: Base de datos PostgreSQL
Tipo R: renovar arquitectura	Carga de trabajo: código abierto	Tecnologías: Migración; bases de datos
Servicios de AWS; Amazon RDS; Amazon Aurora		

Resumen

Al migrar a la edición compatible con PostgreSQL de Amazon Aurora, los usuarios y roles de la base de datos que existen en la base de datos de origen deben crearse en la base de datos de Aurora compatible con PostgreSQL. Puede crear los usuarios y los roles en Aurora compatibles con PostgreSQL mediante dos enfoques diferentes:

- Utilice usuarios y roles similares en la base de datos de destino y en la base de datos de origen. En este enfoque, los lenguajes de definición de datos (DDL) se extraen de la base de datos de origen para los usuarios y las funciones. A continuación, se transforman y se aplican a la base de datos Aurora compatible con PostgreSQL de destino. Por ejemplo, la entrada del blog Usar SQL para asignar usuarios, roles y concesiones de Oracle a PostgreSQL trata sobre el uso de la extracción de un motor de base de datos de origen de Oracle.
- Utilice usuarios y roles estandarizados que se utilizan habitualmente durante el desarrollo, la administración y para realizar otras operaciones relacionadas en la base de datos. Esto incluye las operaciones de solo lectura, lectura/escritura, desarrollo, administración e implementación realizadas por los respectivos usuarios.

Este patrón contiene las concesiones necesarias para la creación de usuarios y roles en Aurora, compatible con PostgreSQL, necesarias para el enfoque estandarizado de usuarios y roles. Los pasos de creación de usuarios y roles están alineados con la política de seguridad de conceder el

privilegio mínimo a los usuarios de la base de datos. La siguiente tabla muestra los usuarios, sus funciones correspondientes y sus detalles en la base de datos.

Usuarios	Roles	Finalidad
`APP_read`	`APP_RO`	Se utiliza para el acceso de solo lectura al esquema `APP`
`APP_WRITE`	`APP_RW`	Se utiliza para las operaciones de escritura y lectura del esquema `APP`
`APP_dev_user`	`APP_DEV`	Se utiliza con fines de desarrollo en el esquema `APP_DEV`, con acceso de solo lectura al esquema `APP`
`Admin_User`	`rds_superuser`	Se utiliza para realizar operaciones de administrador en la base de datos
`APP`	`APP_DEP`	Se utiliza para crear los objetos del esquema `APP` y para la implementación de objetos en el esquema `APP`

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de Amazon Web Services (AWS)
- Una base de datos PostgreSQL, una base de datos Amazon Aurora de edición compatible con PostgreSQL o una base de datos Amazon Relational Database Service (Amazon RDS) para PostgreSQL

Versiones de producto

- Todas las versiones de PostgreSQL

Arquitectura

Pila de tecnología de origen

- Cualquier base de datos

Pila de tecnología de destino

- Amazon Aurora compatible con PostgreSQL

Arquitectura de destino

El siguiente diagrama muestra los roles de usuario y la arquitectura del esquema en la base de datos Aurora compatible con PostgreSQL.

Automatizar y escalar

Este patrón contiene los usuarios, los roles y el script de creación del esquema, que puede ejecutar varias veces sin que ello afecte a los usuarios actuales de la base de datos de origen o destino.

Herramientas

Servicios de AWS

- La edición Amazon Aurora PostgreSQL-Compatible es un motor de base de datos relacional, compatible con ACID y completamente administrado que le permite configurar, administrar y escalar implementaciones de PostgreSQL.

Otros servicios

- psql es una herramienta frontend basada en un terminal que se instala con todas las instalaciones de PostgreSQL Database. Cuenta con una interfaz de línea de comandos para ejecutar comandos de SQL, PL-PGSQL y del sistema operativo.
- pgAdmin es una herramienta de gestión de código abierto para PostgreSQL. Proporciona una interfaz gráfica que permite crear, mantener y utilizar objetos de bases de datos.

Epics

Crear los usuarios y los roles

Tarea	Descripción	Habilidades requeridas
Cree el usuario de implement ación.	El usuario de implementación APP se utilizará para crear y modificar los objetos de la base de datos durante las implementaciones. Utilice los siguientes scripts para crear el rol de usuario de implement ación APP_DEP en el esquema APP. Valide los derechos de acceso para asegurarse de que este usuario solo tiene el privilegio de crear objetos en el esquema APP requerido. 1. Conéctese al usuario administrador y cree el esquema. `CREATE SCHEMA APP;` 2. Crear el usuario . `CREATE USER APP WITH PASSWORD <password> ;` 3. Cree el rol. `CREATE ROLE APP_DEP ; GRANT all on schema APP to APP_DEP ; GRANT USAGE ON SCHEMA APP to APP_DEP ;`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	<pre>GRANT connect on database <db_name> to APP_DEP ; GRANT APP_DEP to APP;</pre> 4. Para probar los privilegios, conéctese a las tablas APP y cree las tablas. <pre>set search_path to APP; SET CREATE TABLE test(id integer) ; CREATE TABLE</pre> 5. Compruebe los privilegios. <pre>select schemaname , tablename , tableowne r from pg_tables where tablename like 'test' ; schemaname 	tablename | tableowner APP | test	APP</pre>	

Tarea	Descripción	Habilidades requeridas
Cree el usuario de solo lectura.	El usuario de solo lectura `APP_read` se utilizará para realizar la operación de solo lectura en el esquema APP. Utilice los siguientes scripts para crear el usuario de solo lectura. Valide los derechos de acceso para asegurars e de que este usuario tiene privilegios para leer únicament e los objetos del esquema APP y para conceder automátic amente el acceso de lectura a cualquier objeto nuevo creado en el esquema APP. 1. Crear el usuario `APP_read`. `create user APP_read ;` `alter user APP_read` `with password` `'your_password' ;` 2. Cree el rol. `CREATE ROLE APP_ro ;` `GRANT SELECT ON ALL` `TABLES IN SCHEMA APP` `TO APP_RO ;` `GRANT USAGE ON SCHEMA` `APP TO APP_RO` `GRANT CONNECT ON` `DATABASE testdb TO` `APP_RO ;` `GRANT APP_RO TO` `APP_read;`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	3. Para probar los privilegios, inicie sesión con el usuario `APP_read`. `set search_path to APP ;` `create table test1( id integer) ;` `ERROR: permission denied for schema APP` `LINE 1: create table test1( id integer) ;` `insert into test values (34) ;` `ERROR: permission denied for table test` `SQL state: 42501` `select from test` `no rows selected`	

Tarea	Descripción	Habilidades requeridas
Cree el usuario de lectura/escritura.	El usuario de lectura/escritura `APP_WRITE` se utilizará para realizar operaciones de lectura y escritura en el esquema APP. Utilice los siguientes scripts para crear el usuario de lectura/escritura y asignarle la función `APP_RW`. Valide los derechos de acceso para asegurarse de que este usuario solo tiene privilegios de lectura y escritura en los objetos del esquema APP y para conceder automáticamente el acceso de lectura y escritura a cualquier objeto nuevo creado en el esquema APP. 1. Crear el usuario . `CREATE USER APP_WRITE ; alter user APP_WRITE with password 'your_password' ;` 2. Cree el rol. `CREATE ROLE APP_RW; GRANT SELECT, INSERT, UPDATE, DELETE ON ALL TABLES IN SCHEMA APP TO APP_RW ; GRANT CONNECT ON DATABASE postgres to APP_RW ;`	

Tarea	Descripción	Habilidades requeridas
	GRANT USAGE ON SCHEMA APP to APP_RW ; ALTER DEFAULT PRIVILEGES IN SCHEMA APP GRANT SELECT, INSERT, UPDATE, DELETE ON TABLES TO APP_RW ; GRANT APP_RW to APP_WRITE 3. Para probar los privilegios, inicie sesión con el usuario APP_WRITE . SET SEARCH_PATH to APP; CREATE TABLE test1(id integer) ; ERROR: permission denied for schema APP LINE 1: create table test1(id integer) ; SELECT * FROM test ; id ---- 12 INSERT INTO test values (31) ; INSERT 0 1	

Tarea	Descripción	Habilidades requeridas
Cree el usuario administrador.	El usuario administrador `Admin_User` se utilizará para realizar operaciones de administración en la base de datos. Algunos ejemplos de estas operaciones son `CREATE ROLE` y `CREATE DATABASE`. `Admin_User` utiliza la función integrada `rds_superuser` para realizar operaciones de administración en la base de datos. Utilice los siguientes scripts para crear y probar el privilegio del usuario administrador `Admin_User` en la base de datos. 1. Cree el usuario y conceda el rol. `create user Admin_User WITH PASSWORD ‘Your password’ ALTER user Admin_user CREATEDB; ALTER user Admin_user CREATEROLE;` 2. Para probar el privilegio, inicie sesión desde el usuario `Admin_User` . `SELECT * FROM APP.test ; id ----`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	31 CREATE ROLE TEST ; CREATE DATABASE test123 ;	

Tarea	Descripción	Habilidades requeridas
Cree el usuario de desarrollo.	El usuario de desarrollo `APP_dev_user` tendrá derechos para crear los objetos en su esquema local APP_DEV y acceso de lectura en el esquema APP. Utilice los siguientes scripts para crear y probar los privilegios del usuario `APP_dev_user` en la base de datos. 1. Crear el usuario . `CREATE USER APP1_dev_ user with password ‘your password’;` 2. Cree el esquema APP_DEV para el `App_dev_user` . `CREATE SCHEMA APP1_DEV ;` 3. Cree el rol APP_DEV. `CREATE ROLE APP1_DEV ; GRANT APP1_RO to APP1_DEV ; GRANT SELECT ON ALL TABLES IN SCHEMA APP1_DEV to APP1_dev_ user GRANT USAGE, CREATE ON SCHEMA APP1_DEV to APP1_DEV_USER GRANT APP1_DEV to APP1_DEV_USER ;`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	4. Para probar los privilegios, inicie sesión desde `APP_dev_user` . `CREATE TABLE APP1_dev.test1( id integer ) ;` `CREATE TABLE` `INSERT into APP1_dev.test1 ( select * from APP1.test );` `INSERT 0 1` `CREATE TABLE APP1.test4 ( id int) ;` `ERROR: permission denied for schema APP1` `LINE 1: create table APP1.test4 ( id int) ;`	

Recursos relacionados

Documentación de PostgreSQL

- CREAR ROL
- CREAR USUARIO
- Roles predefinidos

Información adicional

Mejora de PostgreSQL 14

PostgreSQL 14 proporciona un conjunto de roles predefinidos que dan acceso a determinadas capacidades e información privilegiadas que se necesitan con frecuencia. Los administradores

(incluidos roles con privilegios `CREATE ROLE`) pueden conceder estos roles u otros roles de su entorno a los usuarios, proporcionándoles acceso a la información y las capacidades especificadas.

Los administradores pueden conceder a los usuarios el acceso a estos roles mediante el comando `GRANT`. Por ejemplo, para conceder el rol `pg_signal_backend` al `Admin_User`, puede ejecutar el siguiente comando.

```
GRANT pg_signal_backend TO Admin_User;
```

El objetivo del rol `pg_signal_backend` es permitir a los administradores habilitar roles de confianza que no son de superusuario para enviar señales a otros backends. Para obtener más información, consulte Mejora de PostgreSQL 14.

Afinar el acceso

En algunos casos, puede ser necesario proporcionar un acceso más detallado a los usuarios (por ejemplo, acceso basado en tablas o en columnas). En esos casos, se pueden crear roles adicionales para conceder esos privilegios a los usuarios. Para obtener información, consulte Concesiones de PostgreSQL.

Emule Oracle DR mediante una base de datos global de Aurora compatible con PostgreSQL

Creado por HariKrishna Boorgadda (AWS)

Entorno: PoC o piloto	Origen: Oracle	Destino: Aurora PostgreSQL
Tipo R: renovar arquitectura	Carga de trabajo: Oracle	Tecnologías: migración; modernización; bases de datos
Servicios de AWS: Amazon Aurora		

Resumen

Las prácticas recomendadas para la recuperación de desastres (DR) a nivel empresarial consisten, básicamente, en diseñar e implementar sistemas de hardware y software tolerantes a fallos que puedan sobrevivir a un desastre (continuidad de la actividad empresarial) y reanudar las operaciones normales (reanudación de la actividad empresarial) con una intervención mínima e, idealmente, sin pérdida de datos. Crear entornos tolerantes a fallos para cumplir los objetivos de la DR empresarial puede ser una empresa larga y costosa, y requiere un firme compromiso por parte de la empresa.

Oracle Database ofrece tres enfoques diferentes de recuperación de desastres que proporcionan el nivel más alto de protección y disponibilidad de datos en comparación con cualquier otro enfoque para proteger datos de Oracle.

- Dispositivo de recuperación sin pérdida de datos de Oracle
- Oracle Active Data Guard
- Oráculo GoldenGate

Este patrón proporciona una forma de emular la recuperación ante GoldenGate desastres de Oracle mediante una base de datos global de Amazon Aurora. La arquitectura de referencia utiliza Oracle GoldenGate for DR en tres regiones de AWS. El patrón redefine la plataforma de la arquitectura de origen a la base de datos global de Aurora, nativa en la nube y basada en la edición compatible con PostgreSQL de Amazon Aurora.

Las bases de datos globales de Aurora están diseñadas para aplicaciones con una huella global. Una única base de datos de Aurora puede abarcar varias regiones de AWS con hasta cinco regiones secundarias. Las bases de datos globales de Aurora ofrecen las siguientes características:

- Replicación física a nivel de almacenamiento
- Lecturas globales de baja latencia
- Recuperación de desastres rápida tras interrupciones en toda la región
- Migraciones rápidas entre regiones
- Bajo retraso de replicación en todas las regiones
- L: impacto en el ittle-to-no rendimiento de su base de datos

Para obtener más información sobre las características y ventajas de las bases de datos globales de Aurora, consulte Uso de las bases de datos globales de Amazon Aurora. Para obtener más información sobre las conmutaciones por error gestionadas y no planificadas, consulte Uso de la conmutación por error en una base de datos global de Amazon Aurora.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un controlador PostgreSQL de Java Database Connectivity (JDBC) para conectividad de aplicaciones
- Una base de datos global de Aurora basada en Amazon Aurora compatible con PostgreSQL
- Una base de datos de Oracle Real Application Clusters (RAC) migrada a la base de datos global de Aurora basada en Aurora compatible con PostgreSQL

Limitaciones de las bases de datos globales de Aurora

- Las bases de datos globales de Aurora no están disponibles en todas las regiones de AWS. Para obtener una lista de las regiones compatibles, consulte Bases de datos globales de Aurora con Aurora PostgreSQL.
- Para obtener información sobre las características no compatibles y otras limitaciones de las bases de datos globales de Aurora, consulte Limitaciones de las bases de datos globales de Amazon Aurora.

Versiones de producto

- Amazon Aurora, edición compatible con PostgreSQL, versión 10.14 o posterior

Arquitectura

Pila de tecnología de origen

- Base de datos Oracle RAC de cuatro nodos
- Oracle GoldenGate

Arquitectura de origen

El siguiente diagrama muestra tres clústeres con Oracle RAC de cuatro nodos en diferentes regiones de AWS replicados mediante Oracle. GoldenGate

Pila de tecnología de destino

- Una base de datos global de Amazon Aurora de tres clústeres basada en Aurora compatible con PostgreSQL, con un clúster en la región principal y dos clústeres en diferentes regiones secundarias

Arquitectura de destino

Herramientas

Servicios de AWS

- La edición Amazon Aurora compatible con PostgreSQL es un motor de base de datos relacional compatible con ACID, completamente administrado, que le permite configurar, administrar y escalar implementaciones de PostgreSQL.
- Las bases de datos globales de Amazon Aurora abarcan varias regiones de AWS, lo que permite lecturas globales de baja latencia y proporcionan una recuperación rápida de cualquier interrupción que pueda afectar a toda una región de AWS.

Epics

Agregue regiones con instancias de base de datos de lectura

Tarea	Descripción	Habilidades requeridas
Adjunte uno o varios clústeres de Aurora secundarios.	En la Consola de administración de AWS, seleccione Amazon Aurora. Seleccione el clúster principal, elija Acciones y seleccione Añadir región en la lista desplegable.	Administrador de base de datos
Seleccione la clase de instancia.	Puede cambiar la clase de instancia del clúster secundario. Sin embargo, le recomendamos mantenerla igual que la clase de instancia del clúster principal.	Administrador de base de datos
Añada la tercera región.	Repita los pasos de esta épica para añadir un clúster en la tercera región.	Administrador de base de datos

Error en la base de datos global Aurora

Tarea	Descripción	Habilidades requeridas
Elimine el clúster secundario de la base de datos global de Aurora.	1. Seleccione el clúster principal en la página de Bases de datos. 2. Seleccione Eliminar de global para conmutar por error a un clúster secundario.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Puede volver a configurar la aplicación para desviar el tráfico de escritura al clúster que acaba de promover.	Cambie el punto de conexión de la aplicación por el del clúster recién promocionado.	Administrador de base de datos
Detenga la ejecución de cualquier operación de escritura en el clúster no disponible.	Detenga la aplicación y cualquier actividad del lenguaje de manipulación de datos (DML) en el clúster que ha eliminado.	Administrador de base de datos
Crear una base de datos global de Aurora.	Ahora puede crear una base de datos global de Aurora con el clúster recién promovido como clúster principal.	Administrador de base de datos

Inicie el clúster principal

Tarea	Descripción	Habilidades requeridas
Seleccione el clúster principal que se va a iniciar desde la base de datos global.	En la consola de Amazon Aurora, en la configuración de la base de datos global, elija el clúster principal.	Administrador de base de datos
Iniciar el clúster.	En la lista desplegable Acciones, seleccione Iniciar. Este proceso puede tardar algún tiempo. Actualice la pantalla para ver el estado o compruebe, en la columna Estado, el estado actual del clúster una vez finalizada la operación.	Administrador de base de datos

Limpie los recursos

Tarea	Descripción	Habilidades requeridas
Elimine los clústeres secundarios restantes.	Tras completar el piloto de conmutación por error, elimine los clústeres secundarios de la base de datos global.	Administrador de base de datos
Elimine el clúster principal.	Eliminar el clúster.	Administrador de base de datos

Recursos relacionados

- Uso de bases de datos globales de Amazon Aurora
- Soluciones de recuperación de desastres de Aurora PostgreSQL mediante Base de datos global de Amazon Aurora (publicación de blog)

Migre gradualmente de Amazon RDS para Oracle a Amazon RDS para PostgreSQL con Oracle SQL Developer y AWS SCT

Documento creado por Pinesh Singal (AWS)

Entorno: PoC o piloto	Origen: bases de datos: relacionales	Destino: Amazon RDS PostgreSQL
Tipo R: renovar arquitectura	Carga de trabajo: Oracle; código abierto	Tecnologías: migración; bases de datos; modernización
Servicios de AWS: Amazon EC2; Amazon RDS		

Resumen

Muchas estrategias y enfoques de migración se ejecutan en varias fases y pueden durar desde unas semanas hasta varios meses. Durante este tiempo, puede experimentar retrasos debido a la aplicación de parches o actualizaciones en las instancias de base de datos de Oracle de origen que desee migrar a las instancias de base de datos de PostgreSQL. Para evitar esta situación, le recomendamos que migre de forma incremental el código de base de datos de Oracle restante al código de base de datos de PostgreSQL.

Este patrón proporciona una estrategia de migración incremental sin tiempo de inactividad para una instancia de base de datos Oracle de varios terabytes que tiene un número elevado de transacciones realizadas después de la migración inicial y que debe migrarse a una base de datos PostgreSQL. Puede utilizar el step-by-step enfoque de este patrón para migrar de forma incremental una instancia de base de datos de Amazon Relational Database Service (Amazon RDS) para Oracle a una instancia de base de datos de Amazon RDS for PostgreSQL sin iniciar sesión en la consola de administración de Amazon Web Services (AWS).

El patrón utiliza Oracle SQL Developer para encontrar las diferencias entre dos esquemas de la base de datos Oracle de origen. A continuación, utilice la herramienta de conversión de esquemas de AWS (AWS SCT) para convertir los objetos de esquema de base de datos de Amazon RDS para Oracle en objetos de esquema de base de datos de Amazon RDS para PostgreSQL. A continuación, puede ejecutar un script de Python en la línea de comandos de Windows para crear objetos SCT de AWS para los cambios incrementales en los objetos de la base de datos de origen.

Nota: Antes de migrar sus cargas de trabajo de producción, le recomendamos que ejecute una prueba de concepto (PoC) para el enfoque de este patrón en un entorno de pruebas o ajeno a la producción.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una instancia de base de datos de Amazon RDS para Oracle.
- Una instancia de base de datos de Amazon RDS para PostgreSQL.
- AWS SCT, instalado y configurado con controladores JDBC para motores de bases de datos Oracle y PostgreSQL. Para obtener más información al respecto, consulte Instalación de AWS SCT e Instalación de los controladores de base de datos necesarios en la documentación de AWS SCT.
- Oracle SQL Developer, instalado y configurado. Para obtener más información acerca de estos componentes, consulte la documentación de Oracle SQL Developer.
- El archivo (adjunto) `incremental-migration-sct-sql.zip`, descargado en su equipo local.

Limitaciones

- Los requisitos mínimos para la instancia de base de datos de Amazon RDS para Oracle son:
  - Oracle versiones 10.2 y posteriores (para las versiones 10.x), 11g (versiones 11.2.0.3.v1 y posteriores) y hasta 12.2 y 18c para las ediciones Enterprise, Standard, Standard One y Standard Two
- Los requisitos mínimos para su instancia de base de datos de Amazon RDS para PostgreSQL de destino son:
  - PostgreSQL versiones 9.4 y posteriores (para las versiones 9.x), 10.x y 11.x
- En este patrón, se utiliza Oracle SQL Developer. Los resultados pueden variar si utiliza otras herramientas para buscar y exportar las diferencias de esquema.
- Los scripts SQL generados por Oracle SQL Developer pueden generar errores de transformación, lo que significa que es necesario realizar una migración manual.

- Si las conexiones de prueba de origen y destino de AWS SCT fallan, asegúrese de configurar las versiones del controlador JDBC y las reglas de entrada para que el grupo de seguridad de la nube privada virtual (VPC) acepte el tráfico entrante.

Versiones de producto

- Instancia de base de datos Amazon RDS para Oracle, versión 12.1.0.2 (versión 10.2 y posteriores)
- Instancia de base de datos Amazon RDS para PostgreSQL versión 11.5 (versión 9.4 y posteriores)
- Oracle SQL Developer, versión 19.1 y posteriores
- AWS SCT versión 1.0.632 y versiones posteriores

Arquitectura

Pila de tecnología de origen

- Amazon RDS para instancia Oracle DB

Pila de tecnología de destino

- Amazon RDS para instancia de base de datos para PostgreSQL

Arquitectura de origen y destino

El siguiente diagrama muestra la migración de una instancia de base de datos Amazon RDS para Oracle a una instancia de base de datos Amazon RDS para PostgreSQL.

En el diagrama, se muestra el siguiente flujo de migración:

1. Abra Oracle SQL Developer y conéctese a las bases de datos de origen y destino.
2. Genere un informe de diferencias y, a continuación, genere el archivo de scripts SQL para los objetos de diferencias de esquema. Para obtener más información acerca de los informes de diferencias, consulte Informes de diferencias detallados en la documentación de Oracle.

3. Configure AWS SCT y ejecute el código de Python.
4. El archivo de scripts SQL se convierte de Oracle a PostgreSQL.
5. Ejecute el archivo de scripts SQL en la instancia de base de datos PostgreSQL de destino.

Automatizar y escalar

Para automatizar esta migración se pueden agregar parámetros adicionales y cambios relacionados con la seguridad para múltiples funcionalidades de un solo programa al Script de Python.

Herramientas

- AWS SCT: la herramienta de conversión de esquemas de AWS (AWS SCT) convierte el esquema de base de datos existente de un motor de base de datos a otro.
- Desarrollador de Oracle SQL: Oracle SQL Developer es un entorno de desarrollo integrado (IDE) que simplifica el desarrollo y la administración de las bases de datos de Oracle, tanto en las implementaciones tradicionales como en las basadas en la nube.

Código

El archivo (adjunto) `incremental-migration-sct-sql.zip` contiene el código fuente completo de este patrón.

Epics

Cree el archivo de scripts SQL para las diferencias del esquema de la base de datos de origen

Tarea	Descripción	Habilidades requeridas
Ejecute Database Diff en Oracle SQL Developer.	1. Inicie sesión en la instancia de base de datos de Oracle de origen, seleccione Herramientas y, a continuación, elija Diferencias en base de datos.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	2. Elija la base de datos de origen en Conexión con origen. 3. Elija la base de datos de origen actualizada o parcheada en Conexión de destino. 4. Configure las opciones restantes según sus requisitos, seleccione Siguiente y, a continuación, elija Finalizar para generar el informe de diferencias.	
Genere el archivo de scripts SQL.	Elija Generar script para generar las diferencias en los archivos SQL. Esto genera el archivo de scripts SQL que AWS SCT utiliza para convertir la base de datos de Oracle a PostgreSQL.	Administrador de base de datos

Use el script de Python para crear los objetos de base de datos de destino en AWS SCT

Tarea	Descripción	Habilidades requeridas
Configure AWS SCT con la línea de comandos de Windows.	1. Copie el archivo `AWSSchemaConversionToolBatch.jar` de la carpeta AWS SCT preinstalada y péguelo en su directorio de trabajo.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	2. Implemente el código Python desde el archivo `run_aws_sct_sql.py` de la carpeta (adjunto) `incremental-migration-sct-sql.zip`. Esto crea archivos.xml y archivos.sct en el directorio `projects` con los detalles de configuración del entorno de base de datos de origen y destino. También lee el archivo de scripts SQL que generó en Oracle SQL Developer. Por último, crea objetos de archivo.sql en el directorio `output`. 3. Configure los detalles de configuración del entorno de origen y destino en el archivo `database_migration.txt` con el formato siguiente: `#source_vendor,source_hostname,source_dbname,source_user,source_pwd,source_schema,source_port,source_sid,target_vendor,target_hostname,target_user,target_pwd,target_dbname,target_port`	

Tarea	Descripción	Habilidades requeridas
	`ORACLE,myoracledb.cokmvis0v46q.us-east-1.rds.amazonaws.com,ORCL,orcl,orcl1234,orcl,1521,ORCL,POSTGRESQL,mypgdbinstance.cokmvis0v46q.us-east-1.rds.amazonaws.com,pguser,pgpassword,pgdb,5432` 4. Modifique los parámetros de configuración de AWS SCT según sus requisitos y, a continuación, copie el archivo de scripts SQL en el directorio de trabajo del subdirectorio `input`.	
Ejecute el script de Python.	1. Ejecute el script mediante el comando siguiente: `$ python run_aws_sct_sql.py database_migration.txt` 2. Esto crea el archivo SQL de los objetos de base de datos. Los códigos no convertidos con errores de transformación se pueden convertir manualmente.	Administrador de base de datos
Cree los objetos en Amazon RDS para PostgreSQL	Ejecute los archivos SQL y cree objetos en su instancia de base de datos de Amazon RDS para PostgreSQL.	Administrador de base de datos

Recursos relacionados

- Oracle en Amazon RDS
- PostgreSQL en Amazon RDS
- Uso de la interfaz de usuario de la AWS SCT
- Uso de Oracle como origen para AWS SCT

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Cargar archivos BLOB en TEXT mediante la codificación de archivos en Aurora compatible con PostgreSQL

Creado por Bhanu Ganesh Gudivada (AWS) y Jeevan Shetty (AWS)

Entorno: producción	Origen: Base de datos de Oracle en las instalaciones	Destino: Aurora compatible con PostgreSQL
Tipo R: renovar arquitectura	Carga de trabajo: Oracle; código abierto	Tecnologías: Migración; bases de datos
Servicios de AWS: Amazon Aurora		

Resumen

A menudo, durante la migración, hay casos en los que hay que procesar datos estructurados y no estructurados que se cargan desde archivos de un sistema de archivos local. Los datos también pueden estar en un juego de caracteres diferente del juego de caracteres de la base de datos.

Estos archivos contienen los siguientes tipos de datos:

- Metadatos – Estos datos describen la estructura del archivo.
- Datos semiestructurados – Son cadenas de texto en un formato específico, como JSON o XML. Es posible que pueda hacer afirmaciones sobre dichos datos, como "siempre empezará por '<' " o "no contiene caracteres de nueva línea".
- Texto completo – Estos datos suelen contener todos los tipos de caracteres, incluyendo los caracteres de nueva línea y comillas. También puede consistir en caracteres multibyte en UTF-8.
- Datos binarios: estos datos pueden contener bytes o combinaciones de bytes, incluidos valores nulos y end-of-file marcadores.

Cargar una combinación de estos tipos de datos puede ser complicado.

El patrón se puede usar con bases de datos de Oracle en las instalaciones, bases de datos de Oracle que se encuentran en instancias de Amazon Elastic Compute Cloud (Amazon EC2) en

Amazon Web Services (AWS) y Amazon Relational Database Service (Amazon RDS) para bases de datos de Oracle. Por ejemplo, este patrón utiliza Amazon Aurora de edición compatible con PostgreSQL.

En la base de datos de Oracle, con la ayuda de un puntero `BFILE` (archivo binario), el paquete `DBMS_LOB` y las funciones del sistema Oracle, puede cargar desde un archivo y convertirlo a CLOB con codificación de caracteres. Como PostgreSQL no admite el tipo de datos BLOB al migrar a una base de datos de Amazon Aurora de edición compatible con PostgreSQL, estas funciones deben convertirse en scripts compatibles con PostgreSQL.

Este patrón proporciona dos enfoques para cargar un archivo en una base de datos de una sola columna en una base de datos de Amazon Aurora compatible con PostgreSQL:

- Método 1: Usted importa datos de su bucket de Amazon Simple Storage Service (Amazon S3) utilizando la función `table_import_from_s3` de la extensión `aws_s3` con la opción de codificación.
- Método 2: Usted codifica en formato hexadecimal fuera de la base de datos y, a continuación, decodifica para ver `TEXT` dentro de la base de datos.

Recomendamos usar el Método 1 porque Aurora, compatible con PostgreSQL, tiene una integración directa con la extensión `aws_s3`.

Este patrón utiliza el ejemplo de cargar un archivo plano que contiene una plantilla de correo electrónico, que tiene caracteres multibyte y formatos distintos, en una base de datos de Amazon Aurora compatible con PostgreSQL.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una instancia de Amazon RDS o una instancia de Aurora compatible con PostgreSQL
- Conocimientos básicos de SQL y del sistema de administración de base de datos relacional (RDBMS)
- Un bucket de Amazon Simple Storage Service (Amazon S3)
- Conocimiento de las funciones del sistema en Oracle y PostgreSQL
- Paquete RPM HexDump -XXD-0.1.1 (incluido con Amazon Linux 2)

Limitaciones

- Para el tipo de datos TEXT, la cadena de caracteres más larga posible que se puede almacenar es de aproximadamente 1 GB.

Versiones de producto

- Aurora es compatible con las versiones de PostgreSQL que aparecen en las actualizaciones de PostgreSQL de Amazon Aurora.

Arquitectura

Pila de tecnología de destino

- Aurora compatible con PostgreSQL

Arquitectura de destino

Método 1: Uso de aws_s3.table_import_from_s3

Desde un servidor en las instalaciones, se transfiere a Amazon S3 un archivo que contiene una plantilla de correo electrónico con caracteres multibyte y un formato personalizado. La función de base de datos personalizada que proporciona este patrón utiliza la función `aws_s3.table_import_from_s3` con `file_encoding` para cargar archivos en la base de datos y regresar los resultados de las consultas como tipo de datos TEXT.

1. Los archivos se transfieren al bucket de S3 de almacenamiento temporal.
2. Los archivos se cargan en la base de datos Amazon Aurora compatible con PostgreSQL.
3. Mediante el cliente pgAdmin, la función `load_file_into_clob` personalizada se implementa en la base de datos Aurora.
4. La función personalizada usa internamente `table_import_from_s3` con file_encoding. El resultado de la función se obtiene utilizando `array_to_string` y `array_agg` como salida TEXT.

Método 2: Codificar en hexadecimal fuera de la base de datos y decodificar para ver el TEXTO dentro de la base de datos

Un archivo de un servidor en las instalaciones o de un sistema de archivos local se convierte en un volcado hexadecimal. A continuación, el archivo se importa a PostgreSQL como un campo `TEXT`.

1. Convierta el archivo en un volcado hexadecimal en la línea de comandos mediante la opción `xxd -p`.
2. Cargue los archivos de volcado hexadecimales en una versión de Aurora compatible con PostgreSQL mediante la opción `\copy` y, a continuación, decodifique los archivos de volcado hexadecimales en binarios.
3. Codifique los datos binarios para regresarlos como `TEXT`.

Herramientas

Servicios de AWS

- La edición de Amazon Aurora compatible con PostgreSQL es un motor de base de datos relacional compatible con ACID, completamente administrado que le permite configurar, utilizar y escalar implementaciones de PostgreSQL.
- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.

Otras herramientas

- pgAdmin4 es una plataforma de administración y desarrollo de código abierto para PostgreSQL. pgAdmin4 se puede usar en Linux, Unix, mac OS y Windows para administrar PostgreSQL.

Epics

Método 1: Importación de datos de Amazon S3 a Aurora compatible con PostgreSQL

Tarea	Descripción	Habilidades requeridas
Lanzar una instancia EC2.	Para obtener instrucciones sobre cómo lanzar una	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	instancia, consulte Lanzar su instancia.	
Instale la herramien ta pgAdmin del cliente PostgreSQL.	Descargue e instale pgAdmin.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree una política de IAM.	Cree una de política AWS Identity and Access Management (IAM) denominada `aurora-s3-access-pol` que conceda acceso al bucket de S3 en el que se almacenar án los archivos. Use el siguiente código, sustituye ndo `<bucket-name>` por el nombre de su bucket de S3. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "s3:GetObject", "s3:AbortMultipartUpload", "s3:DeleteObject", "s3:ListMultipartUploadParts", "s3:PutObject", "s3:ListBucket" ], "Resource": [`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	<pre>"arn:aws:s3:::<bucket-name>/*", "arn:aws:s3:::<bucket-name>"] }] }</pre>	
Cree un rol de IAM para la importación de objetos de Amazon S3 a Aurora compatible con PostgreSQL.	Utilice el siguiente código para crear un rol de IAM `aurora-s3-import-role` con el nombre de la AssumeRolerelación de confianza. `AssumeRole` permite a Aurora acceder a otros servicios de AWS en su nombre. <pre>{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow","Principal": { "Service": "rds.amazonaws.com" },"Action": "sts:AssumeRole" }] }</pre>	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Asocie el rol de IAM al clúster.	Para asociar el rol de IAM al clúster de base de datos compatible con Aurora PostgreSQL, ejecute el siguiente comando de la CLI de AWS. Cambie `<Account-ID>` al ID de la cuenta de AWS que aloja la base de datos Aurora compatible con PostgreSQL. Esto permite que la base de datos Aurora compatible con PostgreSQL acceda al bucket de S3. `aws rds add-role-to-db-cluster --db-cluster-identifier aurora-postgres-cl --feature-name s3Import --role-arn arn:aws:iam::<Account-ID>:role/aurora-s3-import-role`	Administrador de base de datos
Cargue el ejemplo en Amazon S3.	1. En la sección de Información adicional de este patrón, copie el código de la plantilla de correo electrónico en un archivo denominado `salary.event.notification.email.vm` . 2. Cargue el archivo en el bucket de S3.	Administrador de base de datos, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Implemente la función personalizada.	1. En la sección Información adicional, copie el contenido del archivo SQL `load_file_into_clob` de la función personalizada en una tabla temporal. 2. Inicie sesión en la base de datos Aurora compatible con PostgreSQL e impleméntela en el esquema de la base de datos mediante el cliente pgAdmin.	Administrador de base de datos, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Ejecute la función personalizada para importar los datos en la base de datos.	Ejecute el siguiente comando SQL y sustituya los elementos entre paréntesis angulares por los valores adecuados. `select load_file _into_clob('aws-s3 -import-test'::tex t,'us-west-1'::tex t,'employee.salary .event.notificatio n.email.vm'::text);` Sustituya los elementos entre paréntesis angulares por los valores adecuados, como se muestra en el siguiente ejemplo, antes de ejecutar el comando. `Select load_file _into_clob('aws-s3 -import-test'::tex t,'us-west-1'::tex t,'employee.salary .event.notificatio n.email.vm'::text);` El comando carga el archivo desde Amazon S3 y regresa el resultado como TEXT.	Administrador de base de datos, propietario de la aplicación

Método 2: Convertir el archivo de plantilla en un volcado hexadecimal en un sistema Linux local

Tarea	Descripción	Habilidades requeridas
Convierta el archivo de plantilla en un volcado hexadecimal.	La utilidad Hexdump muestra el contenido de los archivos binarios en formato hexadecimal, decimal, octal o ASCII. El comando `hexdump` forma parte del paquete `util-linux` y viene preinstalado en las distribuciones de Linux. El paquete RPM Hexdump también forma parte de Amazon Linux 2. Para convertir el contenido del archivo en un volcado hexadecimal, ejecute el siguiente comando del intérprete de comandos. `xxd -p </path/file.vm> | tr -d '\n' > </path/file.hex>` Sustituya la ruta y el archivo por los valores adecuados, como se muestra en el siguiente ejemplo. `xxd -p employee.salary.event.notification.email.vm | tr -d '\n' > employee.salary.event.notification.email.vm.hex`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cargue el archivo hexdump en el esquema de la base de datos.	Utilice los siguientes comandos para cargar el archivo hexdump en la base de datos Aurora compatible con PostgreSQL. 1. Inicie sesión en la base de datos PostgreSQL de Aurora y cree una tabla nueva llamada `email_template_hex` . `CREATE TABLE email_template_hex(hex_data TEXT);` 2. Cargue los archivos del sistema de archivos local en el esquema de base de datos mediante el siguiente comando. `\copy email_template_hex FROM '/path/file.hex';` Sustituya la ruta por la ubicación del sistema de archivos local. `\copy email_template_hex FROM '/tmp/employee.salary.event.notification.email.vm.hex';`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	3. Cree una tabla más llamada `email_template_bytea` . `CREATE TABLE email_template_bytea(hex_data bytea);` 4. Inserte los datos desde `email_template_hex` a `email_template_bytea` . `INSERT INTO email_template_bytea (hex_data)` `(SELECT decode(hex_data, 'hex') FROM email_template_hex limit 1);` 5. Para devolver el código de bytes hexadecimales como datos TEXT, ejecute el siguiente comando. `SELECT encode(hex_data::bytea, 'escape') FROM email_template_bytea;`	

Recursos relacionados

Referencias

- Utilizar una base de datos PostgreSQL como objetivo para el servicio de migración de bases de datos de AWS
- Manual de migración de la base de datos de Oracle 19c a Amazon Aurora con compatibilidad con PostgreSQL (12.4)
- Crear políticas de IAM
- Asociación de un rol de IAM con un clúster de base de datos Amazon Aurora MySQL
- pgAdmin

Tutoriales

- Introducción a Amazon RDS
- Migración de Oracle a Amazon Aurora

Información adicional

Función personalizada load_file_into_clob

```
CREATE OR REPLACE FUNCTION load_file_into_clob(
    s3_bucket_name text,
    s3_bucket_region text,
    file_name text,
    file_delimiter character DEFAULT '&'::bpchar,
    file_encoding text DEFAULT 'UTF8'::text)
    RETURNS text
    LANGUAGE 'plpgsql'
    COST 100
    VOLATILE PARALLEL UNSAFE
AS $BODY$
DECLARE
    blob_data BYTEA;
    clob_data TEXT;
    l_table_name CHARACTER VARYING(50) := 'file_upload_hex';
    l_column_name CHARACTER VARYING(50) := 'template';
    l_return_text TEXT;
    l_option_text CHARACTER VARYING(150);
    l_sql_stmt CHARACTER VARYING(500);

BEGIN
```

```
    EXECUTE format ('CREATE TEMPORARY TABLE %I (%I text, id_serial serial)',
 l_table_name, l_column_name);

    l_sql_stmt := 'select ''(format text, delimiter ''''' || file_delimiter || ''''',
 encoding ''''' || file_encoding ||  ''''')'' ';

    EXECUTE FORMAT(l_sql_stmt)
    INTO l_option_text;

    EXECUTE FORMAT('SELECT aws_s3.table_import_from_s3($1,$2,$6,
 aws_commons.create_s3_uri($3,$4,$5))')
    INTO l_return_text
    USING l_table_name, l_column_name, s3_bucket_name,
 file_name,s3_bucket_region,l_option_text;

    EXECUTE format('select array_to_string(array_agg(%I order by id_serial),E''\n'')
 from %I', l_column_name, l_table_name)
    INTO clob_data;

    drop table file_upload_hex;

    RETURN clob_data;
END;
$BODY$;
```

Plantilla de correo electrónico

```
##############################################################################################
##
 ##
##    johndoe Template Type: email
 ##
##    File: johndoe.salary.event.notification.email.vm
 ##
##    Author: Aimée Étienne    Date 1/10/2021
      ##
##  Purpose: Email template used by EmplmanagerEJB to inform a johndoe they         ##
##        have been given access to a salary event
 ##
##    Template Attributes:
 ##
```

```
##        invitedUser - PersonDetails object for the invited user
  ##
##        salaryEvent - OfferDetails object for the event the user was given access
 ##
##        buyercollege - CompDetails object for the college owning the salary event
 ##
##        salaryCoordinator - PersonDetails of the salary coordinator for the event
 ##
##        idp - Identity Provider of the email recipient
 ##
##        httpWebRoot - HTTP address of the server
 ##
##
 ##
#################################################################################

$!invitedUser.firstname $!invitedUser.lastname,

Ce courriel confirme que vous avez ete invite par $!salaryCoordinator.firstname $!
salaryCoordinator.lastname de $buyercollege.collegeName a participer a l'evenement
 "$salaryEvent.offeringtitle" sur johndoeMaster Sourcing Intelligence.

Votre nom d'utilisateur est $!invitedUser.username

Veuillez suivre le lien ci-dessous pour acceder a l'evenement.

${httpWebRoot}/myDashboard.do?idp=$!{idp}

Si vous avez oublie votre mot de passe, utilisez le lien "Mot de passe oublie" situe
 sur l'ecran de connexion et entrez votre nom d'utilisateur ci-dessus.

Si vous avez des questions ou des preoccupations, nous vous invitons a
 communiquer avec le coordonnateur de l'evenement $!salaryCoordinator.firstname $!
salaryCoordinator.lastname au ${salaryCoordinator.workphone}.

*******

johndoeMaster Sourcing Intelligence est une plateforme de soumission en ligne pour les
 equipements, les materiaux et les services.

Si vous avez des difficultes ou des questions, envoyez un courriel a
 support@johndoeMaster.com pour obtenir de l'aide.
```

Migrar Amazon RDS para Oracle a Amazon RDS para PostgreSQL en modo SSL mediante AWS DMS

Documento creado por Pinesh Singal (AWS)

Entorno: PoC o piloto	Origen: Amazon RDS para Oracle	Destino: Amazon RDS PostgreSQL
Tipo R: renovar arquitectura	Carga de trabajo: Oracle; código abierto	Tecnologías: Migración ; seguridad, identidad, cumplimiento; bases de datos
Servicios de AWS: AWS DMS; Amazon RDS		

Resumen

Este patrón proporciona una guía para migrar una instancia de base de datos de Amazon Relational Database Service (Amazon RDS) para Oracle a una base de datos de Amazon RDS para PostgreSQL en la nube de Amazon Web Services (AWS). Para cifrar las conexiones entre las bases de datos, el patrón utiliza la autoridad de certificación (CA) y el modo SSL en Amazon RDS y AWS Database Migration Service (AWS DMS).

El patrón describe una estrategia de migración en línea con poco o ningún tiempo de inactividad para una base de datos de origen Oracle de varios terabytes con un número elevado de transacciones. Para garantizar la seguridad de los datos, el patrón utiliza SSL al transferir los datos.

Este patrón utiliza la herramienta de conversión de esquemas de AWS (AWS SCT) para convertir el esquema de base de datos de Amazon RDS para Oracle en un esquema de Amazon RDS para PostgreSQL. A continuación, el patrón utiliza AWS DMS para migrar los datos de la base de datos de Amazon RDS para Oracle a la base de datos de Amazon RDS para PostgreSQL.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa

- Una autoridad de certificación (CA) de bases de datos de Amazon RDS configurada únicamente con rds-ca-2019 (el certificado rds-ca-2015 expiró el 5 de marzo de 2020)
- AWS SCT
- AWS DMS
- pgAdmin
- Herramientas de SQL (por ejemplo, SQL Developer o SQL*Plus)

Limitaciones

- Base de datos Amazon RDS para Oracle: el requisito mínimo es para las versiones 19c de Oracle, para las ediciones Enterprise y Standard Two.
- Base de datos Amazon RDS para PostgreSQL: el requisito mínimo es para PostgreSQL versión 12 y versiones posteriores (para las versiones 9.x y posteriores).

Versiones de producto

- Instancia de base de datos de Amazon RDS para Oracle versión 12.1.0.2
- Instancia de base de datos de Amazon RDS para PostgreSQL versión 11.5

Arquitectura

Pila de tecnología de origen

- Una instancia de base de datos de Amazon RDS para Oracle con la versión 12.1.0.2.v18.

Pila de tecnología de destino

- AWS DMS
- Instancia de base de datos de Amazon RDS para PostgreSQL con la versión 11.5.

Arquitectura de destino

El diagrama siguiente muestra la arquitectura de migración de datos entre las bases de datos de Oracle (origen) y de PostgreSQL (destino). La arquitectura incluye lo siguiente:

- Una nube privada virtual (VPC)

- Una zona de disponibilidad
- Una subred privada
- Una base de datos de Amazon RDS para Oracle
- Una instancia de replicación de AWS DMS
- Una base de datos RDS para PostgreSQL

Para cifrar las conexiones de las bases de datos de origen y destino, los modos CA y SSL deben estar habilitados en Amazon RDS y AWS DMS.

Herramientas

Servicios de AWS

- AWS Database Migration Service (AWS DMS) le permite migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones.
- Amazon Relational Database Service (Amazon RDS) para Oracle ayuda a configurar, utilizar y escalar una base de datos relacional de Oracle en la nube de AWS.
- Amazon Relational Database Service (Amazon RDS) para PostgreSQL ayuda a configurar, utilizar y escalar una base de datos relacional de PostgreSQL en la nube de AWS.
- La Herramienta de conversión de esquemas de AWS (AWS SCT) simplifica las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado, lo que incluye las vistas, los procedimientos almacenados y las funciones, a un formato compatible con la base de datos de destino.

Otros servicios

- pgAdmin es una herramienta de administración de código abierto para PostgreSQL. Proporciona una interfaz gráfica que permite crear, mantener y utilizar objetos de bases de datos.

Epics

Configurar la instancia de Amazon RDS para Oracle

Tarea	Descripción	Habilidades requeridas
Cree la instancia de base de datos Oracle.	Inicie sesión en la cuenta de AWS, abra la Consola de administración de AWS y navegue hasta la consola de Amazon RDS. En la consola, seleccione Create database (Crear base de datos) y, a continuación, Oracle.	AWS general, administrador de bases de datos
Configure grupos de seguridad.	Configure grupos de seguridad entrantes y salientes.	AWS general
Cree un grupo de opciones.	Cree un grupo de opciones en la misma VPC y grupo de seguridad que la base de datos Amazon RDS para Oracle. En Option, seleccion e SSL. Para Port, seleccione 2484 (para conexiones SSL).	AWS general
Configure los ajustes de las opciones.	Utilice los siguientes valores: • `SQLNET.CIPHER_SUIT E : SSL_RSA_W ITH_AES_256_CBC_SH A` • `SQLNET.SSL_VERSION : 1.2 or 1.0`	AWS general
Modifique la instancia de base de datos de RDS para Oracle.	Establezca el certificado de CA como rds-ca-2019.	Administrador de base de datos, AWS general

Tarea	Descripción	Habilidades requeridas
	En Option group (Grupo de opciones), adjunte el grupo de opciones creado anteriormente.	

Tarea	Descripción	Habilidades requeridas
Confirme que la instancia de base de datos de RDS para Oracle esté disponible.	Compruebe que la instancia de base de datos Amazon RDS para Oracle esté activa y en ejecución y que se pueda acceder al esquema de la base de datos. Para conectarse a la base de datos de RDS for Oracle, utilice el comando `sqlplus` de la línea de comandos. `$ sqlplus orcl/**** @myoracledb.cokmvis0v46q.us-east-1.rds.amazonaws.com:1521/ORCL` `SQL*Plus: Release 12.1.0.2.0 Production on Tue Oct 15 18:11:07 2019` `Copyright (c) 1982, 2016, Oracle. All rights reserved.` `Last Successful login time: Mon Dec 16 2019 23:17:31 +05:30` `Connected to:` `Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production` `With the Partitioning, OLAP, Advanced Analytics and Real Application Testing options` `SQL>`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree objetos y datos en la base de datos de RDS para Oracle.	Cree objetos e inserte datos en el esquema.	Administrador de base de datos

Configurar la instancia de Amazon RDS para PostgreSQL

Tarea	Descripción	Habilidades requeridas
Cree la base de datos de RDS para PostgreSQL.	En la página Create database (Crear base de datos) de la consola de Amazon RDS, seleccione PostgreSQL para crear una instancia de base de datos de Amazon RDS para PostgreSQL.	Administrador de base de datos, AWS general
Configure grupos de seguridad.	Configure grupos de seguridad entrantes y salientes.	AWS general
Cree un grupo de parámetros.	Si utiliza la versión 11.x de PostgreSQL, cree un grupo de parámetros para configura r los parámetros de SSL. En la versión 12 de PostgreSQL, el grupo de parámetros SSL está habilitado de forma predeterm inada.	AWS general
Edite los parámetros.	Cambie el parámetro `rds.force_ssl` por `1` (activado). De forma predeterminada, el parámetro `ssl` está	AWS general

Tarea	Descripción	Habilidades requeridas
	definido como 1 (activado). Al establecer el `rds.force_ssl` parámetro en 1, se obliga a todas las conexiones a conectarse únicamente a través del modo SSL.	
Modifique la instancia de base de datos RDS para PostgreSQL.	Establezca el certificado de CA como rds-ca-2019. Adjunte el grupo de parámetros predeterminado o el grupo de parámetros creado anteriormente, según la versión de PostgreSQL.	Administrador de base de datos, AWS general

Tarea	Descripción	Habilidades requeridas
Confirme que la instancia de base de datos de RDS para PostgreSQL esté disponible.	Compruebe que la base de datos de Amazon RDS para PostgreSQL esté activa y en funcionamiento. El comando `psql` establece una conexión SSL con el conjunto `sslmode` desde la línea de comandos. Una opción es configurar `sslmode=1` en el grupo de parámetros y usar una conexión `psql` sin incluir el parámetro `sslmode` en el comando. El resultado siguiente muestra que la conexión SSL está establecida. `$ psql -h mypgdbinstance.cokmvis0v46q.us-east-1.rds.amazonaws.com -p 5432 "dbname=pgdb user=pguser"` `Password for user pguser:` `psql (11.3, server 11.5)` `SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off)` `Type "help" for help.`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	pgdb=> Una segunda opción es configurar `sslmode=1` en el grupo de parámetros e incluir el parámetro `sslmode` en el comando `psql`. El resultado siguiente muestra que la conexión SSL está establecida. `$ psql -h mypgdbinstance.cokmvis0v46q.us-east-1.rds.amazonaws.com -p 5432 "dbname=pgdb user=pguser sslmode=require" Password for user pguser: psql (11.3, server 11.5) SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off) Type "help" for help. pgdb=>`	

Configuración y ejecución de AWS SCT

Tarea	Descripción	Habilidades requeridas
Instale AWS SCT.	Instale la versión más reciente de la aplicación AWS SCT.	AWS general

Tarea	Descripción	Habilidades requeridas
Configure AWS SCT con controladores JDBC.	Descargue los controladores de conectividad de bases de datos Java (JDBC) para Oracle (ojdbc8.jar) y PostgreSQL (postgresql-42.2.5.jar). Para configurar los controladores en AWS SCT, seleccione Settings (Configuración), Global settings (Configuración global) y Drivers (Controladores).	AWS general

Tarea	Descripción	Habilidades requeridas
Cree el proyecto AWS SCT.	Cree el proyecto y el informe de AWS SCT con Oracle como motor de base de datos de origen y Amazon RDS para PostgreSQL como motor de base de datos de destino: 1. Pruebe las conexiones a la base de datos Oracle de origen y a la base de datos de destino de Amazon RDS para PostgreSQL proporcio nando los detalles de la conexión. Para la base de datos Oracle de origen, se requieren los permisos o privilegios siguientes: • `CONNECT` • `SELECT_CATALOG_ROL E` • `SELECT ANY DICTIONARY` • `SELECT on SYS.USER$ TO <sct_user>` Para obtener más informaci ón, consulte Using Oracle Database as a source for AWS SCT (Usar la base de datos de Oracle como origen para AWS SCT).	AWS general

Tarea	Descripción	Habilidades requeridas
	Tanto las conexiones de origen como las de destino deben realizarse correctamente antes de que AWS SCT pueda iniciar el informe de migración. 2. Tras el informe, especifiq ue el esquema que desee convertir y seleccione Finish (Finalizar).	

Tarea	Descripción	Habilidades requeridas
Valide los objetos de la base de datos.	1. Seleccione Load schema (Cargar esquema). AWS SCT muestra los objetos de origen y de destino convertidos, incluidos los objetos que tienen errores. Actualice los objetos incorrectos en la base de datos de destino. 2. Revise los errores y elimínelos mediante una intervención manual. 3. Una vez eliminados todos los errores, vuelva a seleccionar Load schema (Cargar esquema). 4. Seleccione Aplicar a la base de datos. 5. Conéctese a pgAdmin o a cualquier herramienta que admita una conexión a base de datos PostgreSQL y compruebe el esquema y los objetos.	Administrador de base de datos, AWS general

Configurar y ejecutar AWS SCT

Tarea	Descripción	Habilidades requeridas
Cree una instancia de replicación.	1. Inicie sesión en la cuenta, abra la Consola de administración de AWS y	AWS general

Tarea	Descripción	Habilidades requeridas
	navegue hasta la consola de AWS DMS. 2. Cree una instancia de replicación con una configuración válida para la VPC, el grupo de seguridad , la zona de disponibilidad y los atributos de conexión adicionales.	
Importe el certificado.	1. Descargue el certificado rds-ca-2019-root.pem. 2. En la página Certificates, importe el certificado como `rds-ca-2019-root` .	AWS general

Tarea	Descripción	Habilidades requeridas
Cree el punto de conexión de origen.	1. Cree un punto de conexión de origen para Amazon RDS para Oracle; para ello, seleccione Select RDS DB instance (Seleccionar instancia de base de datos RDS) y, a continuación, seleccione la instancia de base de datos RDS para Oracle que ha creado. Los detalles de configuración del punto de conexión se rellenarán automáticamente. 2. Seleccione Provide access information manually (Proporcionar información de acceso manualmente). En Port, asegúrese de especificar 2484. 3. En Secure Socket Layer (SSL) mode, seleccione verify-ca, y, a continuación, seleccione el certificado de CA que creó anteriormente. 4. En Endpoint settings (Configuración de punto de conexión), agregue el atributo de conexión adicional `NumberDataTypeScale=-2` para admitir el tipo de datos `NUMBER` sin tamaño.	AWS general

Tarea	Descripción	Habilidades requeridas
	Para obtener información, consulte Using an Oracle database as a source for AWS Database Migration Service (AWS DMS) (Usar una base de datos de Oracle como origen para AWS Database Migration Service (AWS DMS)).	

Tarea	Descripción	Habilidades requeridas
Cree el punto de conexión de destino.	1. Cree un punto de conexión de destino para Amazon RDS para PostgreSQL; para ello, seleccione Select RDS DB instance (Seleccionar instancia de base de datos de RDS) y, a continuación, seleccione su instancia de base de datos de RDS para PostgreSQL. Los detalles de configuración del punto de conexión se rellenarán automáticamente. 2. Seleccione Provide access information manually (Proporcionar información de acceso manualmente). En Port, asegúrese de especificar 2484. Para obtener más información, consulte Using a PostgreSQL database as a target for AWS Database Migration Service (AWS DMS) (Usar una base de datos de PostgreSQL como destino para AWS Database Migration Service (AWS DMS)).	AWS general

Tarea	Descripción	Habilidades requeridas
Pruebe los puntos de conexión.	1. Pruebe los puntos de conexión de origen y destino para confirmar que ambos funcionen correctamente y estén disponibles. 2. Si una prueba tiene errores, asegúrese de que las reglas de entrada del grupo de seguridad sean válidas.	AWS general

Tarea	Descripción	Habilidades requeridas
Cree tareas de migración.	Para crear una tarea de migración para la captura completa de datos y cambios (CDC) o para la validación de datos, siga los pasos siguientes: 1. Para crear una tarea de migración de base de datos, seleccione la instancia de replicación, el punto de conexión de la base de datos de origen y el punto de conexión de la base de datos de destino. Especifique el tipo de migración de una de las maneras siguientes: • Migrar datos existentes (carga completa) • Replicate data changes only (CDC) (Replicar solo los cambios en los datos [CDC]) • Migrate existing data and replicate ongoing changes (Migrar los datos existentes y replicar los cambios continuos) (carga completa y CDC) 2. En Table mappings (Asignaciones de tabla), puede configurar las reglas de selección y las reglas	AWS general

Tarea	Descripción	Habilidades requeridas
	de transformación en los formatos GUI o JSON: • En Selection rules (Reglas de selección), seleccione el esquema, especifique el nombre de la tabla y seleccione la acción (incluir o excluir) que desee configurar; por ejemplo, Schema ORCL, Table name %, Action Include. • En Transformation rules (Reglas de transform ación), realice una de las acciones siguientes: • Seleccione el esquema y elija la acción (mayúscula, prefijo, sufijo); por ejemplo, Target Schema ORCL, Action Make lowercase . • Seleccione el esquema, especifiq ue el nombre de la tabla y elija la acción (mayúsculas, prefijo, sufijo); por ejemplo, Target Schema ORCL, Table %, Action Make lowercase. 3. Activa la supervisión de Amazon CloudWatch Logs.	

Tarea	Descripción	Habilidades requeridas
	4. Para las reglas de asignación, añada el código JSON siguiente. `{ "rules": [{ "rule-type": "transformation", "rule-id": "1", "rule-name": "1", "rule-target": "table", "object-locator": { "schema-name": "%", "table-name": "%" }, "rule-action": "convert-lowercase", "value": null, "old-value": null }, { "rule-type": "transformation", "rule-id": "2", "rule-name": "2", "rule-target": "schema",`	

Tarea	Descripción	Habilidades requeridas
	"object-locator": { "schema-name": "ORCL", "table-name": "%" }, "rule-action": "convert-lowercase", "value": null, "old-value": null }, { "rule-type": "selection", "rule-id": "3", "rule-name": "3", "object-locator": { "schema-name": "ORCL", "table-name": "DEPT" }, "rule-action": "include", "filters": [] }] }	

Tarea	Descripción	Habilidades requeridas
Planifique el ciclo de producción.	Confirme el tiempo de inactividad con las partes interesadas, como los propietarios de las aplicaciones, para ejecutar AWS DMS en los sistemas de producción.	Guía de la migración

Tarea	Descripción	Habilidades requeridas
Ejecute la tarea de migración.	1. Inicie la tarea de AWS DMS que tenga el estado Listo y supervise los registros de tareas de migración en Amazon CloudWatch para detectar cualquier error. Si eligió Migrate existing data and replicate ongoing changes (Migrar los datos existentes y replicar los cambios en curso) como tipo de migración, y el estado es Load complete ongoing replication (Carga completa, replicación en curso), se ha completado la migración completa con los datos de CDC y la validación está en curso. 2. Tras iniciar la migración, puede obtener información adicional sobre la conexión SSL en. CloudWatch En el caso de Oracle, CloudWatch muestra la siguiente cadena de conexión. `2019-12-17T09:15:11 [SOURCE_UNLOAD ]I: Connecting to Oracle: Beginning session (oracle_endpoint_conn.c:834)`	AWS general

Tarea	Descripción	Habilidades requeridas
	La cadena de conexión de PostgreSQL será similar a la del siguiente ejemplo. `2019-12-17T09:15:11 [TARGET_LOAD ]I: Going to connect to ODBC connection string: PROTOCOL=7.4-0;DRIVER={PostgreSQL};SERVER=mypgdbinstance.cokmvis0v46q.us-east-1.rds.amazonaws.com;DATABASE=pgdb;PORT=5432;sslmode=require;UID=pguser; (odbc_endpoint_imp.c:2218)`	

Tarea	Descripción	Habilidades requeridas
Valide los datos.	Revise los resultados y los datos de las tareas de migración en las bases de datos Oracle de origen y PostgreSQL de destino: 1. Conéctese a pgAdmin y compruebe los datos de su base de datos PostgreSQL con el esquema `ORCL`. 2. En el caso de los CDC, compruebe los cambios en curso; para ello, inserte o actualice los datos en la base de datos Oracle de origen.	Administrador de base de datos
Detenga la tarea de migración.	Tras completarse correctamente la validación de datos, detenga la tarea de migración.	AWS general

Limpie los recursos

Tarea	Descripción	Habilidades requeridas
Elimine las tareas de AWS DMS.	1. En la consola de AWS DMS, vaya a Database migration tasks (Tareas de migración de bases de datos) y detenga cualquier tarea de AWS DMS en curso o en ejecución. 2. Seleccione la tarea o las tareas, luego, Actions y,	AWS general

Tarea	Descripción	Habilidades requeridas
	a continuación, Delete (Borrar).	
Elimine los puntos de conexión de AWS DMS.	Seleccione los puntos de conexión de origen y destino que creó, elija Actions y, a continuación Delete (Eliminar).	AWS general
Elimine la instancia de replicación de AWS DMS.	Seleccione la instancia de replicación, elija Actions y, a continuación, Delete (Eliminar).	AWS general
Elimine la base de datos de PostgreSQL.	1. En la consola de Amazon RDS, seleccione Databases (Bases de datos). 2. Seleccione la instancia de base de datos PostgreSQ L que creó, elija Actions y, a continuación, Delete (Eliminar).	AWS general
Elimine la base de datos de Oracle.	En la consola de Amazon RDS, seleccione la instancia de la base de datos Oracle, elija Actions y, a continuación, Delete (Eliminar).	AWS general

Solución de problemas

Problema	Solución
Las conexiones de prueba de origen y destino de AWS SCT no funcionan.	Configure las versiones del controlador JDBC y las reglas de entrada del grupo de seguridad de VPC para que acepten el tráfico entrante.

Problema	Solución
La prueba del punto de conexión de origen de Oracle no se puede ejecutar.	Compruebe la configuración del punto de conexión y si la instancia de replicación está disponible.
Se produce un error en la ejecución a plena carga de la tarea de AWS DMS.	Compruebe si las bases de datos de origen y destino tienen tipos y tamaños de datos coincidentes.
La tarea de migración de validación de AWS DMS devuelve errores.	1. Compruebe si la tabla tiene una clave principal. Las tablas sin clave principal no se validan. 2. Si la tabla tiene una clave principal pero genera errores, compruebe el atributo de conexión adicional en el punto de conexión de origen. El atributo de conexión adicional debe tener `numberDataTypeScale=-2` para admitir el tipo de datos `NUMBER` sin tamaño de forma dinámica en función de los datos disponibles en la tabla.

Recursos relacionados

Bases de datos

- Amazon RDS para Oracle
- Amazon RDS para PostgreSQL

SSL DB connection (Conexión de bases de datos SSL)

- Using SSL/TLS to encrypt a connection to a DB instance (Usar SSL/TLS para cifrar una conexión a una instancia de bases de datos)
  - Using SSL with an RDS for Oracle DB instance (Usar SSL con una instancia de base de datos de RDS para Oracle)

  - Securing connections to RDS for PostgreSQL with SSL/TLS (Proteger las conexiones a RDS para PostgreSQL con SSL/TLS)
  - Download CA-2019 root certificate (Descargar el certificado raíz CA-2019)
- Working with option groups (Trabajar con grupos de opciones)
  - Adding options to Oracle DB instances (Añadir opciones a instancias de base de datos de Oracle)
  - Oracle Secure Sockets Layer (Capa de conexión segura de Oracle)
- Working with parameter groups (Trabajar con grupos de parámetros)
- PostgreSQL sslmode connection parameter (Parámetro de conexión sslmode de PostgreSQL)
- Using SSL from JDBC (Usar SSL desde JDBC)

AWS SCT

- Herramienta de conversión de esquema de AWS
- Guía del usuario de la herramienta de conversión de esquema de AWS
- Using the AWS SCT user interface (Utilizar la interfaz de usuario de AWS SCT)
- Using Oracle Database as a source for AWS SCT (Utilizar la base de datos de Oracle como origen para AWS SCT)

AWS DMS

- AWS Database Migration Service (AWS DMS)
- AWS Database Migration Service User Guide (Guía del usuario de AWS Database Migration Service)
  - Using an Oracle database as a source for AWS DMS (Utilizar una base de datos de Oracle como origen para AWS DMS)
  - Using a PostgreSQL database as a target for AWS DMS (Utilizar una base de datos de PostgreSQL como destino para AWS DMS)
- Using SSL with AWS Database Migration Service (AWS DMS) (Usar SSL con AWS Database Migration Service (AWS DMS))
- Migrar aplicaciones que ejecutan bases de datos relacionales a AWS

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Migre Amazon RDS para Oracle a Amazon RDS para PostgreSQL con AWS SCT y AWS DMS mediante AWS CLI y AWS CloudFormation

Documento creado por Pinesh Singal (AWS)

Entorno: PoC o piloto	Origen: Amazon RDS para Oracle	Destino: Amazon RDS para PostgreSQL
Tipo R: renovar arquitectura	Carga de trabajo: Oracle; código abierto	Tecnologías: Migración; bases de datos
Servicios de AWS: AWS DMS; Amazon RDS; AWS SCT		

Resumen

En este patrón, se muestra cómo migrar una instancia de base de datos de Amazon Relational Database Service (Amazon RDS) para Oracle a una instancia de base de datos de Amazon RDS para PostgreSQL mediante la Interfaz de la línea de comandos de AWS (AWS CLI). Este enfoque proporciona un tiempo de inactividad mínimo y no requiere iniciar sesión en la Consola de administración de AWS.

Este patrón facilita poder evitar las configuraciones manuales y las migraciones individuales mediante el uso de las consolas de Herramienta de conversión de esquemas de AWS (AWS SCT) y AWS Database Migration Service (AWS DMS). La solución establece una configuración única para varias bases de datos y realiza las migraciones mediante AWS SCT y AWS DMS en la AWS CLI.

El patrón utiliza AWS SCT para convertir los objetos del esquema de base de datos de Amazon RDS para Oracle a Amazon RDS para PostgreSQL y, a continuación, utiliza AWS DMS para migrar los datos. Con scripts de Python en la CLI de AWS, puede crear objetos SCT de AWS y tareas de AWS DMS con una plantilla de AWS CloudFormation .

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.

- Una instancia de base de datos de Amazon RDS para Oracle.
- Una instancia de base de datos de Amazon RDS para PostgreSQL.
- Una instancia de Amazon EC2 o una máquina local con sistema operativo Windows o Linux para ejecutar scripts.
- Conocimiento de los siguientes tipos de tareas de migración de AWS DMS: `full-load`, `cdc`, `full-load-and-cdc`. Para obtener más información, consulte Creating a task (Crear una tarea) en la documentación de AWS DMS.
- AWS SCT, instalado y configurado con controladores JDBC (de conectividad de bases de datos Java) para motores de bases de datos Oracle y PostgreSQL. Para obtener más información, consulte Installing AWS SCT (Instalar AWS SCT) e Installing the required database drivers(Instalar los controladores de base de datos necesarios) en la documentación de AWS SCT.
- El archivo `AWSSchemaConversionToolBatch.jar` de la carpeta SCT de AWS instalada, copiado en el directorio de trabajo.
- El archivo `cli-sct-dms-cft.zip` (adjunto), descargado y extraído en el directorio de trabajo.
- La versión más reciente del motor de instancias de replicación de AWS DMS. Para obtener más información, consulte How do I create an AWS DMS replication instance (Cómo crear una instancia de replicación de AWS DMS) en la documentación de AWS Support y las notas de la versión 3.4.4 de AWS DMS en la documentación de AWS DMS.
- AWS CLI versión 2, instalada y configurada con su ID de clave de acceso, clave de acceso secreta y nombre de región de AWS predeterminado para la instancia de Amazon Elastic Compute Cloud (Amazon EC2) o el sistema operativo (OS) en el que se ejecutan los scripts. Para obtener más información, consulte Installing, updating, and uninstalling the AWS CLI version 2 (Instalar, actualizar y desinstalar la AWS CLI versión 2) y Configuring the AWS CLI (Configurar la AWS CLI) en la documentación de la AWS CLI.
- Familiaridad con las CloudFormation plantillas de AWS. Para obtener más información, consulte CloudFormation los conceptos de AWS en la CloudFormation documentación de AWS.
- Python versión 3, instalado y configurado en la instancia o el sistema operativo Amazon EC2 en el que se ejecutan los scripts. Para obtener más información, consulte la documentación de Phyton.

Limitaciones

- Los requisitos mínimos para la instancia de base de datos de Amazon RDS para Oracle son:

  - Versiones 12c (v12.1.0.2, v12.2.0.1), 18c (v18.0.0.0) y 19c (v19.0.0.0) de Oracle para las ediciones Enterprise, Standard, Standard One y Standard Two.
  - Si bien Amazon RDS es compatible con Oracle 18c (v18.0.0.0), esta versión está en desuso porque Oracle ya no proporciona parches para 18c después de esa fecha. end-of-support Para obtener más información, consulte Oracle on Amazon RDS en la documentación de Amazon RDS.
  - Amazon RDS para Oracle 11g ya no se admite.
- Los requisitos mínimos para la instancia de base de datos de Amazon RDS para PostgreSQL son:
  - PostgreSQL versiones 9 (versiones 9.5 y 9.6), 10.x, 11.x, 12.x y 13.x

Versiones de producto

- Instancia de Amazon RDS para Oracle DB versión 12.1.0.2 y posterior
- Instancia de Amazon RDS para PostgreSQL DB versión 11.5 y posterior
- CLI de AWS versión 2
- La versión más reciente de AWS SCT
- La versión más reciente de Python 3

Arquitectura

Pila de tecnología de origen

- Amazon RDS para Oracle

Pila de tecnología de destino

- Amazon RDS para PostgreSQL

Arquitectura de origen y destino

El diagrama siguiente muestra la migración de una instancia de base de datos Amazon RDS para Oracle a una instancia de base de datos Amazon RDS para PostgreSQL mediante scripts de AWS DMS y Python.

En el diagrama, se muestra el siguiente flujo de trabajo de migración:

1. El script de Python usa AWS SCT para conectarse a las instancias de base de datos de origen y destino.
2. El usuario inicia AWS SCT con el script de Python, convierte el código de Oracle a código PostgreSQL y lo ejecuta en la instancia de base de datos de destino.
3. El script de Python crea tareas de replicación de AWS DMS para las instancias de base de datos de origen y destino.
4. El usuario implementa scripts de Python para iniciar las tareas de AWS DMS y, a continuación, las detiene una vez finalizada la migración de datos.

Automatizar y escalar

Para automatizar esta migración se pueden agregar parámetros adicionales y cambios relacionados con la seguridad para múltiples funcionalidades de un solo programa al Script de Python.

Herramientas

- La Interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que permite interactuar con los servicios de AWS mediante comandos en el intérprete de comandos de línea de comandos.
- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS. Este patrón convierte el archivo de entrada .csv en un archivo de entrada .json mediante un script de Python. El archivo.json se usa en los comandos de la CLI de AWS para crear una CloudFormation pila de AWS que crea varias tareas de replicación de AWS DMS con nombres de recursos de Amazon (ARN), tipos de migración, configuraciones de tareas y asignaciones de tablas.
- AWS Database Migration Service (AWS DMS) le permite migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones. Este patrón usa AWS DMS para crear, iniciar y detener tareas con un script de Python que se ejecuta en la línea de comandos y crea la plantilla de AWS. CloudFormation
- La Herramienta de conversión de esquemas de AWS (AWS SCT) simplifica las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado, lo que incluye las vistas, los procedimientos almacenados y las funciones, a un formato compatible con la base de datos de destino. Este

patrón requiere el archivo `AWSSchemaConversionToolBatch.jar` del directorio de AWS SCT instalado.

Código

El archivo `cli-sct-dms-cft.zip` (adjunto) contiene el código fuente completo de este patrón.

Epics

Configurar AWS SCT y crear objetos de base de datos en la AWS CLI

Tarea	Descripción	Habilidades requeridas
Configure AWS SCT para que se ejecute desde la AWS CLI.	1. Configure los detalles de configuración del entorno de origen y destino en el archivo `database_migration.txt` con el formato siguiente: `#source_vendor,source_hostname,source_dbname,source_user,source_pwd,source_schema,source_port,source_sid,target_vendor,target_hostname,target_user,target_pwd,target_dbname,target_port` `ORACLE,myoracledb.cokmvis0v46q.us-east-1.rds.amazonaws.com,ORCL,orcl,orcl1234,orcl,1521,ORCL,POSTGRESQL,mypgdbinstance.cokmvis0v46q.us-east-1.rds.amazonaws.com,pguser,pgpassword,pgdb,5432`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	2. Modifique los parámetros de configuración de AWS SCT según sus requisitos en los siguientes archivos: `project_settings.xml`, `Oracle_PG_Test_Batch.xml` y `ORACLE-orcl-to-POSTGRESQL.xml`.	
Ejecute el script de Python run_aws_sct.py.	Ejecute el script de Python `run_aws_sct.py` mediante el comando siguiente: `$ python run_aws_sct.py database_migration.txt` El script de Python convierte los objetos de la base de datos de Oracle a PostgreSQL y crea archivos SQL en formato PostgreSQL. El script también crea el archivo `Database migration assessment report` .pdf que proporciona recomendaciones detalladas y estadísticas de conversión para los objetos de la base de datos.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree objetos en Amazon RDS para PostgreSQL.	1. Modifique manualmente los archivos SQL generados por AWS SCT, si es necesario. 2. Ejecute los archivos SQL y cree objetos en su instancia de base de datos de Amazon RDS para PostgreSQL.	Administrador de base de datos

Configure y cree tareas de AWS DMS mediante la CLI de AWS y AWS CloudFormation

Tarea	Descripción	Habilidades requeridas
Cree una instancia de replicación de AWS DMS.	Inicie sesión en la Consola de administración de AWS, abra la consola de AWS DMS y cree una instancia de replicación configurada de acuerdo con sus requisitos. Para obtener más información, consulte Creating a replication instance (Crear una instancia de replicación) en la documentación de AWS DMS y How do I create an AWS DMS replication instance (Cómo crear una instancia de replicación de AWS DMS) en la documentación de AWS Support.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree el punto de conexión de origen.	En la consola de AWS DMS, seleccione Endpoints (Puntos de conexión) y, a continuación, cree un punto de conexión de origen para la base de datos Oracle de acuerdo con sus requisitos. Nota: El atributo de conexión adicional debe ser `numberDataTypeScale` con un valor `-2`. Para obtener más información, consulte Creating source and target endpoints (Crear puntos de conexión de origen y destino) en la documentación de AWS DMS.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree el punto de conexión de destino.	En la consola de AWS DMS, seleccione Endpoints (Puntos de conexión) y, a continquación, cree un punto de conexión de destino para la base de datos de PostgreSQL de acuerdo con sus requisitos. Para obtener más informaci ón, consulte Creating source and target endpoints (Crear puntos de conexión de origen y destino) en la documenta ción de AWS DMS.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Configure los detalles de la replicación de AWS DMS para que se ejecuten desde la AWS CLI.	Configure los puntos de conexión de origen y destino de AWS DMS y los detalles de replicación en el archivo `dms-arn-list.txt` con el ARN del punto de conexión de origen, el ARN del punto de conexión de destino y el ARN de la instancia de replicación mediante el formato siguiente: `#sourceARN,targetARN,repARN` `arn:aws:dms:us-east-1:123456789012:endpoint:EH7AINRUDZ5GOYIY6HVMXECMCQ` `arn:aws:dms:us-east-1:123456789012:endpoint:HHJVUV57N7O3CQF4PJZKGIOYY5` `arn:aws:dms:us-east-1:123456789012:rep:LL57N77AQQAHHJF4PJFHNEDZ5G`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Ejecute el script de Python dms-create-task .py para crear las tareas de AWS DMS.	1. Ejecute el script de Python `dms-create-task.py` mediante el comando siguiente: `$ python dms-create-task.py database_migration.txt dms-arn-list.txt <cft-stack-name> <migration-type>` • `database_migration.txt` es el archivo de texto de migración de la base de datos • `dms-arn-list.txt` es la lista de ARN de AWS DMS • `<cft-stack-name>` es el nombre de la CloudFormation pila de AWS definido por el usuario • `<migration-type>` es el tipo de migración (carga completa, cdc o) full-load-and-cdc 2. Según el tipo de migración, puede usar los comandos siguientes para crear tres tipos de tareas de AWS DMS: • `$ python dms-create-task.py database_`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	migration.txt dms-arn-list.txt dms-cli-cft-stack full-load • $ python dms-create-task.py database_migration.txt dms-arn-list.txt dms-cli-cft-stack cdc • $ python dms-create-task.py database_migration.txt dms-arn-list.txt dms-cli-cft-stack full-load-and-cdc 3. Se crean la CloudFormation pila de AWS y las tareas de AWS DMS	
Compruebe que las tareas de AWS DMS estén listas.	En la consola de AWS, compruebe que las tareas de AWS DMS estén en estado Ready en la sección Status.	Administrador de base de datos

Inicie y detenga las tareas de AWS DMS mediante la AWS CLI

Tarea	Descripción	Habilidades requeridas
Inicie las tareas de AWS DMS.	Ejecute el script de Python dms-start-task.py	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	mediante el comando siguiente: `$ python dms-start-task.py start '<cdc-start-datetime>'` Nota: La fecha y la hora de inicio deben estar en los formatos de tipo de datos de marca de tiempo `'DD-MON-YYYY'` o `'YYYY-MM-DDTHH:MI:SS'` (por ejemplo `'01-Dec-2019'` o `'2018-03-08T12:12:12'`) Puede revisar el estado de las tareas de AWS DMS en la pestaña Table statistics de sus tareas de migración en la página Tasks de la consola de AWS DMS.	

Tarea	Descripción	Habilidades requeridas
Valide los datos.	1. Una vez completada la migración a plena carga, la tarea se mantiene en ejecución de forma continua para garantizar el cambio continuo de datos (CDC). 2. Cuando se complete el CDC o no sea necesario migrar más cambios, revise y valide los resultados y los datos de las tareas de migración en sus bases de datos de Oracle y PostgreSQL. 3. Para validar sus datos puede comprobar las columnas de estado y recuento (`Validation state`, `Validation pending`, `Validation failed`, `Validation suspended` y `Validation details`) en la pestaña Table statistics de la tarea de migración de la base de datos en la página Tasks de la consola de AWS DMS. Para obtener más información consulte la AWS DMS data validation (Validación	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	de datos de AWS DMS) en la documentación de AWS DMS.	
Detenga las tareas de AWS DMS.	Ejecute el script de Python mediante el comando siguiente: `$ python dms-start-task.py stop` Nota: Es posible que las tareas de AWS DMS se detengan con un estado `failed`, en función del estado de la validación. Para obtener más información, consulte la tabla de solución de problemas en la sección Información adicional.	Administrador de base de datos

Solución de problemas

Problema	Solución
Las conexiones de prueba de origen y destino de AWS SCT no funcionan	Configure las versiones del controlador JDBC y las reglas de entrada del grupo de seguridad de VPC para que acepten el tráfico entrante.
La prueba del punto de conexión de origen o destino no se puede ejecutar	Compruebe si la configuración del punto de conexión y la instancia de replicación están en estado `Available` . Compruebe si el estado de la conexión del punto de conexión es `Successful` . Para obtener más información, consulte How can I troubleshoot AWS DMS endpoint

Problema	Solución
	connectivity failures (Cómo solucionar los errores de conectividad de los puntos de conexión de AWS DMS) en la documentación de AWS Support.
La carga completa no se puede ejecutar	Compruebe si las bases de datos de origen y destino tienen tipos y tamaños de datos coincidentes. Para obtener más información, consulte Troubleshooting migration tasks in AWS DMS (Solucionar problemas de las tareas de migración en AWS DMS) en la documentación de AWS DMS.
Errores al ejecutar la validación	Compruebe si la tabla tiene una clave principal , ya que las tablas de claves no principales no están validadas. Si la tabla tiene una clave principal y errores, compruebe que el atributo de conexión adicional del punto de conexión de origen tenga `numberDataTypeScale=-2` . Para obtener más información, consulte Atributos de conexión adicionales al utilizar Oracle como fuente de AWS DMS y Solución de problemas en la documentación de AWS DMS. OracleSettings

Recursos relacionados

- Installing AWS SCT (Instalar AWS SCT)
- Introducción a AWS DMS (vídeo)
- Uso de la CLI de AWS en AWS CloudFormation

- Using the AWS SCT user interface (Utilizar la interfaz de usuario de AWS SCT)
- Using an Oracle database as a source for AWS DMS (Utilizar una base de datos de Oracle como origen para AWS DMS)
- Using Oracle as a source for AWS SCT (Utilizar Oracle como origen para AWS SCT)
- Using a PostgreSQL database as a target for AWS DMS (Utilizar una base de datos de PostgreSQL como destino para AWS DMS)
- Sources for data migration in AWS DMS (Orígenes para la migración de datos en AWS DMS)
- Targets for data migration in AWS DMS (Destinos para la migración de datos en AWS DMS)
- cloudformation (documentación de AWS CLI)
- cloudformation create-stack (documentación de AWS CLI)
- dms (documentación de AWS CLI)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Migre los paquetes pragma SERIALLY_REUTILIZABLE de Oracle a PostgreSQL

Creado por Vinay Paladi (AWS)

Entorno: PoC o piloto	Origen: base de datos de Oracle	Destino: PostgreSQL
Tipo R: renovar arquitectura	Carga de trabajo: Oracle; código abierto	Tecnologías: migración; bases de datos
Servicios de AWS: AWS SCT; Amazon Aurora		

Resumen

Este patrón proporciona un step-by-step enfoque para migrar paquetes de Oracle que se definen como pragma SERIALLY_REUTILIZABLE a PostgreSQL en Amazon Web Services (AWS). Este enfoque mantiene la funcionalidad del pragma SERIALLY_REUTILIZABLE.

PostgreSQL no admite el concepto de paquetes ni el pragma SERIALLY_REUTILIZABLE. Para obtener una funcionalidad similar en PostgreSQL, puede crear esquemas para paquetes e implementar todos los objetos relacionados (como funciones, procedimientos y tipos) dentro de los esquemas. Para lograr la funcionalidad del pragma SERIALLY_REUTILIZABLE, el script de función contenedora de ejemplo que se proporciona en este patrón utiliza un paquete de extensiones de Herramienta de conversión de esquemas de AWS (AWS SCT).

Para obtener más información, consulte SERIALLY_REUSABLE Pragma en la documentación de Oracle.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- La versión más reciente de AWS SCT y los controladores necesarios

- Una base de datos de Edición compatible con Amazon Aurora PostgreSQL o una Amazon Relational Database Service (Amazon RDS) para PostgreSQL

Versiones de producto

- Oracle Database versión 10g y posteriores

Arquitectura

Pila de tecnología de origen

- Oracle Database en las instalaciones

Pila de tecnología de destino

- Aurora compatible con PostgreSQL o Amazon RDS para PostgreSQL
- AWS SCT

Arquitectura de migración

Herramientas

Servicios de AWS

- La Herramienta de conversión de esquemas de AWS (AWS SCT) simplifica las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado, lo que incluye las vistas, los procedimientos almacenados y las funciones, a un formato compatible con la base de datos de destino.
- La edición Amazon Aurora compatible con PostgreSQL es un motor de base de datos relacional compatible con ACID, completamente administrado, que le permite configurar, administrar y escalar implementaciones de PostgreSQL.
- Amazon Relational Database Service (Amazon RDS) para PostgreSQL le ayuda a configurar, utilizar y escalar una base de datos relacional de PostgreSQL en la nube de AWS.

Otras herramientas

- pgAdmin es una herramienta de gestión de código abierto para PostgreSQL. Proporciona una interfaz gráfica que permite crear, mantener y utilizar objetos de bases de datos.

Epics

Migre el paquete de Oracle mediante AWS SCT

Tarea	Descripción	Habilidades requeridas
Configure SCT de AWS.	Configure la conectividad de AWS SCT con la base de datos de origen. Para obtener más información, consulte Uso de una base de datos de Oracle como origen para AWS SCT.	Administrador de base de datos, desarrollador
Convierta el script.	Utilice AWS SCT para convertir el paquete de Oracle seleccionando la base de datos de destino como compatible con Aurora PostgreSQL.	Administrador de base de datos, desarrollador
Guarde los archivos.sql.	Antes de guardar el archivo.sql, modifique la opción Configuración del proyecto en AWS SCT a Archivo único por etapa. AWS SCT separará el archivo.sql en varios archivos.sql según el tipo de objeto.	Administrador de base de datos, desarrollador
Cambiar el código.	Abra la función `init` generada por AWS SCT y cámbiela como se muestra en el ejemplo de la sección Información adicional. Añadirá una variable para lograr la	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
	funcionalidad de `pg_serialize = 0` .	
Pruebe la conversión.	Implemente la función `init` en la base de datos compatible con Aurora PostgreSQL y pruebe los resultados.	Administrador de base de datos, desarrollador

Recursos relacionados

- Herramienta de conversión de esquemas de AWS
- Amazon RDS
- Características de Amazon Aurora
- SERIALLY_REUTILIZABLE Pragma

Información adicional

```
Source Oracle Code:

CREATE OR REPLACE PACKAGE test_pkg_var
IS
PRAGMA SERIALLY_REUSABLE;
PROCEDURE function_1
 (test_id number);
PROCEDURE function_2
 (test_id number
 );
END;

CREATE OR REPLACE PACKAGE BODY test_pkg_var
IS
PRAGMA SERIALLY_REUSABLE;
v_char VARCHAR2(20) := 'shared.airline';
v_num number := 123;

PROCEDURE function_1(test_id number)
IS
```

```
begin
dbms_output.put_line( 'v_char-'|| v_char);
dbms_output.put_line( 'v_num-'||v_num);
v_char:='test1';
function_2(0);
END;

PROCEDURE function_2(test_id number)
is
begin
dbms_output.put_line( 'v_char-'|| v_char);
dbms_output.put_line( 'v_num-'||v_num);
END;
END test_pkg_var;

Calling the above functions

set serveroutput on


EXEC test_pkg_var.function_1(1);


EXEC test_pkg_var.function_2(1);


Target Postgresql Code:


CREATE SCHEMA test_pkg_var;

CREATE OR REPLACE FUNCTION test_pkg_var.init(pg_serialize IN INTEGER DEFAULT 0)

RETURNS void
AS
$BODY$

DECLARE

BEGIN

if aws_oracle_ext.is_package_initialized( 'test_pkg_var' ) AND pg_serialize = 0

then
```

```
return;

end if;

PERFORM aws_oracle_ext.set_package_initialized( 'test_pkg_var' );

PERFORM aws_oracle_ext.set_package_variable( 'test_pkg_var', 'v_char',
 'shared.airline.basecurrency'::CHARACTER

VARYING(100));

PERFORM aws_oracle_ext.set_package_variable('test_pkg_var', 'v_num', 123::integer);

END;

$BODY$

LANGUAGE plpgsql;


CREATE OR REPLACE FUNCTION test_pkg_var.function_1(pg_serialize int default 1)

RETURNS void
AS

$BODY$
DECLARE

BEGIN

PERFORM test_pkg_var.init(pg_serialize);

raise notice 'v_char%',aws_oracle_ext.get_package_variable( 'test_pkg_var', 'v_char');

raise notice 'v_num%',aws_oracle_ext.get_package_variable( 'test_pkg_var', 'v_num');

PERFORM aws_oracle_ext.set_package_variable( 'test_pkg_var', 'v_char',
 'test1'::varchar);

PERFORM test_pkg_var.function_2(0);
END;

$BODY$
```

```
LANGUAGE plpgsql;


CREATE OR REPLACE FUNCTION test_pkg_var.function_2(IN pg_serialize integer default 1)

RETURNS void

AS

$BODY$

DECLARE

BEGIN

PERFORM test_pkg_var.init(pg_serialize);

raise notice 'v_char%',aws_oracle_ext.get_package_variable( 'test_pkg_var', 'v_char');

raise notice 'v_num%',aws_oracle_ext.get_package_variable( 'test_pkg_var', 'v_num');

END;
$BODY$
LANGUAGE plpgsql;


Calling the above functions

select test_pkg_var.function_1()

 select test_pkg_var.function_2()
```

Migre tablas externas de Oracle a Amazon Aurora compatible con PostgreSQL

Creado por anuradha chintha (AWS) y Rakesh Raghav (AWS)

Entorno: PoC o piloto	Origen: Oracle	Destino: Aurora PostgreSQL
Tipo R: renovar arquitectura	Carga de trabajo: código abierto	Tecnologías: migración; bases de datos; modernización
Servicios de AWS: AWS Identity and Access Management; AWS Lambda; Amazon S3; Amazon SNS; Amazon Aurora		

Resumen

Las tablas externas permiten a Oracle consultar los datos almacenados fuera de la base de datos en archivos planos. Puede usar el controlador ORACLE_LOADER para acceder a cualquier dato almacenado en cualquier formato que pueda cargar la utilidad SQL*Loader. No puede usar el Lenguaje de Manipulación de Datos (DML) en tablas externas, pero puede usar las tablas externas para operaciones de consulta, unión y clasificación.

Amazon Aurora compatible con PostgreSQL no proporciona una funcionalidad similar a las tablas externas de Oracle. En su lugar, debe adoptar la modernización para desarrollar una solución escalable que cumpla con los requisitos funcionales y sea eficiente.

Este patrón proporciona los pasos para migrar diferentes tipos de tablas externas de Oracle a la edición de Aurora compatible con PostgreSQL en la nube de Amazon Web Services (AWS) mediante la extensión `aws_s3`.

Recomendamos probar exhaustivamente esta solución antes de implementarla en un entorno de producción.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Interfaz de la línea de comandos de AWS (AWS CLI)
- Una instancia disponible de base de datos Aurora compatible con PostgreSQL.
- Una base de datos de Oracle en las instalaciones con una tabla externa
- API de pg.Client
- Archivos de datos

Limitaciones

- Este patrón no proporciona la funcionalidad necesaria para sustituir a las tablas externas de Oracle. Sin embargo, los pasos y el código de muestra se pueden mejorar aún más para lograr sus objetivos de modernización de la base de datos.
- Los archivos no deben contener el carácter que se emplea como delimitador en las funciones de exportación e importación de `aws_s3`.

Versiones de producto

- Para realizar la importación de Amazon S3 en RDS para PostgreSQL, la base de datos debe ejecutar la versión PostgreSQL 10.7 o superior.

Arquitectura

Pila de tecnología de origen

- Oracle

Arquitectura de origen

Pila de tecnología de destino

- Amazon Aurora compatible con PostgreSQL
- Amazon CloudWatch
- AWS Lambda

- AWS Secrets Manager
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)

Arquitectura de destino

En el siguiente diagrama se muestra una representación de alto nivel de la solución.

1. Los archivos se cargan en el bucket de S3.
2. Se inicia la función de Lambda.
3. La función de Lambda inicia la llamada a la función de base de datos.
4. Secrets Manager proporciona las credenciales para acceder a la base de datos.
5. Según la función de la base de datos, se crea una alarma de SNS.

Automatizar y escalar

Cualquier adición o cambio en las tablas externas se puede gestionar mediante el mantenimiento de los metadatos.

Herramientas

- Amazon Aurora compatible con PostgreSQL: la edición de Amazon Aurora compatible con PostgreSQL es un motor de bases de datos relacionales, completamente administrado, compatible con PostgreSQL y conforme a ACID, que combina la velocidad y la fiabilidad de las bases de datos comerciales de tecnología avanzada con la rentabilidad de las bases de datos de código abierto.
- AWS CLI: la Interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta unificada para administrar los servicios de AWS. Solo tendrá que descargar y configurar una única herramienta para poder controlar varios servicios de AWS desde la línea de comando y automatizarlos mediante secuencias de comandos.
- Amazon CloudWatch: Amazon CloudWatch supervisa los recursos y la utilización de Amazon S3.
- AWS Lambda: AWS Lambda es un servicio de computación sin servidor que permite ejecutar código sin aprovisionar ni administrar servidores, crear una lógica de escalado de clústeres adaptada a las cargas de trabajo, mantener las integraciones de eventos o gestionar los tiempos

de ejecución. En este patrón, Lambda ejecuta la función de base de datos cada vez que se carga un archivo en Amazon S3.

- AWS Secrets Manager: AWS Secrets Manager es un servicio de almacenamiento y recuperación de credenciales. Con Secrets Manager puede reemplazar las credenciales codificadas en el código, incluidas las contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) proporciona una capa de almacenamiento que permite recibir y almacenar archivos para su consumo y transmisión hacia y desde el clúster de Aurora compatible con PostgreSQL.
- aws_s3: la extensión `aws_s3` integra Amazon S3 y Aurora compatible con PostgreSQL.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) coordina y administra la entrega o el envío de mensajes entre publicadores y clientes. En este patrón, Amazon SNS se usa para enviar notificaciones.

Código

Siempre que se ubique un archivo en el bucket de S3, se debe crear una función de base de datos a la que llamar desde la aplicación de procesamiento o la función de Lambda. Para obtener más información, consulte el código (adjunto).

Epics

Cree un archivo externo

Tarea	Descripción	Habilidades requeridas
Añada un archivo externo a la base de datos de origen.	Cree un archivo externo y trasládelo al directorio `oracle`.	Administrador de base de datos

Configure el objetivo (Aurora compatible con PostgreSQL)

Tarea	Descripción	Habilidades requeridas
Cree una base de datos de Aurora PostgreSQL.	Cree una instancia de base de datos en su clúster de	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Amazon Aurora compatible con PostgreSQL.	
Cree un esquema, una extensión aws_s3 y tablas.	Use el código que aparece en la sección `ext_tbl_scripts` de Información adicional. Las tablas incluyen tablas reales, tablas de ensayo, tablas de errores y registros y una metatabla.	Administrador de base de datos, desarrollador
Cree la función de base de datos.	Para crear la función de base de datos, use el código que aparece bajo la función `load_external_table_latest` en la sección de Información adicional.	Administrador de base de datos, desarrollador

Creación y configuración de la función de Lambda

Tarea	Descripción	Habilidades requeridas
Crear un rol.	Cree un rol con permisos para acceder a Amazon S3 y a Amazon Relational Database Service (Amazon RDS). Esta función se asignará a Lambda para ejecutar el patrón.	Administrador de base de datos
Crear la función de Lambda.	Cree una función de Lambda que lea el nombre del archivo de Amazon S3 (por ejemplo, `file_key = info.get('object', {}).get('key') )` y llame	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	a la función de base de datos (por ejemplo, `curs.callproc("load_external_tables", [file_key])`) con el nombre del archivo como parámetro de entrada. Según el resultado de la llamada a la función, se iniciará una notificación de SNS (por ejemplo, `client.publish(TopicArn='arn:',Message='fileloadsuccess',Subject='fileloadsuccess')`). En función de las necesidades de su empresa, puede crear una función de Lambda con código adicional si es necesario. Para más información, consulte la documentación de Lambda.	
Configure un desencadenante de eventos en el bucket de S3.	Configure un mecanismo para llamar a la función de Lambda en todos los eventos de creación de objetos en el bucket de S3.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Creación de un secreto.	Cree un nombre secreto para las credenciales de la base de datos mediante Secrets Manager. Pase el secreto a la función de Lambda.	Administrador de base de datos
Cargue los archivos de soporte de Lambda.	Cargue un archivo .zip que contenga los paquetes de soporte de Lambda y el script de Python adjunto para conectar a Aurora compatibl e con PostgreSQL. El código Python llamará a la función que creó en la base de datos.	Administrador de base de datos
Cree un tema de SNS.	Cree un tema de SNS para enviar un correo si la carga de datos se ha realizado correctamente o no.	Administrador de base de datos

Añadir integración con Amazon S3

Tarea	Descripción	Habilidades requeridas
Crear un bucket de S3.	En la consola de Amazon S3, cree un bucket de S3 con un nombre único que no contenga barras diagonale s en el inicio. Un nombre de bucket S3 es globalmente único y todas las cuentas de AWS comparten el espacio de nombres.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Crear políticas de IAM .	Para crear las políticas de AWS Identity and Access Management (IAM), use el código que se describe en la sección `s3bucketpolicy_for_import` de Información adicional.	Administrador de base de datos
Crear roles.	Cree dos roles para Aurora compatible con PostgreSQL, uno para Importar y otro para Exportar. Asigne las políticas correspondientes a los roles.	Administrador de base de datos
Adjunte los roles al clúster de Aurora compatible con PostgreSQL.	En Administrar roles, adjunte los roles de Importar y Exportar al clúster de Aurora PostgreSQL.	Administrador de base de datos
Cree objetos de apoyo para Aurora compatible con PostgreSQL.	Para las tablas de scripts, utilice el código de `ext_tbl_scripts` en la sección Información adicional. Para la función personalizada, utilice el código de `load_external_Table_latest` en la sección Información adicional.	Administrador de base de datos

Procese un archivo de prueba

Tarea	Descripción	Habilidades requeridas
Cargar un archivo en el bucket de S3.	Para cargar un archivo de prueba en el bucket de S3, use la consola o ejecute el siguiente comando en la CLI de AWS. `aws s3 cp /Users/Desktop/ukpost/exttbl/"testing files"/aps s3://s3importtest/inputext/aps` En cuanto se carga el archivo, el evento de bucket inicia la función de Lambda, que ejecuta la función Aurora compatible con PostgreSQL.	Administrador de base de datos
Compruebe los datos y los archivos de registro y error.	La función de Aurora compatible con PostgreSQL carga los archivos en la tabla principal y crea los archivos `.log` y `.bad` en el bucket de S3.	Administrador de base de datos
Supervise la solución.	En la CloudWatch consola de Amazon, supervise la función Lambda.	Administrador de base de datos

Recursos relacionados

- Integración de Amazon S3
- Amazon S3

- Trabajar con la versión de Amazon Aurora compatible con PostgreSQL
- AWS Lambda
- Amazon CloudWatch
- AWS Secrets Manager
- Configuración de notificaciones de Amazon SNS

Información adicional

ext_table_scripts

```
CREATE EXTENSION aws_s3 CASCADE;
CREATE TABLE IF NOT EXISTS meta_EXTERNAL_TABLE
(
    table_name_stg character varying(100) ,
    table_name character varying(100)  ,
    col_list character varying(1000)  ,
    data_type character varying(100)  ,
    col_order numeric,
    start_pos numeric,
    end_pos numeric,
    no_position character varying(100)  ,
    date_mask character varying(100)  ,
    delimeter character(1)  ,
    directory character varying(100)  ,
    file_name character varying(100)  ,
    header_exist character varying(5)
);
CREATE TABLE IF NOT EXISTS ext_tbl_stg
(
    col1 text
);
CREATE TABLE IF NOT EXISTS error_table
(
    error_details text,
    file_name character varying(100),
    processed_time timestamp without time zone
);
CREATE TABLE IF NOT EXISTS log_table
(
    file_name character varying(50) COLLATE pg_catalog."default",
    processed_date timestamp without time zone,
```

```
    tot_rec_count numeric,
    proc_rec_count numeric,
    error_rec_count numeric
);
sample insert scripts of meta data:
INSERT INTO meta_EXTERNAL_TABLE (table_name_stg, table_name, col_list, data_type,
 col_order, start_pos, end_pos, no_position, date_mask, delimeter, directory,
 file_name, header_exist) VALUES ('F_EX_APS_TRANSACTIONS_STG', 'F_EX_APS_TRANSACTIONS',
 'source_filename', 'character varying', 2, 8, 27, NULL, NULL, NULL, 'databasedev',
 'externalinterface/loaddir/APS', 'NO');
INSERT INTO meta_EXTERNAL_TABLE (table_name_stg, table_name, col_list, data_type,
 col_order, start_pos, end_pos, no_position, date_mask, delimeter, directory,
 file_name, header_exist) VALUES ('F_EX_APS_TRANSACTIONS_STG', 'F_EX_APS_TRANSACTIONS',
 'record_type_identifier', 'character varying', 3, 28, 30, NULL, NULL, NULL,
 'databasedev', 'externalinterface/loaddir/APS', 'NO');
INSERT INTO meta_EXTERNAL_TABLE (table_name_stg, table_name, col_list, data_type,
 col_order, start_pos, end_pos, no_position, date_mask, delimeter, directory,
 file_name, header_exist) VALUES ('F_EX_APS_TRANSACTIONS_STG', 'F_EX_APS_TRANSACTIONS',
 'fad_code', 'numeric', 4, 31, 36, NULL, NULL, NULL, 'databasedev', 'externalinterface/
loaddir/APS', 'NO');
INSERT INTO meta_EXTERNAL_TABLE (table_name_stg, table_name, col_list, data_type,
 col_order, start_pos, end_pos, no_position, date_mask, delimeter, directory,
 file_name, header_exist) VALUES ('F_EX_APS_TRANSACTIONS_STG', 'F_EX_APS_TRANSACTIONS',
 'session_sequence_number', 'numeric', 5, 37, 42, NULL, NULL, NULL, 'databasedev',
 'externalinterface/loaddir/APS', 'NO');
INSERT INTO meta_EXTERNAL_TABLE (table_name_stg, table_name, col_list, data_type,
 col_order, start_pos, end_pos, no_position, date_mask, delimeter, directory,
 file_name, header_exist) VALUES ('F_EX_APS_TRANSACTIONS_STG', 'F_EX_APS_TRANSACTIONS',
 'transaction_sequence_number', 'numeric', 6, 43, 48, NULL, NULL, NULL, 'databasedev',
 'externalinterface/loaddir/APS', 'NO');
```

s3bucketpolicy_for import

```
---Import role policy
--Create an IAM policy to allow, Get,  and list actions on S3 bucket
 {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "s3import",
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
```

```
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::s3importtest",
                "arn:aws:s3:::s3importtest/*"
            ]
        }
    ]
}
--Export Role policy
--Create an IAM policy to allow, put,  and list actions on S3 bucket
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "s3export",
            "Action": [
                "S3:PutObject",
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::s3importtest/*"
            ]
        }
    ]
}
```

Ejemplo de función de base de datos load_external_tables_latest

```
CREATE OR REPLACE FUNCTION public.load_external_tables(pi_filename text)
 RETURNS character varying
 LANGUAGE plpgsql
AS $function$
/* Loading data from S3 bucket into a APG table */
DECLARE
 v_final_sql TEXT;
 pi_ext_table TEXT;
 r refCURSOR;
 v_sqlerrm text;
 v_chunk numeric;
 i integer;
 v_col_list TEXT;
```

```
v_postion_list CHARACTER VARYING(1000);
v_len  integer;
v_delim varchar;
v_file_name CHARACTER VARYING(1000);
v_directory CHARACTER VARYING(1000);
v_table_name_stg CHARACTER VARYING(1000);
v_sql_col TEXT;
v_sql TEXT;
v_sql1 TEXT;
v_sql2 TEXT;
v_sql3 TEXT;
v_cnt integer;
v_sql_dynamic TEXT;
v_sql_ins TEXT;
proc_rec_COUNT integer;
error_rec_COUNT integer;
tot_rec_COUNT integer;
v_rec_val integer;
rec record;
v_col_cnt integer;
kv record;
v_val text;
v_header text;
j integer;
ERCODE VARCHAR(5);
v_region text;
cr CURSOR FOR
SELECT distinct DELIMETER,
  FILE_NAME,
  DIRECTORY
FROM  meta_EXTERNAL_TABLE
WHERE table_name = pi_ext_table
  AND DELIMETER IS NOT NULL;


cr1 CURSOR FOR
  SELECT   col_list,
  data_type,
  start_pos,
  END_pos,
  concat_ws('',' ',TABLE_NAME_STG) as TABLE_NAME_STG,
  no_position,date_mask
FROM  meta_EXTERNAL_TABLE
WHERE table_name = pi_ext_table
```

```
 order by col_order asc;
cr2 cursor FOR
SELECT  distinct table_name,table_name_stg
   FROM  meta_EXTERNAL_TABLE
   WHERE upper(file_name) = upper(pi_filename);


BEGIN
 -- PERFORM utl_file_utility.init();
   v_region := 'us-east-1';
   /* find tab details from file name */


   --DELETE FROM  ERROR_TABLE WHERE file_name= pi_filename;
  -- DELETE FROM  log_table WHERE file_name= pi_filename;


 BEGIN


   SELECT distinct table_name,table_name_stg INTO strict pi_ext_table,v_table_name_stg
   FROM  meta_EXTERNAL_TABLE
   WHERE upper(file_name) = upper(pi_filename);
 EXCEPTION
   WHEN NO_DATA_FOUND THEN
    raise notice 'error 1,%',sqlerrm;
    pi_ext_table := null;
    v_table_name_stg := null;
      RAISE USING errcode = 'NTFIP' ;
    when others then
        raise notice 'error others,%',sqlerrm;
 END;
 j :=1 ;

for rec in  cr2
 LOOP




  pi_ext_table     := rec.table_name;
  v_table_name_stg := rec.table_name_stg;
  v_col_list := null;
```

```
IF pi_ext_table IS NOT NULL
 THEN
   --EXECUTE concat_ws('','truncate table  ' ,pi_ext_table) ;
  EXECUTE concat_ws('','truncate table  ' ,v_table_name_stg) ;




      SELECT distinct DELIMETER INTO STRICT v_delim
      FROM  meta_EXTERNAL_TABLE
      WHERE table_name = pi_ext_table;


      IF v_delim IS NOT NULL THEN
    SELECT distinct DELIMETER,
      FILE_NAME,
      DIRECTORY ,
      concat_ws('',' ',table_name_stg),
      case  header_exist when 'YES' then 'CSV HEADER' else 'CSV' end as header_exist
    INTO STRICT v_delim,v_file_name,v_directory,v_table_name_stg,v_header
    FROM  meta_EXTERNAL_TABLE
    WHERE table_name = pi_ext_table
      AND DELIMETER IS NOT NULL;


    IF    upper(v_delim) = 'CSV'
    THEN
      v_sql := concat_ws('','SELECT aws_s3.table_import_FROM_s3 ( ''',
      v_table_name_stg,''','''',
      ''DELIMITER '''','''' CSV HEADER QUOTE '''''''''''', aws_commons.create_s3_uri
( ''',
      v_directory,''','''',v_file_name,''', ''',v_region,'''))');
      ELSE
      v_sql := concat_ws('','SELECT aws_s3.table_import_FROM_s3(''',
          v_table_name_stg, ''','''', ''DELIMITER AS ''''^''''',''',','
         aws_commons.create_s3_uri
          ( ''',v_directory, ''','''',
          v_file_name, ''',',
           '''',v_region,''')
         )');
         raise notice 'v_sql , %',v_sql;
      begin
       EXECUTE  v_sql;
```

```
      EXCEPTION
        WHEN OTHERS THEN
          raise notice 'error 1';
        RAISE USING errcode = 'S3IMP' ;
      END;


      select count(col_list) INTO v_col_cnt
      from  meta_EXTERNAL_TABLE where table_name = pi_ext_table;







       -- raise notice 'v_sql 2, %',concat_ws('','update ',v_table_name_stg, ' set
col1 = col1||''',v_delim,''''');


      execute concat_ws('','update ',v_table_name_stg, ' set col1 =
col1||''',v_delim,''''');




      i :=1;
      FOR rec in cr1
      loop
      v_sql1 := concat_ws('',v_sql1,'split_part(col1,''',v_delim,''',', i,')',' as
',rec.col_list,',');
      v_sql2 := concat_ws('',v_sql2,rec.col_list,',');
  --    v_sql3 := concat_ws('',v_sql3,'rec.',rec.col_list,'::',rec.data_type,',');


      case
        WHEN upper(rec.data_type) = 'NUMERIC'
        THEN v_sql3 := concat_ws('',v_sql3,' case WHEN
length(trim(split_part(col1,''',v_delim,''',', i,'))) =0
               THEN null
                ELSE
                coalesce((trim(split_part(col1,''',v_delim,''',',
i,')))::NUMERIC,0)::',rec.data_type,' END as ',rec.col_list,',') ;
        WHEN UPPER(rec.data_type) = 'TIMESTAMP WITHOUT TIME ZONE' AND rec.date_mask =
'YYYYMMDD'
```

```
        THEN v_sql3 := concat_ws('',v_sql3,' case WHEN
length(trim(split_part(col1,''',v_delim,''',', i,'))) =0
               THEN null
                ELSE
                to_date(coalesce((trim(split_part(col1,''',v_delim,''',',
i,'))),''99990101''),''YYYYMMDD''):',rec.data_type,' END as ',rec.col_list,',');
        WHEN UPPER(rec.data_type) = 'TIMESTAMP WITHOUT TIME ZONE' AND rec.date_mask =
 'MM/DD/YYYY hh24:mi:ss'
        THEN v_sql3 := concat_ws('',v_sql3,' case WHEN
length(trim(split_part(col1,''',v_delim,''',', i,'))) =0
               THEN null
                ELSE
                to_date(coalesce((trim(split_part(col1,''',v_delim,''',',
i,'))),''01/01/9999 0024:00:00''),''MM/DD/YYYY hh24:mi:ss''):',rec.data_type,' END as
',rec.col_list,',');
         ELSE
       v_sql3 := concat_ws('',v_sql3,' case WHEN
length(trim(split_part(col1,''',v_delim,''',', i,'))) =0
               THEN null
                ELSE
                 coalesce((trim(split_part(col1,''',v_delim,''',',
i,'))),''''):',rec.data_type,' END as ',rec.col_list,',') ;
      END case;


      i :=i+1;
      end loop;


        -- raise notice 'v_sql 3, %',v_sql3;


      SELECT trim(trailing ' ' FROM v_sql1) INTO v_sql1;
      SELECT trim(trailing ',' FROM v_sql1) INTO v_sql1;


      SELECT trim(trailing ' ' FROM v_sql2) INTO v_sql2;
      SELECT trim(trailing ',' FROM v_sql2) INTO v_sql2;


      SELECT trim(trailing ' ' FROM v_sql3) INTO v_sql3;
      SELECT trim(trailing ',' FROM v_sql3) INTO v_sql3;
```

```
       END IF;
      raise notice 'v_delim , %',v_delim;


     EXECUTE concat_ws('','SELECT COUNT(*) FROM ',v_table_name_stg)  INTO v_cnt;


    raise notice 'stg cnt , %',v_cnt;


    /* if upper(v_delim) = 'CSV' then
       v_sql_ins := concat_ws('', ' SELECT * from ' ,v_table_name_stg );
     else
      -- v_sql_ins := concat_ws('',' SELECT ',v_sql1,'  from (select col1 from
 ' ,v_table_name_stg , ')sub ');
       v_sql_ins := concat_ws('',' SELECT ',v_sql3,'  from (select col1 from
 ' ,v_table_name_stg , ')sub ');
       END IF;*/


v_chunk := v_cnt/100;




for i in 1..101
loop
     BEGIN
    -- raise notice 'v_sql , %',v_sql;
       -- raise notice 'Chunk number , %',i;
       v_sql_ins := concat_ws('',' SELECT ',v_sql3,'  from (select col1 from
 ' ,v_table_name_stg , ' offset ',v_chunk*(i-1), ' limit ',v_chunk,') sub ');


     v_sql := concat_ws('','insert into  ', pi_ext_table ,' ', v_sql_ins);
     -- raise notice 'select statement , %',v_sql_ins;
          -- v_sql := null;
     -- EXECUTE concat_ws('','insert into  ', pi_ext_table ,' ', v_sql_ins, 'offset
 ',v_chunk*(i-1), ' limit ',v_chunk );
     --v_sql := concat_ws('','insert into  ', pi_ext_table ,' ', v_sql_ins );


     -- raise notice 'insert statement , %',v_sql;
```

```
   raise NOTICE 'CHUNK START %',v_chunk*(i-1);
  raise NOTICE 'CHUNK END %',v_chunk;


    EXECUTE v_sql;


 EXCEPTION
      WHEN OTHERS THEN
      -- v_sql_ins := concat_ws('',' SELECT ',v_sql1, '  from (select col1 from
' ,v_table_name_stg , ' )sub ');
        -- raise notice 'Chunk number for cursor , %',i;


   raise NOTICE 'Cursor - CHUNK START %',v_chunk*(i-1);
  raise NOTICE 'Cursor -  CHUNK END %',v_chunk;
        v_sql_ins := concat_ws('',' SELECT ',v_sql3, '  from (select col1 from
' ,v_table_name_stg , ' )sub ');


        v_final_sql := REPLACE (v_sql_ins, ''''::text, ''''''::text);
       -- raise notice 'v_final_sql %',v_final_sql;
        v_sql :=concat_ws('','do $a$ declare  r refcursor;v_sql text; i
numeric;v_conname text;  v_typ  ',pi_ext_table,'[]; v_rec  ','record',';
          begin







          open r for execute ''select col1 from ',v_table_name_stg ,'  offset
',v_chunk*(i-1), ' limit ',v_chunk,''';
          loop
          begin
          fetch r into v_rec;
          EXIT WHEN NOT FOUND;
```

```
          v_sql := concat_ws('''','insert into  ',pi_ext_table,' SELECT ',REPLACE
 (v_sql3, '''::text, ''''''::text) , '  from ( select ''''''',v_rec.col1,''''''' as
 col1) v'');
           execute v_sql;


          exception
           when others then
         v_sql := ''INSERT INTO  ERROR_TABLE VALUES (concat_ws(''''''''','''Error
 Name: ''''',$$''||SQLERRM||''$$,''''Error State: ''''',''''''||
SQLSTATE||''''''','''record : ''''',$$''||v_rec.col1||''$$),'''''||
pi_filename||''''',now())'';


             execute v_sql;
            continue;
          end ;
          end loop;
          close r;
          exception
          when others then
        raise;
          end ; $a$');
     -- raise notice ' inside excp v_sql %',v_sql;
         execute v_sql;
     --  raise notice 'v_sql %',v_sql;
       END;
  END LOOP;
     ELSE


     SELECT distinct DELIMETER,FILE_NAME,DIRECTORY ,concat_ws('',' ',table_name_stg),
       case  header_exist when 'YES' then 'CSV HEADER' else 'CSV' end as header_exist
       INTO STRICT v_delim,v_file_name,v_directory,v_table_name_stg,v_header
     FROM  meta_EXTERNAL_TABLE
     WHERE table_name = pi_ext_table                  ;
     v_sql := concat_ws('','SELECT aws_s3.table_import_FROM_s3(''',
       v_table_name_stg, ''','''', ''DELIMITER AS ''''#'''' ',v_header,' '','','
      aws_commons.create_s3_uri
       ( ''',v_directory, ''','''',
       v_file_name, ''',',
        '''',v_region,''')
      )');
         EXECUTE  v_sql;
```

```
    FOR rec in cr1
    LOOP


     IF rec.start_pos IS NULL AND rec.END_pos IS NULL AND rec.no_position = 'recnum'
     THEN
       v_rec_val := 1;
     ELSE


      case
        WHEN upper(rec.data_type) = 'NUMERIC'
        THEN v_sql1 := concat_ws('',' case WHEN length(trim(substring(COL1,
',rec.start_pos ,',', rec.END_pos,'-',rec.start_pos ,'+1))) =0
               THEN null
                ELSE
                coalesce((trim(substring(COL1, ',rec.start_pos ,',',
rec.END_pos,'-',rec.start_pos ,'+1)))::NUMERIC,0)::',rec.data_type,' END as
',rec.col_list,',') ;
        WHEN UPPER(rec.data_type) = 'TIMESTAMP WITHOUT TIME ZONE' AND rec.date_mask =
'YYYYMMDD'
        THEN v_sql1 := concat_ws('','case WHEN length(trim(substring(COL1,
',rec.start_pos ,',', rec.END_pos,'-',rec.start_pos ,'+1))) =0
               THEN null
                ELSE
                to_date(coalesce((trim(substring(COL1, ',rec.start_pos ,',',
rec.END_pos,'-',rec.start_pos ,'+1))),''99990101''),''YYYYMMDD''):',rec.data_type,'
END as ',rec.col_list,',');
        WHEN UPPER(rec.data_type) = 'TIMESTAMP WITHOUT TIME ZONE' AND rec.date_mask =
'YYYYMMDDHH24MISS'
        THEN v_sql1 := concat_ws('','case WHEN length(trim(substring(COL1,
',rec.start_pos ,',', rec.END_pos,'-',rec.start_pos ,'+1))) =0
               THEN null
                ELSE
                to_date(coalesce((trim(substring(COL1, ',rec.start_pos ,',',
rec.END_pos,'-',rec.start_pos ,'+1))),''9999010100240000''),''YYYYMMDDHH24MISS''):',rec.data_
END as ',rec.col_list,',');
         ELSE
       v_sql1 := concat_ws('',' case WHEN length(trim(substring(COL1,
',rec.start_pos ,',', rec.END_pos,'-',rec.start_pos ,'+1))) =0
               THEN null
                ELSE
```

```
                coalesce((trim(substring(COL1, ',rec.start_pos ,',',
rec.END_pos,'-',rec.start_pos ,'+1))),''''):::',rec.data_type,' END as
',rec.col_list,',') ;
      END case;


     END IF;
     v_col_list := concat_ws('',v_col_list ,v_sql1);
    END LOOP;




          SELECT trim(trailing ' ' FROM v_col_list) INTO v_col_list;
          SELECT trim(trailing ',' FROM v_col_list) INTO v_col_list;


          v_sql_col   :=  concat_ws('',trim(trailing ',' FROM v_col_list) , ' FROM
 ',v_table_name_stg,' WHERE col1 IS NOT NULL AND length(col1)>0 ');




          v_sql_dynamic := v_sql_col;


          EXECUTE  concat_ws('','SELECT COUNT(*) FROM ',v_table_name_stg) INTO v_cnt;




        IF v_rec_val = 1 THEN
            v_sql_ins := concat_ws('',' select row_number() over(order by ctid) as
line_number ,' ,v_sql_dynamic) ;


        ELSE
              v_sql_ins := concat_ws('',' SELECT' ,v_sql_dynamic) ;
          END IF;


    BEGIN
      EXECUTE concat_ws('','insert into  ', pi_ext_table ,' ', v_sql_ins);
          EXCEPTION
```

```
             WHEN OTHERS THEN
         IF v_rec_val = 1 THEN
                v_final_sql := ' select row_number() over(order by ctid) as
line_number ,col1 from ';
              ELSE
               v_final_sql := ' SELECT col1 from';
             END IF;
      v_sql :=concat_ws('','do $a$ declare  r refcursor;v_rec_val numeric :=
',coalesce(v_rec_val,0),';line_number numeric; col1 text; v_typ  ',pi_ext_table,'[];
v_rec  ',pi_ext_table,';
            begin
            open r for execute ''',v_final_sql, ' ',v_table_name_stg,' WHERE col1 IS
NOT NULL AND length(col1)>0 '' ;
            loop
            begin
            if   v_rec_val = 1 then
            fetch r into line_number,col1;
            else
            fetch r into col1;
            end if;


            EXIT WHEN NOT FOUND;
             if v_rec_val = 1 then
             select line_number,',trim(trailing ',' FROM v_col_list) ,' into v_rec;
             else
               select ',trim(trailing ',' FROM v_col_list) ,' into v_rec;
             end if;


            insert into  ',pi_ext_table,' select v_rec.*;
             exception
             when others then
              INSERT INTO  ERROR_TABLE VALUES (concat_ws('''',''Error Name:
'',SQLERRM,''Error State: '',SQLSTATE,''record : '',v_rec),''',pi_filename,''',now());
              continue;
             end ;
              end loop;
            close r;
             exception
             when others then
             raise;
             end ; $a$');
        execute v_sql;
```

```
    END;

        END IF;

  EXECUTE concat_ws('','SELECT COUNT(*) FROM  ' ,pi_ext_table)   INTO proc_rec_COUNT;

  EXECUTE concat_ws('','SELECT COUNT(*) FROM  error_table WHERE file_name
='''',pi_filename,''' and processed_time::date = clock_timestamp()::date')  INTO
error_rec_COUNT;

  EXECUTE concat_ws('','SELECT COUNT(*) FROM ',v_table_name_stg)   INTO tot_rec_COUNT;

  INSERT INTO  log_table values(pi_filename,now(),tot_rec_COUNT,proc_rec_COUNT,
error_rec_COUNT);

  raise notice 'v_directory, %',v_directory;

  raise notice 'pi_filename, %',pi_filename;

  raise notice 'v_region, %',v_region;

 perform aws_s3.query_export_to_s3('SELECT
replace(trim(substring(error_details,position(''('' in
error_details)+1),'')''),'','','';''),file_name,processed_time FROM  error_table WHERE
file_name = '''||pi_filename||'''',
  aws_commons.create_s3_uri(v_directory, pi_filename||'.bad', v_region),
  options :='FORmat csv, header, delimiter $$,$$'
  );

raise notice 'v_directory, %',v_directory;
```

```
   raise notice 'pi_filename, %',pi_filename;


   raise notice 'v_region, %',v_region;


  perform aws_s3.query_export_to_s3('SELECT * FROM  log_table WHERE file_name = '''||
pi_filename||'''',
   aws_commons.create_s3_uri(v_directory, pi_filename||'.log', v_region),
   options :='FORmat csv, header, delimiter $$,$$'
   );




   END IF;
 j := j+1;
 END LOOP;


       RETURN 'OK';
EXCEPTION
    WHEN  OTHERS THEN
  raise notice 'error %',sqlerrm;
   ERCODE=SQLSTATE;
   IF ERCODE = 'NTFIP' THEN
     v_sqlerrm := concat_Ws('',sqlerrm,'No data for the filename');
   ELSIF ERCODE = 'S3IMP' THEN
    v_sqlerrm := concat_Ws('',sqlerrm,'Error While exporting the file from S3');
   ELSE
      v_sqlerrm := sqlerrm;
   END IF;


 select distinct directory into v_directory from  meta_EXTERNAL_TABLE;




 raise notice 'exc v_directory, %',v_directory;


   raise notice 'exc pi_filename, %',pi_filename;
```

```
   raise notice 'exc v_region, %',v_region;


  perform aws_s3.query_export_to_s3('SELECT * FROM  error_table WHERE file_name = '''||
pi_filename||'''',
   aws_commons.create_s3_uri(v_directory, pi_filename||'.bad', v_region),
   options :='FORmat csv, header, delimiter $$,$$'
   );
    RETURN null;
END;
$function$
```

Migre índices basados en funciones de Oracle a PostgreSQL

Creado por Veeranjaneyulu Grandhi (AWS) y Navakanth Talluri (AWS)

Entorno: producción	Origen: Oracle	Destino: PostgreSQL
Tipo R: renovar arquitectura	Carga de trabajo: Oracle	Tecnologías: Migración; bases de datos

Resumen

Los índices son una forma común de mejorar el rendimiento de las bases de datos. Un índice permite al servidor de bases de datos encontrar y recuperar filas específicas mucho más rápido de lo que lo haría sin un índice. Sin embargo, los índices también añaden una sobrecarga al sistema de bases de datos en su conjunto, por lo que deben utilizarse con sensatez. Los índices basados en funciones, que se basan en una función o expresión, pueden incluir varias columnas y expresiones matemáticas. Un índice basado en funciones mejora el rendimiento de las consultas que utilizan la expresión de índice.

De forma nativa, PostgreSQL no admite la creación de índices basados en funciones mediante funciones cuya volatilidad se define como estable. Sin embargo, puede crear funciones similares con volatilidad `IMMUTABLE` y utilizarlas en la creación de índices.

Una función `IMMUTABLE` no puede modificar la base de datos y se garantiza que devolverá los mismos resultados con los mismos argumentos para siempre. Esta categoría permite al optimizador evaluar previamente la función cuando una consulta la llama con argumentos constantes.

Este patrón ayuda a migrar los índices basados en funciones de Oracle cuando se utilizan con funciones como `to_char`, `to_date` y `to_number` al equivalente de PostgreSQL.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de Amazon Web Services (AWS)
- Una instancia de base de datos de Oracle de origen con el servicio de escucha configurado y en ejecución

- Familiaridad con bases de datos PostgreSQL

Limitaciones

- El límite de tamaño de la base de datos es de 64 TB
- Las funciones utilizadas en la creación de índices deben ser INMUTABLES.

Versiones de producto

- Todas las ediciones de bases de datos Oracle para las versiones 11g (versiones 11.2.0.3.v1 y posteriores) y hasta 12.2, y 18c
- Versiones 9.6 y posteriores de PostgreSQL

Arquitectura

Pila de tecnología de origen

- Una base de datos Oracle en las instalaciones o en una instancia de Amazon Elastic Compute Cloud (Amazon EC2), o una instancia de base de datos de Amazon RDS para Oracle.

Pila de tecnología de destino

- Cualquier motor de PostgreSQL

Herramientas

- pgAdmin 4 es una herramienta de administración de código abierto para Postgres. La herramienta pgAdmin 4 proporciona una interfaz gráfica para crear, mantener y utilizar objetos de base de datos.
- Oracle SQL Developer es un entorno de desarrollo integrado (IDE) para desarrollar y gestionar bases de datos Oracle tanto en implementaciones tradicionales como en la nube.

Epics

Cree un índice basado en funciones mediante una función predeterminada

Tarea	Descripción	Habilidades requeridas
Cree un índice basado en funciones en una columna mediante la función to_char.	Utilice el siguiente código para crear el índice basado en funciones. `postgres=# create table funcindex( col1 timestamp without time zone);` `CREATE TABLE` `postgres=# insert into funcindex values (now());` `INSERT 0 1` `postgres=# select * from funcindex;` `col1` `----------` `2022-08-09 16:00:57.77414` `(1 rows)` `postgres=# create index funcindex_idx on funcindex(to_char(col1,'DD-MM-YYYY HH24:MI:SS'));` `ERROR: functions in index expression must be marked IMMUTABLE` Nota: PostgreSQL no permite crear un índice basado en	Administrador de base de datos, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	funciones sin la cláusula `IMMUTABLE` .	
Compruebe la volatilidad de la función.	Para comprobar la volatilidad de la función, utilice el código de la sección Información adicional.	Administrador de base de datos

Crear índices basados en funciones utilizando una función envolvente

Tarea	Descripción	Habilidades requeridas
Cree una función de encapsulación.	Para crear una función de encapsulación, utilice el código de la sección de información adicional.	Desarrollador de PostgreSQL
Cree un índice mediante la función de encapsulación.	Utilice el código de la sección Información adicional para crear una función definida por el usuario con la palabra clave `IMMUTABLE` en el mismo esquema que la aplicación y consúltela en el script de creación de índices. Si se crea una función definida por el usuario en un esquema común (del ejemplo anterior), actualice `search_path` tal como se muestra. `ALTER ROLE <ROLENAME>` `set search_path=$user,` `COMMON;`	Administrador de base de datos, desarrollador de PostgreSQL

Validar creación del índice

Tarea	Descripción	Habilidades requeridas
Valide la creación del índice.	Valide que es necesario crear el índice en función de los patrones de acceso a las consultas.	Administrador de base de datos
Valide que se pueda utilizar el índice.	Para comprobar si el optimizador de PostgreSQL recoge el índice basado en funciones, ejecute una instrucción SQL mediante explain o explain analyze. Utilice el código de la sección Información adicional. Si es posible, recopile también las estadísticas de la tabla. Nota: si observa el plan de explicación, el optimizador de PostgreSQL ha elegido un índice basado en funciones debido a la condición de predicado.	Administrador de base de datos

Recursos relacionados

- Índices basados en funciones (documentación de Oracle)
- Índices de expresiones (documentación de PostgreSQL)
- Volatilidad de PostgreSQL (documentación de PostgreSQL)
- PostgreSQL search_path (documentación de PostgreSQL)
- Manual de migración de Oracle Database 19c a Amazon Aurora PostgreSQL

Información adicional

Crear una función de encapsulación

```
CREATE OR REPLACE FUNCTION myschema.to_char(var1 timestamp without time zone, var2
 varchar) RETURNS varchar AS $BODY$ select to_char(var1, 'YYYYMMDD'); $BODY$ LANGUAGE
 sql IMMUTABLE;
```

Crear un índice mediante la función de encapsulación

```
postgres=# create function common.to_char(var1 timestamp without time zone, var2
 varchar) RETURNS varchar AS $BODY$ select to_char(var1, 'YYYYMMDD'); $BODY$ LANGUAGE
 sql IMMUTABLE;
CREATE FUNCTION
postgres=# create index funcindex_idx on funcindex(common.to_char(col1,'DD-MM-YYYY
 HH24:MI:SS'));
CREATE INDEX
```

Comprobar la volatilidad de la función

```
SELECT DISTINCT p.proname as "Name",p.provolatile as "volatility" FROM
 pg_catalog.pg_proc p
 LEFT JOIN pg_catalog.pg_namespace n ON n.oid = p.pronamespace
 LEFT JOIN pg_catalog.pg_language l ON l.oid = p.prolang
 WHERE n.nspname OPERATOR(pg_catalog.~) '^(pg_catalog)$' COLLATE pg_catalog.default AND
 p.proname='to_char'GROUP BY p.proname,p.provolatile
ORDER BY 1;
```

Validar que se pueda utilizar el índice

```
explain analyze <SQL>


postgres=# explain select col1 from funcindex where common.to_char(col1,'DD-MM-YYYY
 HH24:MI:SS') = '09-08-2022 16:00:57';
                                                        QUERY PLAN
-------------------------------------------------------------------------------------------
 Index Scan using funcindex_idx on funcindex  (cost=0.42..8.44 rows=1 width=8)
   Index Cond: ((common.to_char(col1, 'DD-MM-YYYY HH24:MI:SS'::character
 varying))::text = '09-08-2022 16:00:57'::text)
(2 rows)
```

Migrar las funciones nativas de Oracle a PostgreSQL mediante extensiones

Documento creado por Pinesh Singal (AWS)

Entorno: PoC o piloto	Origen: bases de datos: relacionales	Destino: Amazon RDS PostgreSQL
Tipo R: renovar arquitectura	Carga de trabajo: Oracle; código abierto	Tecnologías: migración; bases de datos
Servicios de AWS: Amazon EC2; Amazon RDS		

Resumen

Este patrón de migración proporciona step-by-step orientación para migrar una base de datos de Amazon Relational Database Service (Amazon RDS) para Oracle a una base de datos de Amazon RDS for PostgreSQL o Amazon Aurora PostgreSQL Edition compatible con PostgreSQL mediante la modificación y las extensiones del código integrado nativo de PostgreSQL (). `aws_oracle_ext` `orafce` `psql` Esto ahorrará tiempo de procesamiento.

El patrón describe una estrategia de migración manual fuera de línea sin tiempo de inactividad para una base de datos de origen Oracle de varios terabytes con un elevado número de transacciones.

El proceso de migración utiliza la herramienta de conversión de esquemas de AWS (AWS SCT) con las extensiones `aws_oracle_ext` y `orafce` para convertir un esquema de base de datos de Amazon RDS para Oracle en un esquema de base de datos compatible con Amazon RDS para PostgreSQL o Aurora PostgreSQL. Luego, el código se cambia manualmente al código integrado de `psql` nativo compatible con PostgreSQL. Esto se debe a que las llamadas a la extensión afectan al procesamiento del código en el servidor de bases de datos PostgreSQL y no todo el código de la extensión es totalmente compatible o compatible con el código PostgreSQL.

Este patrón se centra principalmente en la migración manual de códigos SQL mediante AWS SCT y las extensiones `aws_oracle_ext` y. `orafce` Las extensiones que ya se utilizan se convierten en elementos integrados (`psql`) nativos de PostgreSQL. A continuación, se eliminan todas las referencias a las extensiones y se convierten los códigos en consecuencia.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Sistema operativo (Windows o Mac) o instancia Amazon EC2 (en funcionamiento)
- Orafce

Limitaciones

No todas las funciones de Oracle que utilizan extensiones `aws_oracle_ext` o `orafce` se pueden convertir en funciones nativas de PostgreSQL. Es posible que necesite una revisión manual para poder compilarlo con las bibliotecas de PostgreSQL.

Un inconveniente del uso de extensiones SCT de AWS es su lento rendimiento a la hora de ejecutar y obtener los resultados. Su coste se puede entender a partir del simple plan EXPLAIN de PostgreSQL (plan de ejecución de una declaración) sobre la migración de la función `SYSDATE` Oracle a la función PostgreSQL `NOW()` entre los tres códigos (`aws_oracle_ext`, `orafce` y `psql` por defecto), como se explica en la sección de comprobación comparativa del rendimiento del documento adjunto.

Versiones de producto

- Origen: base de datos 10.2 y versiones posteriores de Amazon RDS para Oracle (para 10.x), 11g (11.2.0.3.v1 y versiones posteriores) y hasta 12.2, 18c y 19c (y versiones posteriores) para Enterprise Edition, Standard Edition, Standard Edition 1 y Standard Edition 2
- Destino: base de datos compatible con Amazon RDS para PostgreSQL o Aurora PostgreSQL 9.4 y versiones posteriores (para 9.x), 10.x, 11.x, 12.x, 13.x y 14.x (y versiones posteriores)
- AWS SCT: última versión (este patrón se probó con 1.0.632)
- Oracle: última versión (este patrón se probó con la versión 3.9.0)

Arquitectura

Pila de tecnología de origen

- Instancia de base de datos de Amazon RDS para Oracle con versión 12.1.0.2.v18

Pila de tecnología de destino

- Una instancia de base de datos compatible con Amazon RDS para PostgreSQL o Aurora PostgreSQL con la versión 11.5

Arquitectura de migración de bases de datos

El siguiente diagrama representa la arquitectura de migración de bases de datos entre las bases de datos Oracle de origen y PostgreSQL de destino. La arquitectura incluye la nube de AWS, una nube privada virtual (VPC), zonas de disponibilidad, una subred privada, una base de datos Amazon RDS para Oracle, AWS SCT, una base de datos Amazon RDS para PostgreSQL o Aurora compatible con PostgreSQL, extensiones para Oracle (`aws_oracle_ext` y `orafce`) y archivos de lenguaje de consulta estructurado (SQL).

1. Inicie la instancia de base de datos de Amazon RDS para Oracle (base de datos de origen).
2. Utilice AWS SCT con los `aws_oracle_ext` paquetes de `orafce` extensión para convertir el código fuente de Oracle a PostresQL.
3. La conversión produce archivos.sql migrados compatibles con PostgreSQL.
4. Convierta manualmente los códigos de extensión de Oracle no convertidos en códigos PostgreSQL (`psql`).
5. La conversión manual produce archivos.sql convertidos compatibles con PostgreSQL.
6. Ejecute estos archivos.sql en su instancia de base de datos de Amazon RDS para PostgreSQL (base de datos de destino).

Herramientas

Herramientas

Servicios de AWS

- AWS SCT: la herramienta de conversión de esquemas de AWS (AWS SCT) convierte el esquema de base de datos existente de un motor de base de datos a otro. Puede convertir un esquema de procesamiento de transacciones en línea (OLTP) relacional o un esquema de almacenamiento de datos. Su esquema convertido es adecuado para una instancia de base de datos de Amazon RDS para MySQL, un clúster de base de datos de Amazon Aurora, una instancia de base de datos de

Amazon RDS para PostgreSQL o un clúster de Amazon Redshift. El esquema convertido también se puede utilizar con una base de datos en una instancia de Amazon EC2 o almacenarse como datos en un bucket de Amazon S3.

AWS SCT proporciona una interfaz de usuario basada en proyectos para convertir automáticamente el esquema de la base de datos de origen a un formato compatible con su instancia de Amazon RDS de destino.

Puede usar AWS SCT para realizar la migración desde una base de datos de origen de Oracle a cualquiera de los destinos enumerados anteriormente. Con AWS SCT, puede exportar las definiciones de los objetos de la base de datos de origen, como el esquema, las vistas, los procedimientos almacenados y las funciones.

Puede utilizar AWS SCT para convertir datos de Oracle a Amazon RDS para PostgreSQL o Amazon Aurora PostgreSQL-Compatible Edition.

Este patrón utiliza AWS SCT para convertir y migrar el código de Oracle a PostgreSQL mediante las extensiones `aws_oracle_ext` y `orafce` migrar manualmente los códigos `psql` de extensión a código integrado nativo o predeterminado.

- El paquete de extensión de AWS SCT es un módulo complementario que simula funciones presentes en la base de datos de origen que son necesarias a la hora de convertir objetos a la base de datos de destino. Antes de poder instalar el paquete de extensión AWS SCT, debe convertir el esquema de su base de datos.

  Cuando convierte su base de datos o esquema de almacén de datos, AWS SCT agrega un esquema adicional a su base de datos de destino. Este esquema implementa las funciones del sistema SQL de la base de datos de origen que son necesarias al escribir su esquema convertido en la base de datos de destino. El esquema adicional se denomina esquema del paquete de extensión.

  El esquema del paquete de extensión para bases de datos OLTP se nombra según la base de datos de origen. Para las bases de datos de Oracle, el esquema del paquete de extensiones es `AWS_ORACLE_EXT`.

Otras herramientas

- Oracle: Orafce es un módulo que implementa funciones, tipos de datos y paquetes compatibles con Oracle. Es una herramienta de código abierto con una licencia de Berkeley Source Distribution

(BSD) para que cualquiera pueda usarla. El módulo `orafce` es útil para migrar de Oracle a PostgreSQL porque tiene muchas funciones de Oracle implementadas en PostgreSQL.

Código

Para obtener una lista de todos los códigos más utilizados y migrados de Oracle a PostgreSQL para evitar el uso del código de extensión SCT de AWS, consulte el documento adjunto.

Epics

Configuración de la base de datos de origen de Amazon RDS para Oracle

Tarea	Descripción	Habilidades requeridas
Cree la instancia de base de datos Oracle.	Cree una instancia de base de datos compatible con Amazon RDS para Oracle o Aurora PostgreSQL desde la consola de Amazon RDS.	AWS general, administrador de bases de datos
Configuración de los grupos de seguridad.	Configure grupos de seguridad entrantes y salientes.	AWS general
Crear la base de datos.	Crear la base de datos de Oracle con los usuarios y esquemas necesarios.	AWS general, administrador de bases de datos
Crear los objetos.	Crear objetos e introducir datos en el esquema.	Administrador de base de datos

Configuración de la base de datos de destino de Amazon RDS para PostgreSQL

Tarea	Descripción	Habilidades requeridas
Cree la instancia de base de datos PostgreSQL.	Cree una instancia de base de datos de Amazon RDS para	AWS general, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	PostgreSQL o de Amazon Aurora mediante la consola de Amazon RDS.	
Configuración de los grupos de seguridad.	Configure grupos de seguridad entrantes y salientes.	AWS general
Crear la base de datos.	Cree la base de datos PostgreSQL con los usuarios y esquemas necesarios.	AWS general, administrador de bases de datos
Valide las extensiones.	Asegúrese de que `aws_oracle_ext` y `orafce` están instalados y configura dos correctamente en la base de datos PostgreSQL.	Administrador de base de datos
Compruebe que la base de datos PostgreSQL esté disponible.	Asegúrese de que la base de datos PostgreSQL esté activa y en funcionamiento.	Administrador de base de datos

Migre el esquema de Oracle a PostgreSQL con AWS SCT y las extensiones

Tarea	Descripción	Habilidades requeridas
Instale AWS SCT.	Instale la versión más reciente de AWS SCT.	Administrador de base de datos
Configure AWS SCT.	Configure AWS SCT con los controladores de conectividad de bases de datos Java (JDBC) para Oracle (`ojdbc8.jar`) y PostgreSQ	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	L (`postgresql-42.2.5.jar`).	
Habilite el paquete o la plantilla de extensiones SCT de AWS.	En AWS SCT Configuración de proyecto, habilite la implementación de funciones integradas con las extensiones `aws_oracle_ext` y `orafce` para el esquema de base de datos de Oracle.	Administrador de base de datos
Convierta el esquema.	En AWS SCT, seleccione Convertir esquema para convertir el esquema de Oracle a PostgreSQL y generar los archivos.sql.	Administrador de base de datos

Convierta el código de extensión SCT de AWS en código psql

Tarea	Descripción	Habilidades requeridas
Convertir el código manualmente.	Convierta manualmente cada línea de código compatible con la extensión en código integrado predeterminado `psql`, como se detalla en el documento adjunto. Por ejemplo, cambie `AWS_ORACLE_EXT.SYSDATE()` a `ORACLE.SYSDATE()` o `NOW()`.	Administrador de base de datos
Valida el código	(Opcional) Valide cada línea de código ejecutándola	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	temporalmente en la base de datos PostgreSQL.	
Cree objetos en la base de datos PostgreSQL.	Para crear objetos en la base de datos de PostgreSQL, ejecute los archivos.sql generados por AWS SCT y modificados en los dos pasos anteriores.	Administrador de base de datos

Recursos relacionados

- Database
  - Oracle en Amazon RDS
  - PostgreSQL en Amazon RDS
  - Uso de Amazon Aurora PostgreSQL
  - Plan EXPLAIN de PostgreSQL
- AWS SCT
  - Descripción general de la herramienta Schema Conversion Tool de AWS
  - Guía del usuario de AWS SCT
  - Uso de la interfaz de usuario de la AWS SCT
  - Utilizar la base de datos de Oracle como origen para AWS SCT
- Extensiones para AWS SCT
  - Uso del paquete de extensión de AWS SCT
  - Funcionalidad de Oracle (en)
  - PGXN oracle
  - GitHub orace

Información adicional

Para obtener más información, siga los comandos detallados, con sintaxis y ejemplos, para convertir el código manualmente en el documento adjunto.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Migrar una base de datos de Db2 de Amazon EC2 a Aurora compatible con MySQL mediante AWS DMS

Documento creado por Pinesh Singal (AWS)

Entorno: PoC o piloto	Origen: IBM Db2 en Amazon EC2	Destino: edición de Amazon Aurora compatible con MySQL
Tipo R: renovar arquitectura	Carga de trabajo: IBM	Tecnologías: Migración; bases de datos
Servicios de AWS: AWS DMS; Amazon EC2; AWS SCT; Amazon Aurora		

Resumen

Tras migrar su Base de datos IBM Db2 para LUW a Amazon Elastic Compute Cloud (Amazon EC2), considere la posibilidad de rediseñar la base de datos pasando a una base de datos nativa en la nube de Amazon Web Services (AWS). Este patrón cubre la migración de una base de datos IBM Db2 para una base de datos LUW que se ejecuta en una instancia de Amazon EC2 a una base de datos de Edición de Amazon Aurora compatible con MySQL en AWS.

El patrón describe una estrategia de migración en línea con un tiempo de inactividad mínimo para una base de datos fuente de Db2 de varios terabytes con un número elevado de transacciones.

Este patrón utiliza la Herramienta de conversión de esquemas de AWS (AWS SCT) para convertir el esquema de la base de datos de Db2 en un esquema de Aurora compatible con MySQL. A continuación, el patrón utiliza AWS Database Migration Service (AWS DMS) para migrar datos desde la base de datos Db2 a la base de datos de Aurora compatible con MySQL. Se requerirán conversiones manuales para el código que AWS SCT no convierta.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa con una nube privada virtual (VPC)
- AWS SCT

- AWS DMS

Versiones de producto

- Versión más reciente de AWS SCT
- Db2 para Linux, versión 11.1.4.4 y posteriores

Arquitectura

Pila de tecnología de origen

- DB2/Linux x86-64 bits montado en una instancia EC2

Pila de tecnología de destino

- Una instancia de base de datos de la edición de Amazon Aurora compatible con MySQL

Arquitectura de origen y destino

El siguiente diagrama muestra la arquitectura de migración de datos entre las bases de datos compatibles con MySQL de Aurora de origen y de destino. La arquitectura de la nube de AWS incluye una nube privada virtual (VPC), una zona de disponibilidad, una subred pública para la instancia de Db2 y la instancia de replicación de AWS DMS, y una subred privada para la base de datos Aurora compatible con MySQL.

Herramientas

Servicios de AWS

- Amazon Aurora es un motor de base de datos relacional completamente administrado diseñado para la nube y compatible con MySQL y PostgreSQL.
- AWS Database Migration Service (AWS DMS) le permite migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones.
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.

- La Herramienta de conversión de esquemas de AWS (AWS SCT) simplifica las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado, lo que incluye las vistas, los procedimientos almacenados y las funciones, a un formato compatible con la base de datos de destino. AWS SCT admite como origen las versiones 9.1, 9.5, 9.7, 10.1, 10.1, 10.5, 11.1 y 11.5 de IBM Db2 para LUW.

Prácticas recomendadas

Para prácticas recomendadas, consulte Prácticas recomendadas para AWS Database Migration Service (AWS DMS).

Epics

Configurar la base de datos IBM Db2 de origen

Tarea	Descripción	Habilidades requeridas
Cree la base de datos IBM Db2 en Amazon EC2.	Puede crear una base de datos IBM Db2 en una instancia EC2 mediante una Imagen de máquina de Amazon (AMI) de AWS Marketplace o instalando el software Db2 en una instancia EC2. Para lanzar una instancia EC2, seleccione una AMI para IBM Db2 (por ejemplo, IBM Db2 v11.5.7 RHEL 7.9), que es similar a una base de datos en las instalaciones.	Administrador de base de datos, AWS general
Configuración de grupos de seguridad.	Configure las reglas de entrada del grupo de seguridad de VPC para SSH (Secure Shell) y TCP con los	AWS general

Tarea	Descripción	Habilidades requeridas
	puertos 22 y 50000, respectiv amente.	

Tarea	Descripción	Habilidades requeridas
Crear la instancia de base de datos.	Cree una instancia (usuario) y una base de datos (esquema) nuevas, o utilice la instancia y la base de datos `db2inst1` de muestra predeterminadas. 1. Conéctese a la instancia EC2 mediante el terminal para conectarse a la base de datos Db2. Como alternativa, puede instalar cualquier software cliente de base de datos que se conecte a la base de datos de Db2. 2. Para establecer la contraseña del usuario db2inst1, ejecute el comando `sudo passwd db2inst1`. 3. Para conectarse a la instancia db2inst1, ejecute el comando `sudo su - db2inst1`. 4. Para conectarse a la base de datos de Db2, ejecute el comando `db2`. 5. Para conectarse a la base de datos de muestra, utilice el comando `connect to sample`. Como alternativa, conéctese a la base de datos que creó.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	6. Tras conectarse a la instancia de base de datos, cree objetos e inserte datos en estos objetos mediante declaraciones de SQL de Db2.	
Confirme que la instancia de la base de datos Db2 está disponible.	Para confirmar que la instancia de la base de datos de Db2 está activa y en ejecución, utilice el comando `Db2pd -`.	Administrador de base de datos

Configurar la base de datos de destino de Aurora compatible con MySQL

Tarea	Descripción	Habilidades requeridas
Cree la base de datos de Aurora compatible con MySQL.	Crear una base de datos de Amazon Aurora con compatibilidad con MySQL desde el servicio de AWS RDS • Crear una base de datos en Amazon Aurora con compatibilidad con MySQL y la versión que prefiera, por ejemplo Aurora (MySQL)-5.6.10a • Instalar la aplicación MySQL Workbench o su software cliente de base de datos preferido, que le permite conectarse a la base de datos MySQL	Administrador de base de datos, AWS general

Tarea	Descripción	Habilidades requeridas
Configuración de grupos de seguridad.	Configure las reglas de entrada del grupo de seguridad de la VPC para las conexiones SSH y TCP.	AWS general
Confirme que la base de datos de Aurora esté disponible.	Para asegurarse de que la base de datos de Aurora compatible con MySQL esté en funcionamiento, haga lo siguiente: 1. Conéctese a la instancia EC2 a través de SSH. 2. Configure y conéctese a la instancia de Aurora compatible con MySQL desde MySQL Workbench. Utilice el punto de conexión como nombre de host, tal y como se muestra en el siguiente ejemplo. `mysql-cluster-instance-1.cokmvis0v46q.us-east-1.rds.amazonaws.com` 3. Cree el nuevo esquema y conéctese al nuevo esquema (por ejemplo, `mysql-sample-db2`). 4. Ejecute las declaraciones de MySQL para comprobar los esquemas y objetos de la base de datos.	Administrador de base de datos

Configuración y ejecución de AWS SCT

Tarea	Descripción	Habilidades requeridas
Instale AWS SCT.	Descargue e instale la versión más reciente de AWS SCT (la versión actual más reciente es 1.0.628).	AWS general
Configure AWS SCT.	1. Descargue los controladores de conectividad de bases de datos Java (JDBC) para IBM Db2 (versión 4.22.X) y MySQL (8.x). 2. Para configurar los controladores en AWS SCT, seleccione Settings (Configuración), Global settings (Configuración global) y Drivers (Controladores).	AWS general
Cree un proyecto de AWS SCT.	Cree un proyecto y un informe de AWS SCT que utilice Db2 para LUW como motor de base de datos de origen y Aurora compatible con MySQL para el motor de base de datos de destino. Para identificar los privilegios necesarios para conectarse a una base de datos de Db2 para LUW, consulte Uso de Db2 LUW como fuente de AWS SCT.	AWS general

Tarea	Descripción	Habilidades requeridas
Valide los objetos.	Seleccione Cargar esquema, validar los objetos. Actualice cualquier objeto incorrecto en la base de datos de destino: 1. Conéctese al servidor de Amazon Aurora compatibl e con MySQL proporcio nando los detalles de la conexión y seleccione Probar conexión. Tanto las conexiones de origen como las de destino deben realizarse correctamente antes de que AWS SCT pueda iniciar el informe de migración. 2. Una vez completado el informe, introduzca el esquema que desee convertir y seleccione Finalizar. AWS SCT muestra todos los objetos de origen y destino que se han convertido y tienen errores. 3. Revise los errores y elimínelos manualmente. 4. Una vez que se hayan borrado todos los errores, abra el menú contextua l (haga clic con el botón derecho) del esquema	Administrador de base de datos, AWS general

Tarea	Descripción	Habilidades requeridas
	y seleccione Cargar esquema. 5. Seleccione Aplicar a la base de datos. 6. En MySQL Workbench , conéctese a la base de datos de Aurora compatible con MySQL y compruebe el esquema y los objetos.	

Configurar y ejecutar AWS SCT

Tarea	Descripción	Habilidades requeridas
Crear una instancia de replicación.	Inicie sesión en la consola de administración de AWS, navegue hasta el servicio AWS DMS y cree una instancia de replicación con una configuración válida para el grupo de seguridad de VPC que configuró para las bases de datos de origen y destino.	AWS general
Crear puntos de conexión.	Cree el punto de conexión de origen para la base de datos Db2 y cree el punto de conexión de destino para la base de datos Aurora compatible con MySQL: 1. Cree un punto de conexión para IBM Db2 como origen seleccionando Seleccion	AWS general

Tarea	Descripción	Habilidades requeridas
	ar la instancia de base de datos RDS y, a continuación, seleccionando la instancia de Db2 que ha creado. Los detalles de configuración del punto de conexión se rellenarán automáticamente. 2. En la configuración específica del punto de conexión, añada los siguientes atributos de conexión adicionales. `CurrentLSN=<scan>; MaxKBytesPerRead=64; SetDataCaptureChanges=true` Si no menciona estos atributos, la conexión de prueba del punto de conexión de origen no se realizará correctamente. Para obtener más información, consulte Uso de IBM Db2 LUW como fuente de AWS DMS. 3. Para crear un punto de conexión de Aurora compatible con MySQL como destino, seleccione Seleccionar instancia de base de datos RDS y, a continuación, seleccion	

Tarea	Descripción	Habilidades requeridas
	e la instancia de Aurora compatible con MySQL que creó. Los detalles de configuración del punto de conexión se rellenará n automáticamente. Para obtener más información, consulte Usar una base de datos compatible con MySQL como destino para AWS Database Migration Service (AWS DMS). 4. Pruebe los puntos de conexión de origen y destino. Confirme que ambos son correctos y están disponibles. 5. Si la prueba falla, asegúrese de que las reglas de entrada del grupo de seguridad sean válidas.	

Tarea	Descripción	Habilidades requeridas
Crear tareas de migración.	Cree una o varias tareas de migración para completar la carga y validar los CDC o los datos: 1. Para crear una tarea de migración de base de datos, seleccione la instancia de replicación, el punto de conexión de la base de datos de origen y el punto de conexión de la base de datos de destino. Especifique el tipo de migración como Migrar los datos existentes (carga completa), Replicar solo los cambios de datos (CDC) o Migrar los datos existente s y replicar los cambios en curso (carga completa y CDC). 2. En las Asignaciones de tablas, puede configurar las reglas de selección y las reglas de transformación en formatos GUI o JSON. 3. En Reglas de selección , seleccione el esquema, introduzca el nombre de la tabla y seleccione la Acción (Incluir/Excluir) que desee configurar (por ejemplo, Esquema:	AWS general

Tarea	Descripción	Habilidades requeridas
	MUESTRA; Nombre de tabla: %, Acción: Incluir). 4. En Reglas de transformación, seleccione el objetivo (esquema, tabla o columna). Seleccione el nombre del esquema y seleccione la acción (mayúscula, prefijo, sufijo); por ejemplo, Objetivo: Esquema; `mysql-sample-db` ; Acción: Convertir a minúsculas. 5. Activa la supervisión de Amazon CloudWatch Logs.	
Planifique el ciclo de producción.	Confirme el tiempo de inactividad con las partes interesadas, como los propietarios de las aplicaciones, para ejecutar AWS DMS en los sistemas de producción.	Líder de migración
Ejecute las tareas de migración.	1. Inicie la tarea de AWS DMS que tenga el estado Listo. 2. Supervisa los registros de tareas de migración en Amazon CloudWatch Logs para detectar cualquier error.	AWS general

Tarea	Descripción	Habilidades requeridas
Valide los datos.	Revise los resultados y los datos de las tareas de migración en las bases de datos Db2 de origen y MySQL de destino: 1. Si el estado es Cargar la replicación en curso completa, significa que la carga completa con la migración de datos de los CDC se ha completado y la validación está en curso. 2. Conéctese a la base de datos de Aurora compatibl e con MySQL y compruebe los datos. 3. Compruebe los cambios en curso insertando o actualiza ndo los datos en la base de datos Db2.	Administrador de base de datos
Detenga las tareas de migración.	Una vez que la validación de datos se haya completad o correctamente, detenga las tareas de migración de la validación.	AWS general

Solución de problemas

Problema	Solución
Las conexiones de prueba de origen y destino de AWS SCT no funcionan.	Configure las versiones del controlador JDBC y las reglas de entrada del grupo de seguridad de VPC para que acepten el tráfico entrante.
Se produce un error en la ejecución de la prueba del punto de conexión de origen de Db2.	Configure la configuración `CurrentLSN=<scan>;` de conexión adicional.
La AWSDMS tarea no se puede conectar a la fuente de Db2 y aparece el siguiente error. `database is recoverable if either or both of the database configuration parameters LOGARCHMETH1 and LOGARCHMETH2 are set to ON`	Para evitar el error, ejecute los siguientes comandos: 1. `$ db2 update db cfg for sample using LOGARCHMETH1 DISK:/home/db2inst1/logs` 2. `$ db2stop` 3. `$ db2start` 4. `$ db2 connect to sample` `SQL1116N A connection to or activation of database "SAMPLE" cannot be made because of BACKUP PENDING. SQLSTATE=57019` 5. `$ db2 backup database sample to ../logs` `SQL2036N The path for the file or device "../logs" is not valid` 6. `$ cd` 7. `$ pwd` `/home/db2inst1` 8. `$ mkdir /tmp/backup`

Problema	Solución
	9. `$ db2 backup database sample to /tmp/backup` `Backup successful. The timestamp for this backup image is : 20190530084921` 10. `$ db2 connect to sample` `Database Connection Information` `Database server = DB2/LINUX 9.7.1` `SQL authorization ID = DB2INST1` `Local database alias = SAMPLE`

Recursos relacionados

Amazon EC2

- Amazon EC2
- Guías del usuario de Amazon EC2

Bases de datos

- Base de datos IBM Db2
- Amazon Aurora
- Uso de Amazon Aurora MySQL

AWS SCT

- Conversión de esquemas AWS DMS
- Guía del usuario de la herramienta de conversión de esquema de AWS
- Using the AWS SCT user interface (Utilizar la interfaz de usuario de AWS SCT)
- Uso de IBM Db2 LUW como origen para AWS SCT

AWS DMS

- AWS Database Migration Service (AWS DMS)
- Guía del usuario de AWS Database Migration Service (AWS DMS)
- Orígenes para la migración de datos
- Destinos para la migración de datos
- AWS Database Migration Service (AWS DMS) y la herramienta de conversión de esquemas de AWS ahora admiten IBM Db2 LUW como fuente (entrada del blog)
- Migrar aplicaciones que ejecutan bases de datos relacionales a AWS

Migración de una base de datos de Microsoft SQL Server de Amazon EC2 a Amazon DocumentDB mediante AWS DMS

Origen: Microsoft SQL Server en Amazon EC2	Destino: Amazon DocumentDB	Tipo R: renovar arquitectura
Entorno: PoC o piloto	Tecnologías: nativas en la nube; bases de datos; migración	Carga de trabajo: Microsoft
Servicios de AWS: Amazon EC2; Amazon DocumentDB		

Resumen

Este patrón describe cómo usar AWS Database Migration Service (AWS DMS) para migrar una base de datos de Microsoft SQL Server alojada en una instancia de Amazon Elastic Compute Cloud (Amazon EC2) a una base de datos Amazon DocumentDB (con compatibilidad con MongoDB).

La tarea de replicación de AWS DMS lee la estructura de tablas de la base de datos de SQL Server, crea la colección correspondiente en Amazon DocumentDB y lleva a cabo una migración de carga completa.

También se puede usar este patrón para migrar una instancia de base de datos de SQL Server en las instalaciones o Amazon Relational Database Service (Amazon RDS) para SQL Server a Amazon DocumentDB. Para obtener más información, consulte la guía Migrating Microsoft SQL Server databases to the AWS Cloud (Migrar bases de datos de Microsoft SQL Server a la nube de AWS) en el sitio web de Recomendaciones de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una base de datos de SQL Server existente en una instancia EC2.

- Función de base de datos fija (db_owner) asignada a AWS DMS en la base de datos de SQL Server. Para obtener más información, consulte Database-level roles (Roles en el nivel de base de datos) de la documentación de SQL Server.
- Familiaridad con el uso de los programas de utilidades `mongodump`, `mongorestore`,`mongoexport` y `mongoimport` para mover datos dentro y fuera de un clúster de Amazon DocumentDB.
- Microsoft SQL Server Management Studio, instalado y configurado.

Limitaciones

- El límite de tamaño del clúster en Amazon DocumentDB es de 64 TB. Para obtener más información, consulte Cluster limits (Límites de los clústeres) en la documentación de Amazon DocumentDB.
- AWS DMS no permite combinar varias tablas de origen en una sola colección de Amazon DocumentDB.
- Si AWS DMS procesa los cambios de una tabla de origen sin una clave principal, omitirá las columnas de objetos grandes (LOB) de la tabla de origen.

Arquitectura

Pila de tecnología de origen

- Amazon EC2

Arquitectura de destino

Pila de tecnología de destino

- Amazon DocumentDB

Herramientas

- WS DMS: AWS Database Migration Service (AWS DMS) ayuda a migrar los datos de forma rápida y segura.

- Amazon DocumentDB: Amazon DocumentDB (con compatibilidad con MongoDB) es un servicio de bases de datos rápido, fiable y totalmente gestionado.
- Amazon EC2: Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de AWS.
- Microsoft SQL Server: SQL Server es un sistema de administración de bases de datos relacionales.
- SQL Server Management Studio (SSMS): SSMS es una herramienta para administrar SQL Server, que incluye el acceso, la configuración y la administración de los componentes de SQL Server.

Epics

Crear y configurar una VPC

Tarea	Descripción	Habilidades requeridas
Cree una VPC.	Inicie sesión en la consola de administración de AWS y abra la consola de Amazon VPC. Cree una nube privada virtual (VPC) con un rango de bloques de CIDR de IPv4.	Administrador de sistemas
Cree grupos de seguridad y ACL de red.	En la consola de Amazon VPC, cree grupos de seguridad y listas de control de acceso de la red (ACL de la red) para su VPC, según sus requisitos. También puede utilizar la configura ción predeterminada para estas configuraciones. Para obtener más información sobre esta y otras explicaci ones, consulte la sección «Recursos relacionados».	Administrador de sistemas

Crear y configurar el clúster de Amazon DocumentDB

Tarea	Descripción	Habilidades requeridas
Cree un clúster de Amazon DocumentDB.	Abra la consola de Amazon DocumentDB y seleccione «Clústeres». Elija «Crear» y cree un clúster de Amazon DocumentDB con una instancia. Importante: Asegúrese de configurar este clúster con los grupos de seguridad de su VPC.	Administrador de sistemas
Instale el intérprete de comandos de mongo.	El intérprete de comandos de mongo es un programa de utilidad de línea de comandos que se utiliza para conectars e al clúster de Amazon DocumentDB y consultarlo. Para instalarlo, ejecute el comando «/etc/yum.repos.d/ mongodb-org-3.6.repo» para crear el archivo de repositor io. Ejecute el comando «sudo yum install -y mongodb-org-shell» para instalar el shell mongo. Para cifrar los datos en tránsito, descargue la clave pública de Amazon DocumentDB y, a continuac ión, conéctese a su instancia de Amazon DocumentDB. Para obtener más informaci ón sobre este y otros pasos, consulte la sección «Recursos relacionados».	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Cree una base de datos en el clúster de Amazon DocumentDB.	Ejecute el comando «use» con el nombre de la base de datos para crear una base de datos en el clúster de Amazon DocumentDB.	Administrador de sistemas

Cree y configure una instancia de replicación de AWS DMS

Tarea	Descripción	Habilidades requeridas
Cree una instancia de replicación de AWS DMS.	Abra la consola de AWS DMS y seleccione «Create replication instance» (Crear instancia de replicación). Especifique un nombre y una descripción para la tarea de replicación. Seleccione la clase de instancia, la versión del motor, el almacenamiento, la VPC y las zonas de disponibilidad múltiples (Multi-AZ) y póngalas a disposición del público. Seleccione la pestaña «Advanced» para establecer la configuración de red y de cifrado. Especifique la configuración de mantenimiento y, a continuación, seleccione «Create replication instance» (Crear instancia de replicación).	Administrador de sistemas
Configure la base de datos de SQL Server.	Inicie sesión en Microsoft SQL Server y agregue una regla	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	de entrada para la comunicac ión entre el punto de conexión de origen y la instancia de replicación de AWS DMS. Utilice la dirección IP privada de la instancia de replicación como origen. Importante: La instancia de replicación y el punto de conexión de destino deben estar en la misma VPC. Utilice un origen alternativo en el grupo de seguridad si las VPC son diferentes para las instancias de origen y de replicación.	

Cree y pruebe los puntos de conexión de origen y destino en AWS DMS

Tarea	Descripción	Habilidades requeridas
Cree puntos de conexión de base de datos de origen y destino.	Abra la consola de AWS DMS y seleccione «Connect source and target database endpoints» (Conectar puntos de conexión de base de datos de origen y destino). Especifique la informaci ón de conexión para las bases de datos de origen y destino. Si es necesario , seleccione la pestaña «Advanced» (Avanzado) para establecer los valores de «Extra connection attribute	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	s» (Atributos de conexión adicionales). Descargue y utilice el grupo de certificados de la configuración del punto de conexión.	
Pruebe la conexión del punto de conexión.	Para probar la conexión, seleccione «Run test» (Ejecutar prueba). Para solucionar cualquier mensaje de error, compruebe la configuración del grupo de seguridad y las conexiones a la instancia de replicación de AWS DMS desde las instancia s de base de datos de origen y destino.	Administrador de sistemas

Migración de datos

Tarea	Descripción	Habilidades requeridas
Cree la tarea de migración de AWS DMS.	En la consola de AWS DMS, seleccione «Tasks» (Tareas) y «Create task» (Crear tarea). Especifique las opciones de la tarea, incluidos los nombres de los puntos de conexión de origen y destino y los nombres de las instancias de replicación. En «Migratio n type» (Tipo de migración), seleccione «Migrate existing data» (Migrar datos existente s) y «Replicate data changes	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	only» (Replicar solo los cambios de datos). Seleccione «Start task» (Iniciar tarea).	
Ejecute la tarea de migración de AWS DMS.	En «Task settings» (Configuración de tareas), especifique los ajustes del modo de preparación de tablas, como «Do nothing» (No hacer nada), «Drop tables on target» (Colocar las tablas en el destino), «Truncate» (Truncar) e «Include LOB column in replication» (Incluir columnas LOB en la replicación). Establezca un tamaño de LOB máximo que AWS DMS acepte y seleccione «Enable logging» (Habilitar registro). Deje «Advanced settings» (Configuración avanzada) en sus valores predeterminados y seleccione «Create task» (Crear tarea).	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Supervise la migración.	En la consola de AWS DMS, seleccione «Tasks» (Tareas) y, a continuación, su tarea de migración. Seleccione «Task monitoring» (Supervisión de tareas) para supervisar su tarea. La tarea se detiene cuando la migración de carga completa finaliza y se aplican los cambios guardados en la memoria caché.	Administrador de sistemas

Probar y verificar la aplicación

Tarea	Descripción	Habilidades requeridas
Conéctese al clúster de Amazon DocumentDB mediante el intérprete de comandos de mongo.	Abra la consola de Amazon DocumentDB y seleccion e el clúster que le interese en «Clústeres». En la pestaña «Connectivity and Security» (Conectividad y seguridad), seleccione «Connect to this cluster with the mongo shell» (Conectarse a este clúster con el intérprete de comandos de mongo).	Administrador de sistemas
Verifique los resultados de la migración.	Ejecute el comando «use» con el nombre de su base de datos y, a continuación, ejecute el comando «show collections». Ejecute el comando «db. .count ();»	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	con el nombre de su base de datos. Si los resultados coinciden con la base de datos de origen, la migración se ha realizado correctamente.	

Recursos relacionados

Create and configure a VPC (Crear y configurar una VPC)

- Create a security group for your VPC (Crear un grupo de seguridad para la VPC)
- Create a network ACL (Crear una ACL de red)

Create and configure the Amazon DocumentDB cluster (Crear y configurar el clúster de Amazon DocumentDB)

- Create an Amazon DocumentDB cluster (Crear un clúster de Amazon DocumentDB)
- Install the mongo shell for Amazon DocumentDB (Instalar el intérprete de comandos de mongo para Amazon DocumentDB)
- Connect to your Amazon DocumentDB cluster (Conectarse al clúster de Amazon DocumentDB)

Create and configure the AWS DMS replication instance (Crear y configurar una instancia de replicación de AWS DMS)

- Use public and private replication instances (Usar instancias de replicación pública y privada)

Create and test the source and target endpoints in AWS DMS (Crear y probar los puntos de conexión de origen y destino en AWS DMS)

- Use Amazon DocumentDB as a target for AWS DMS (Utilizar Amazon DocumentDB como destino para AWS DMS)
- Use a SQL Server database as a source for AWS DMS (Utilizar una base de datos de SQL Server como origen para AWS DMS)
- Use AWS DMS endpoints (Utilizar puntos de conexión de AWS DMS)

Migración de datos

- Migrate to Amazon DocumentDB (Migrar a Amazon DocumentDB)

Otros recursos

- Limitations on using SQL Server as a source for AWS DMS (Restricciones en el uso de SQL Server como origen para AWS DMS)
- How to use Amazon DocumentDB to build and manage applications at scale (Cómo utilizar Amazon DocumentDB para crear y gestionar aplicaciones a gran escala)

Migre una base de datos ThoughtSpot Falcon local a Amazon Redshift

Creado por Battulga Purevragchaa (AWS) y Antony Prasad Thevaraj (AWS)

Entorno: PoC o piloto	Fuente: base de datos Falcon local ThoughtSpot	Destino: Amazon Redshift
Tipo R: renovar arquitectura	Carga de trabajo: todas las demás cargas de trabajo	Tecnologías: Migración; bases de datos
Servicios de AWS: AWS DMS; Amazon Redshift		

Resumen

El almacenamiento de datos en las instalaciones requiere una cantidad considerable de tiempo y recursos de administración, especialmente en el caso de conjuntos de datos de gran tamaño. El costo financiero de compilar, mantener y hacer crecer estos almacenes también es muy alto. Para ayudar a administrar los costos, mantener baja la complejidad de extracción, transformación y carga (ETL) y ofrecer rendimiento a medida que sus datos crecen, debe elegir constantemente qué datos cargar y qué datos archivar.

Al migrar sus bases de datos ThoughtSpot Falcon locales a la nube de Amazon Web Services (AWS), puede acceder a lagos de datos y almacenes de datos basados en la nube que aumentan la agilidad, la seguridad y la confiabilidad de las aplicaciones de su empresa, además de reducir los costos generales de infraestructura. Amazon Redshift ayuda a reducir considerablemente los costos y los gastos operativos de un almacenamiento de datos. También puede usar Amazon Redshift Spectrum para analizar grandes cantidades de datos en su formato nativo sin necesidad de cargar los datos.

Este patrón describe los pasos y el proceso para migrar una base de datos ThoughtSpot Falcon de un centro de datos local a una base de datos de Amazon Redshift en la nube de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa

- Una base de datos ThoughtSpot Falcon alojada en un centro de datos local

Versiones de producto

- ThoughtSpot versión 7.0.1

Arquitectura

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Los datos se alojan en una base de datos relacional en las instalaciones.
2. La herramienta de conversión de esquemas de AWS (AWS SCT) convierte el lenguaje de definición de datos (DDL) que es compatible con Amazon Redshift.
3. Una vez creadas las tablas, puede migrar los datos mediante AWS Database Migration Service (AWS DMS).
4. Los datos se cargan en Amazon Redshift.
5. Los datos se almacenan en Amazon Simple Storage Service (Amazon S3) si utiliza Redshift Spectrum o si ya aloja los datos en Amazon S3.

Herramientas

- AWS DMS: AWS Data Migration Service (AWS DMS) le ayuda a migrar bases de datos a AWS de forma rápida y segura.
- Amazon Redshift: Amazon RedShift es un servicio de almacenamiento de datos de escala de petabyte rápido, totalmente administrado, que hace que sea simple y rentable analizar de manera eficiente todos sus datos utilizando sus herramientas de inteligencia empresariales existentes.
- AWS SCT: la herramienta de conversión de esquemas de AWS (AWS SCT) convierte el esquema de base de datos existente de un motor de base de datos a otro.

Epics

Preparación para la migración

Tarea	Descripción	Habilidades requeridas
Identifique la configuración de Amazon Redshift adecuada.	Identifique la configuración de clúster de Amazon Redshift adecuada en función de sus requisitos y volumen de datos. Para obtener más información, consulte Clústeres de Amazon Redshift en la documentación de Amazon Redshift.	Administrador de base de datos
Investigue Amazon Redshift para evaluar si cumple con sus requisitos.	Consulte las Preguntas frecuentes de Amazon Redshift para comprender y evaluar si Amazon Redshift cumple con sus requisitos.	Administrador de base de datos

Preparación del clúster de Amazon Redshift de destino

Tarea	Descripción	Habilidades requeridas
Crear un clúster de Amazon Redshift.	Inicie sesión en la consola de administración de AWS, abra la consola de Amazon Redshift y, a continuación, cree un clúster de Amazon Redshift en una nube privada virtual (VPC). Para obtener más informaci ón, consulte Creación de	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	un clúster en una VPC en la documentación de Amazon Redshift.	
Lleve a cabo una PoC para el diseño de su base de datos de Amazon Redshift.	Siga las prácticas recomendadas de Amazon Redshift realizando una prueba de concepto (PoC) para el diseño de su base de datos. Para obtener más información, consulte Realización de una prueba de concepto para Amazon Redshift en la documentación de Amazon Redshift.	Administrador de base de datos
Cree usuarios de bases de datos.	Cree los usuarios en la base de datos de Amazon Redshift y asigne los roles adecuados para acceder al esquema y a las tablas. Para obtener más información, consulte Conceder privilegios de acceso a un usuario o grupo de usuarios en la documentación de Amazon Redshift.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Aplique los parámetros de configuración a la base de datos de destino.	Aplique los parámetros de configuración a la base de datos de Amazon Redshift según sus requisitos. Para obtener más informaci ón sobre cómo habilitar los parámetros de base de datos, sesión y servidor, consulte la Referencia de configura ción en la documentación de Amazon Redshift.	Administrador de base de datos

Crear objetos en el clúster de Amazon Redshift

Tarea	Descripción	Habilidades requeridas
Cree tablas manualmente con DDL en Amazon Redshift.	(Opcional) Si utiliza AWS SCT, las tablas se crean automáticamente. Sin embargo, si se producen errores al replicar los DDL, debe crear las tablas manualmente	Administrador de base de datos
Crear tablas externas para Redshift Spectrum.	Cree una tabla externa con un esquema externo para Amazon Redshift Spectrum. Para crear tablas externas, debe ser el propietario del esquema externo o un superusuario de base de datos.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Para obtener más información, consulte Creación de tablas externas para Amazon Redshift Spectrum en la documentación de Amazon Redshift.	

Migración de datos utilizando AWS DMS

Tarea	Descripción	Habilidades requeridas
Utilice AWS DMS para migrar los datos.	Tras crear el DDL de las tablas en la base de datos de Amazon Redshift, migre sus datos a Amazon Redshift mediante AWS DMS. Para obtener instrucciones y pasos detallados, consulte Uso de una base de datos de Amazon Redshift como destino de AWS DMS en la documentación de AWS DMS.	Administrador de base de datos
Uso del comando COPY para cargar datos.	Utilice el comando `COPY` de Amazon Redshift para cargar los datos desde Amazon S3 a Amazon Redshift. Para obtener más información, consulte Uso del comando COPIAR para cargar desde Amazon S3 en la documentación de Amazon Redshift.	Administrador de base de datos

Validar el clúster de Amazon Redshift

Tarea	Descripción	Habilidades requeridas
Valide los registros de origen y destino.	Valide el recuento de tablas de los registros de origen y destino que se cargaron desde el sistema de origen.	Administrador de base de datos
Implemente las prácticas recomendadas de Amazon Redshift para el ajuste del rendimiento.	Implemente las prácticas recomendadas de Amazon Redshift para el diseño de tablas y bases de datos. Para obtener más informaci ón, consulte la siguiente entrada del blog: Las 10 técnicas principales de ajuste del rendimiento de Amazon Redshift.	Administrador de base de datos
Optimizar el rendimiento de la consulta.	Amazon RedShift utiliza consultas basadas en SQL para interactuar con datos y objetos en el sistema. El Data Manipulation Language (DML, Lenguaje de manipulación de datos) es el subconjunto de SQL que el usuario utiliza para ver, añadir, cambiar y eliminar datos. DDL es el subconjun to de SQL que el usuario utiliza para añadir, cambiar y eliminar objetos de la base de datos como tablas y vistas. Para obtener más información, consulte Ajuste del rendimien	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	to de las consultas en la documentación de Amazon Redshift.	
Implemente WLM.	Puede utilizar workload management (WLM) para definir varias colas de consultas y dirigir las consultas a las colas adecuadas en tiempo de ejecución. Para obtener más información, consulte Implementación de la administración de la carga de trabajo en la documentación de Amazon Redshift.	Administrador de base de datos
Trabajar con escalado de concurrencia.	Al usar la característica de escalado de concurren cia, puede admitir usuarios concurrentes prácticam ente ilimitados y consultas concurrentes, con un rendimiento de consulta consistentemente rápido. Para obtener más informaci ón, consulte Uso del escalado de simultaneidad en la documentación de Amazon Redshift.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Use las prácticas recomendadas de Amazon RedShift para el diseño de tablas.	Cuando planifica su base de datos, ciertas decisiones importantes de diseño de tabla pueden influir considerablemente en el rendimiento general de la consulta. Para obtener más información sobre seleccionar la opción de diseño de tablas más adecuada, consulte Prácticas recomendadas de Amazon Redshift para el diseño de tablas en la documentación de Amazon Redshift.	Administrador de base de datos
Crear vistas materializadas en Amazon Redshift.	Una vista materializada contiene un conjunto de resultados computados previamente, basados en una consulta de SQL sobre una o más tablas base. Puede emitir instrucciones SELECT para consultar una vista materializada, de la misma manera que puede consultar otras tablas o vistas en la base de datos. Para obtener más información, consulte Creación de vistas materializadas en Amazon Redshift en la documentación de Amazon Redshift.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Defina las uniones entre las tablas.	Para buscar en más de una tabla al mismo tiempo ThoughtSpot, debe definir las uniones entre las tablas especificando columnas que contengan datos coincidentes en dos tablas. Estas columnas representan la `primary key` y `foreign key` de la unión. Puede definirlos mediante el `ALTER TABLE` comando de Amazon Redshift o. ThoughtSpot Para obtener más información, consulte ALTER TABLE en la documentación de Amazon RedShift.	Administrador de base de datos

Configurar la ThoughtSpot conexión a Amazon Redshift

Tarea	Descripción	Habilidades requeridas
Añada una conexión de Amazon Redshift.	Añada una conexión Amazon Redshift a su base de datos Falcon local. ThoughtSpot Para obtener más informaci ón, consulte Añadir una conexión Amazon Redshift en la ThoughtSpot documenta ción.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Edite la conexión de Amazon Redshift.	Puede editar la conexión de Amazon Redshift para añadir tablas y columnas. Para obtener más información, consulte Edición de una conexión de Amazon Redshift en la ThoughtSpot documentación.	Administrador de base de datos
Reasigne la conexión de Amazon Redshift.	Modifique los parámetros de conexión editando el archivo .yaml de asignación de origen que se creó al añadir la conexión de Amazon Redshift. Por ejemplo, puede reasignar la tabla o columna existente a una tabla o columna diferente en una conexión de base de datos existente. ThoughtSpot recomienda comprobar las dependencias antes y después de volver a mapear una tabla o columna de una conexión para asegurarse de que se muestran según sea necesario. Para obtener más información, consulte Remapear una conexión de Amazon Redshift en ThoughtSpot la documentación.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Elimine una tabla de la conexión de Amazon Redshift.	(Opcional) Si intenta eliminar una tabla de una conexión de Amazon Redshift, ThoughtSpot comprueba las dependencias y muestra una lista de objetos dependientes. Puede elegir los objetos de la lista para eliminarlos o eliminar la dependencia. A continuación puede eliminar la tabla. Para obtener más información, consulte Eliminar una tabla de una conexión de Amazon Redshift en la ThoughtSpot documentación.	Administrador de base de datos
Elimine una tabla con objetos dependientes de una conexión de Amazon Redshift.	(Opcional) Si intenta eliminar una tabla con objetos dependientes, la operación se bloquea. Se muestra una ventana `Cannot delete` con una lista de enlaces a objetos dependientes. Cuando se eliminen todas las dependencias, podrá eliminar la tabla Para obtener más información, consulte Eliminar una tabla con objetos dependientes de una conexión de Amazon Redshift en la ThoughtSpot documentación.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Elimine una conexión de Amazon Redshift.	(Opcional) Como una conexión se puede utilizar en varios orígenes de datos o visualizaciones, debe eliminar todas las fuentes y tareas que utilizan esa conexión antes de poder eliminar la conexión de Amazon Redshift. Para obtener más informaci ón, consulte Eliminar una conexión de Amazon Redshift en la ThoughtSpot documenta ción.	Administrador de base de datos
Compruebe la referencia de conexión de Amazon Redshift.	Asegúrese de proporcionar la información necesaria para su conexión a Amazon Redshift utilizando la referencia de conexión de la documenta ción. ThoughtSpot	Administrador de base de datos

Información adicional

- Análisis basados en IA a cualquier escala con Amazon ThoughtSpot Redshift
- Precios de Amazon Redshift
- Introducción a AWS SCT
- Introducción a Amazon Redshift
- Uso de agentes de extracción de datos
- Chick-fil-A mejora la velocidad de obtención de información con AWS ThoughtSpot

Migrar una base de datos de Oracle a Amazon DynamoDB mediante AWS DMS

Creado por Rambabu Karnena (AWS)

Entorno: PoC o piloto	Origen: bases de datos: relacionales	Destino: Amazon DynamoDB
Tipo R: renovar arquitectura	Carga de trabajo: Oracle	Tecnologías: Migración; bases de datos
Servicios de AWS: Amazon DynamoDB		

Resumen

Este patrón le guía por los pasos para migrar una base de datos de Oracle a Amazon DynamoDB mediante AWS Database Migration Service (AWS DMS). Abarca tres tipos de bases de datos de origen:

- Bases de datos Oracle en las instalaciones
- Bases de datos de Oracle en Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Relational Database Service (Amazon RDS) para instancias de bases de datos de Oracle

En esta prueba de concepto, este patrón se centra en la migración desde una instancia de BD de Amazon RDS para Oracle.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una aplicación que se conecta a una base de datos de Amazon RDS para Oracle
- Una tabla creada en la base de datos de Amazon RDS para Oracle de origen con una clave principal y datos de muestra

Limitaciones

- Los objetos de la base de datos de Oracle, como los procedimientos, las funciones, los paquetes y los desencadenadores, no se consideran para la migración porque Amazon DynamoDB no admite estos objetos de base de datos.

Versiones de producto

- Este patrón se aplica a todas las ediciones y versiones de las bases de datos de Oracle compatibles con AWS DMS. Para obtener más información, consulte el uso de una base de datos de Oracle como origen para AWS DMS y el uso de una base de datos de Amazon DynamoDB como destino para AWS DMS. Le recomendamos utilizar las versiones más recientes de AWS DMS para obtener el soporte más completo de versiones y características.

Arquitectura

Pila de tecnología de origen

- Instancias de base de datos de Amazon RDS para Oracle, Oracle en Amazon EC2 o bases de datos Oracle en las instalaciones.

Pila de tecnología de destino

- Amazon DynamoDB

Arquitectura de migración de datos de AWS

Herramientas

- AWS Database Migration Service (AWS DMS) le permite migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones.
- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- Amazon Relational Database Service (Amazon RDS) le ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS. Este patrón utiliza Amazon RDS para Oracle.

Epics

Planifique la migración

Tarea	Descripción	Habilidades requeridas
Cree una VPC.	En su cuenta de AWS, cree una nube privada virtual (VPC) y una subred privada.	Administrador de sistemas
Crear grupos de seguridad y listas de control de acceso a la red.	Para obtener más información, consulte la documentación de AWS.	Administrador de sistemas
Configure e inicie la instancia de BD de Amazon RDS para Oracle.	Para obtener más información, consulte la documentación de AWS.	Administrador de base de datos, administrador de sistemas

Migrar datos

Tarea	Descripción	Habilidades requeridas
Crear un rol de IAM para acceder a DynamoDB.	En la consola de AWS Identity and Access Management (IAM), cree el rol, adjunte la política `AmazonDynamoDBFullAccess to it` y seleccione AWS DMS como servicio.	Administrador de sistemas
Crear una instancia de replicación de AWS DMS para la migración.	La instancia de replicación debe estar en la misma zona de disponibilidad y VPC que la base de datos de origen.	Administrador de sistemas
Crear puntos de conexión de origen y destino en AWS DMS.	Para crear el punto de conexión de la base de datos de origen, tiene dos opciones:	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	• En la consola de Amazon RDS, elija Bases de datos, Identificador de base BD, Conectividad y seguridad y elija el punto de conexión. • En la consola de AWS DMS, elija Seleccionar instancia de RDS DB. Para crear el punto de conexión de la base de datos de destino, elija el rol de Nombre de recurso de Amazon (ARN) de la tarea anterior para acceder a DynamoDB.	
Cree una tarea de AWS DMS para cargar las tablas de base de datos Oracle de origen en DynamoDB.	Elija los nombres de los puntos de conexión de origen y destino y la instancia de replicación en los pasos anteriores. El tipo puede ser de carga completa. Elija el esquema de Oracle y especifique % para seleccion ar todas las tablas.	Administrador de sistemas
Valide las tablas en DynamoDB.	Para ver los resultados de la migración, seleccione Tablas en el panel de navegación izquierdo de la consola de DynamoDB.	Administrador de base de datos

Migrar la aplicación

Tarea	Descripción	Habilidades requeridas
Modificar el código de la aplicación	Para conectarse y recuperar datos de DynamoDB, actualice el código de la aplicación.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Cambie los clientes de la aplicación para que usen DynamoDB.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cierre los recursos de AWS.	Por ejemplo, cierre la instancia de Amazon RDS para Oracle, DynamoDB y la instancia de replicación de AWS DMS.	Administrador de base de datos, administrador de sistemas
Recopile métricas.	Las métricas incluyen el tiempo de migración, los porcentajes de trabajo manual y realizado por la herramienta y el ahorro de costos.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Recursos relacionados

- AWS Database Migration Service (AWS DMS) y Amazon DynamoDB: lo que necesita saber (entrada del blog)
- Uso de una base de datos de Oracle como origen para AWS DMS
- Uso de una base de datos de Amazon DynamoDB como objetivo del servicio de migración de bases de datos de AWS
- Prácticas recomendadas para migrar de RDBMS a Amazon DynamoDB (documento técnico)

Migre una tabla particionada de Oracle a PostgreSQL mediante AWS DMS

Creado por Saurav Mishra (AWS) y Eduardo Valentim (AWS)

Entorno: PoC o piloto	Origen: Oracle	Destino: PostgreSQL 9.0
Tipo R: renovar arquitectura	Carga de trabajo: Oracle	Tecnologías: modernización; bases de datos; almacenamiento y respaldo
Servicios de AWS: AWS DMS		

Resumen

Este patrón describe cómo acelerar la carga de una tabla particionada de Oracle a PostgreSQL mediante AWS Database Migration Service (AWS DMS), que no admite el particionamiento nativo. La base de datos PostgreSQL de destino puede instalarse en Amazon Elastic Compute Cloud (Amazon EC2) o puede ser una instancia de base de datos de Amazon Relational Database Service (Amazon RDS) para PostgreSQL o instancia de base de datos Edition compatible con PostgreSQL o Amazon Aurora PostgreSQL.

La carga de una tabla particionada incluye los pasos siguientes:

1. Cree una tabla principal similar a la tabla de particiones de Oracle, pero no incluya ninguna partición.
2. Cree tablas secundarias que hereden de la tabla principal que se creó en el paso 1.
3. Cree una función de procedimiento y un disparador para gestionar las inserciones en la tabla principal.

Sin embargo, dado que el disparador se activa para cada inserción, la carga inicial con AWS DMS puede ser muy lenta.

Para acelerar las cargas iniciales de Oracle a PostgreSQL 9.0, este patrón crea una tarea de AWS DMS independiente para cada partición y carga las tablas secundarias correspondientes. A continuación, se crea un disparador durante la transición.

La versión 10 de PostgreSQL admite particiones nativas. Sin embargo, en algunos casos puede decidir utilizar la partición heredada. Para obtener más información, consulte la sección Additional information (Información adicional).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una base de datos Oracle de origen con una tabla particionada
- Una base de datos PostgreSQL en AWS

Versiones de producto

- PostgreSQL 9.0

Arquitectura

Pila de tecnología de origen

- Una tabla particionada en Oracle

Pila de tecnología de destino

- Una tabla particionada en PostgreSQL (en Amazon EC2, Amazon RDS para PostgreSQL o Aurora PostgreSQL)

Arquitectura de destino

Herramientas

- AWS Database Migration Service (AWS DMS) le permite migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones.

Epics

Configure AWS DMS

Tarea	Descripción	Habilidades requeridas
Cree las tablas en PostgreSQL.	Cree las tablas principales y secundarias correspondientes en PostgreSQL con las condiciones de comprobación necesarias para las particiones.	Administrador de base de datos
Cree la tarea AWS DMS para cada partición.	Incluya el estado del filtro de la partición en la tarea de AWS DMS. Asigne las particiones a las tablas secundarias de PostgreSQL correspondientes.	Administrador de base de datos
Ejecute las tareas de AWS DMS con captura de datos de cambio y carga completa (CDC).	Además, compruebe que el parámetro `StopTaskCachedChangesApplied` está establecido en `true` y que el parámetro `StopTaskCachedChangesNotApplied` está establecido en `false`.	Administrador de base de datos

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Detiene la tarea de replicación.	Antes de detener las tareas, confirme que el origen y el destino están sincronizados.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree un disparador en la tabla principal.	Como la tabla principal recibirá todos los comandos de inserción y actualización, cree un activador que dirija estos comandos a las tablas secundarias respectivas en función de la condición de partición.	Administrador de base de datos

Recursos relacionados

- AWS DMS
- Particionamiento de tablas (documentación de PostgreSQL)

Información adicional

Aunque la versión 10 de PostgreSQL admite la partición nativa, puede decidir usar la partición heredada para los siguientes casos de uso:

- La partición impone una regla según la cual todas las particiones deben tener el mismo conjunto de columnas que la principal, pero la herencia de tablas permite que las particiones secundarias tengan columnas adicionales.
- La herencia de tablas admite herencias múltiples.
- La partición declarativa solo admite la partición de listas y rangos. Con la herencia de tablas, puede dividir los datos como desee. Sin embargo, si la exclusión de la restricción no puede reducir las particiones de forma eficaz, el rendimiento de las consultas se verá afectado.
- Algunas operaciones necesitan un bloqueo más fuerte cuando se usa la partición declarativa que cuando se usa la herencia de tablas. Por ejemplo, añadir o quitar una partición de una tabla particionada requiere un bloqueo `ACCESS EXCLUSIVE` en la tabla principal, mientras que un bloqueo `SHARE UPDATE EXCLUSIVE` es suficiente para una herencia normal.

Si utiliza particiones de trabajo independientes, también puede volver a cargar las particiones si hay algún problema de validación de AWS DMS. Para mejorar el rendimiento y el control de la replicación, ejecute las tareas en instancias de replicación independientes.

Migrar de Amazon RDS para Oracle a Amazon RDS para MySQL

Creado por Jitender Kumar (AWS), Neha Sharma (AWS) y Srini Ramaswamy (AWS)

Entorno: PoC o piloto	Origen: Amazon RDS para Oracle	Destino: Amazon RDS para MySQL
Tipo R: renovar arquitectura	Carga de trabajo: Oracle	Tecnologías: migración; bases de datos
Servicios de AWS: Amazon RDS		

Resumen

Este patrón proporciona orientación para migrar una instancia de base de datos Amazon Relational Database Service (Amazon RDS) para Oracle a una instancia de base de datos Amazon RDS for MySQL en Amazon Web Services (AWS). El patrón utiliza AWS Database Migration Service (AWS DMS) y AWS Schema Conversion Tool (AWS SCT).

El patrón proporciona las prácticas recomendadas para gestionar la migración de los procedimientos almacenados. También cubre y codifica los cambios para admitir la capa de aplicación.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una base de datos de origen de Amazon RDS para Oracle.
- Una base de datos de destino de Amazon RDS para MySQL. Las bases de datos de origen y destino deben estar en la misma nube privada virtual (VPC). Si utiliza varias VPC o debe tener los permisos de acceso necesarios.
- Grupos de seguridad que permiten la conectividad entre las bases de datos de origen y destino, AWS SCT, el servidor de la aplicación y AWS DMS.
- Una cuenta de usuario con los privilegios necesarios para ejecutar AWS SCT en la base de datos de origen.
- Se habilitó el registro suplementario para ejecutar AWS DMS en la base de datos de origen.

Limitaciones

- El límite de tamaño de la base de datos de Amazon RDS de origen y destino es de 64 TB. Para obtener información sobre el tamaño de Amazon RDS, consulte la documentación de AWS.
- Oracle distingue mayúsculas de minúsculas para los objetos de base de datos, pero MySQL no. AWS SCT puede solucionar este problema al crear un objeto. Sin embargo, es necesario realizar algunos trabajos manuales para no distinguir entre mayúsculas y minúsculas.
- Esta migración no utiliza extensiones de MySQL para habilitar las funciones nativas de Oracle. AWS SCT gestiona la mayor parte de la conversión, pero es necesario trabajar un poco para cambiar el código manualmente.
- Se requieren cambios en el controlador de Java Database Connectivity (JDBC) en la aplicación.

Versiones de producto

- Amazon RDS para Oracle 12.2.0.1 y versiones posteriores. Para ver las versiones de RDS para Oracle compatibles actualmente, consulte la documentación de AWS.
- Amazon RDS for MySQL 8.0.15 y versiones posteriores. Para ver las versiones de RDS para MySQL compatibles actualmente, consulte la documentación de AWS.
- AWS DMS versión 3.3.0 y posteriores. Consulte la documentación de AWS para obtener más información sobre los puntos de enlace de origen y destino compatibles con AWS DMS.
- AWS SCT versión 1.0.628 y posteriores. Consulte la matriz de soporte de puntos finales de origen y destino de AWS SCT en la documentación de AWS.

Arquitectura

Pila de tecnología de origen

- Amazon RDS para Oracle. Para obtener más información, consulte Uso de una base de datos de Oracle como fuente para AWS DMS.

Pila de tecnología de destino

- Amazon RDS para MySQL. Para obtener más información, consulte Uso de una base de datos compatible con MySQL como destino para AWS DMS.

Arquitectura de migración

En el siguiente diagrama, AWS SCT copia y convierte los objetos de esquema de la base de datos de origen de Amazon RDS for Oracle y envía los objetos a la base de datos de destino de Amazon RDS for MySQL. AWS DMS replica los datos de la base de datos de origen y los envía a la instancia de Amazon RDS for MySQL.

Herramientas

- AWS Data Migration Service le ayuda a migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones locales y en la nube.
- Amazon Relational Database Service (Amazon RDS) lo ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS. Este patrón utiliza Amazon RDS para Oracle y Amazon RDS para MySQL.
- La Herramienta de conversión de esquemas de AWS (AWS SCT) simplifica las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado, lo que incluye las vistas, los procedimientos almacenados y las funciones, a un formato compatible con la base de datos de destino.

Epics

Para preparar la migración

Tarea	Descripción	Habilidades requeridas
Valide las versiones de las bases de datos de origen y de destino.		Administrador de base de datos
Identifique los requisitos de hardware del servidor de destino.		DBA, SysAdmin
Identifique los requisitos de almacenamiento (como el tipo y la capacidad de almacenamiento).		DBA, SysAdmin

Tarea	Descripción	Habilidades requeridas
Elija el tipo de instancia de destino en función de la capacidad, las características de almacenamiento y las características de red.		DBA, SysAdmin
Identifique los requisitos de seguridad de acceso a la red de las bases de datos de origen y destino.		DBA, SysAdmin
Elija una estrategia de migración de aplicaciones.	Considere si desea un tiempo de inactividad total o parcial para las actividades en transición.	DBA, propietario de la SysAdmin aplicación

Configurar la infraestructura

Tarea	Descripción	Habilidades requeridas
Creación de una VPC y de subredes.		SysAdmin
Cree grupos de seguridad y listas de control de acceso (ACL) a la red.		SysAdmin
Configure e inicie la instancia de Amazon RDS para Oracle.		DBA, SysAdmin
Configure e inicie la instancia de Amazon RDS para MySQL.		DBA, SysAdmin

Tarea	Descripción	Habilidades requeridas
Prepare un caso de prueba para la validación de la conversión de código.	Esto ayudará a realizar pruebas unitarias para el código convertido.	Administrador de base de datos, desarrollador
Configure la instancia de AWS DMS.		
Configure los puntos de conexión de origen y destino en AWS DMS.		

Migrar datos

Tarea	Descripción	Habilidades requeridas
Generar el script de la base de datos de destino mediante AWS SCT.	Compruebe la precisión del código convertido por AWS SCT. Será necesario realizar algunos trabajos manuales.	Administrador de base de datos, desarrollador
En AWS SCT, elija la configuración “Sin distinción entre mayúsculas y minúsculas”.	En AWS SCT, elija Configuración del proyecto, Distinción entre mayúsculas y minúsculas del destino, Sin distinción entre mayúsculas y minúsculas.	Administrador de base de datos, desarrollador
En AWS SCT, opte por no utilizar la función nativa de Oracle.	En configuración del proyecto, compruebe las funciones TO_CHAR/TO_NUMBER/TO_DATE.	Administrador de base de datos, desarrollador
Realice cambios en el código “sql%notfound”.	Puede que tenga que convertir el código manualmente.	

Tarea	Descripción	Habilidades requeridas
Realice consultas sobre tablas y objetos en procedimientos almacenados (utilice consultas en minúsculas).		Administrador de base de datos, desarrollador
Cree el script principal después de realizar todos los cambios y, a continuación, impleméntelo en la base de datos de destino.		Administrador de base de datos, desarrollador
Realice pruebas unitarias de procedimientos almacenad os y llamadas a aplicaciones utilizando datos de muestra.		
Limpie los datos que se crearon durante las pruebas unitarias.		Administrador de base de datos, desarrollador
Elimine las restricciones de clave externa en la base de datos de destino.	Este paso es obligatorio para cargar los datos iniciales. Si no desea eliminar las restricci ones de clave externa, debe crear una tarea de migración para los datos específicos de las tablas principal y secundari a.	Administrador de base de datos, desarrollador
Coloque las claves principales y las claves únicas en la base de datos de destino.	Este paso da como resultado un mejor rendimiento para la carga inicial.	Administrador de base de datos, desarrollador
Habilitar el registro suplement ario en la base de datos de origen.		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree una tarea de migración para la carga inicial en AWS DMS y ejecútela.	Seleccione la opción de migrar datos existentes.	Administrador de base de datos
Añada las claves principales y las claves externas a la base de datos de destino.	Las restricciones deben añadirse después de la carga inicial.	Administrador de base de datos, desarrollador
Cree una tarea de migración para la replicación continua.	La replicación continua mantiene la base de datos de destino sincronizada con la base de datos de origen.	Administrador de base de datos

Migración de aplicaciones

Tarea	Descripción	Habilidades requeridas
Sustituya las funciones nativas de Oracle por funciones nativas de MySQL.		Propietario de la aplicación
Asegúrese de que solo se usen nombres en minúscula para los objetos de base de datos en las consultas SQL.		DBA, propietario de la SysAdmin aplicación

Realizar la transición a la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Apague el servidor de la aplicación.		Propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Valide que las bases de datos de origen y destino estén sincronizadas.		Administrador de base de datos, propietario de la aplicación
Detenga la instancia de base de datos de Amazon RDS para Oracle.		Administrador de base de datos
Detenga la tarea de migración.	Se detendrá automáticamente después de completar el paso anterior.	Administrador de base de datos
Cambie la conexión JDBC de Oracle a MySQL.		Administrador de base de datos, propietario de la aplicación
Inicie la aplicación.		DBA, propietario de la SysAdmin aplicación

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Revise y valide los documentos del proyecto.		DBA, SysAdmin
Recopile métricas como el tiempo de migración, el porcentaje de tareas manuales frente a las de la herramienta, el ahorro de costos, etc.		DBA, SysAdmin
Detenga y elimine las instancias de AWS DMS.		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Elimine los puntos de conexión de la base de datos de origen y de destino.		Administrador de base de datos
Elimine las tareas de migración.		Administrador de base de datos
Realice una instantánea de la instancia de base de datos de Amazon RDS para Oracle.		Administrador de base de datos
Elimine la instancia de base de datos de Amazon RDS para Oracle.		Administrador de base de datos
Cierre y elimine cualquier otro recurso temporal de AWS que haya utilizado.		DBA, SysAdmin
Cierre el proyecto y envíe sus comentarios.		Administrador de base de datos

Recursos relacionados

- AWS DMS
- AWS SCT
- Precios de Amazon RDS
- Introducción a AWS DMS
- Introducción a Amazon RDS

Migrar de IBM Db2 en Amazon EC2 a compatible con Aurora PostgreSQL mediante AWS DMS y AWS SCT

Creado por Sirsendu Halder (AWS) y Sachin Kotwal (AWS)

Entorno: PoC o piloto	Origen: IBM Db2	Destino: compatible con Aurora PostgreSQL
Tipo R: renovar arquitectura	Carga de trabajo: IBM	Tecnologías: migración; bases de datos
Servicios de AWS: Amazon Aurora; AWS DMS; AWS SCT		

Resumen

Este patrón proporciona orientación para migrar una base de datos de IBM Db2 de una instancia de Amazon Elastic Compute Cloud (Amazon EC2) a una instancia de base de datos de Edición compatible con Amazon Aurora PostgreSQL. Este patrón utiliza AWS Database Migration Service (AWS DMS) y Herramienta de conversión de esquemas de AWS (AWS SCT) para la migración de datos y la conversión de esquemas.

El patrón describe una estrategia de migración en línea con poco o ningún tiempo de inactividad para una base de datos IBM Db2 de varios terabytes que tiene un número elevado de transacciones. Le recomendamos que convierta las columnas de claves principales (primary keys, PK) y claves externas (foreign keys, FK) con el tipo de datos `NUMERIC` a `INT` o `BIGINT` en PostgreSQL para mejorar el rendimiento.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos IBM Db2 de origen en una instancia EC2

Versiones de producto

- DB2/LINUXX8664 versión 11.1.4.4 y posteriores

Arquitectura

Pila de tecnología de origen

- Una base de datos Db2 en una instancia EC2

Pila de tecnología de destino

- Una instancia de base de datos compatible con Aurora PostgreSQ versión 10.18 o instancia de base de datos posterior

Arquitectura de migración de base de datos

Herramientas

- AWS Database Migration Service (AWS DMS) ayuda a migrar los bases de datos a la nube de AWS o entre combinaciones de configuraciones en las instalaciones y en la nube. La base de datos de origen permanece totalmente operativa durante la migración, minimizando así el tiempo de inactividad de las aplicaciones que dependen de ella. Puede utilizar AWS DMS puede migrar sus datos desde y hasta las bases de datos comerciales y de código abierto más usadas. AWS DMS admite migraciones heterogéneas entre diferentes plataformas de bases de datos, como IBM Db2 a una versión 10.18 o posterior compatible con Aurora PostgreSQL. Para obtener más información, consulte Fuentes de migración de datos y Objetivos de migración de datos en la documentación de AWS DMS.
- Herramienta de conversión de esquemas de AWS (AWS SCT) ademite las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayor parte de los objetos de código de base de datos, incluidas las vistas, los procedimientos almacenados y las funciones, a un formato que sea compatible con la base de datos de destino. Los objetos que no se conviertan automáticamente se marcan claramente para que puedan convertirse manualmente con el objetivo de completar la migración. AWS SCT también puede analizar el código fuente de su aplicación en busca de instrucciones de SQL incrustadas y convertirlas.

Epics

Configurar el entorno

Tarea	Descripción	Habilidades requeridas
Crear una instancia de base de datos compatible con Aurora PostgreSQL.	Para crear una instancia de base de datos, siga las instrucciones de la documentación de AWS. Para engine type (Tipo de motor), elija Amazon Aurora. En edition (edición), seleccione Edición compatible con Amazon Aurora PostgreSQL. La instancia de base de datos de la versión 10.18 o posterior compatible con Aurora PostgreSQL debe estar en la misma nube privada virtual (VPC) que la base de datos de origen de IBM Db2.	Amazon RDS

Convertir su esquema de base de dato

Tarea	Descripción	Habilidades requeridas
Instalar y verificar AWS SCT.	1. Instale AWS SCT siguiendo los pasos de la documentación de AWS SCT. 2. Verifique la instalación siguiendo los procedimientos de la documentación de AWS SCT.	Administrador de AWS, administrador de base de datos, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
Inicie AWS SCT y cree un proyecto.	Para iniciar la herramienta AWS SCT y crear un nuevo proyecto para ejecutar un informe de evaluación de la migración de bases de datos, siga las instrucciones de la documentación de AWS SCT.	Ingeniero de migraciones
Añada servidores de bases de datos y cree una regla de asignación.	1. Añada servidores de bases de datos de origen y destino siguiendo las instrucciones de la documentación de AWS SCT. 2. Cree una regla de asignación para definir la plataforma de base de datos de destino para su base de datos de origen. Para obtener instrucciones, consulte la documentación de AWS SCT.	Ingeniero de migraciones
Crear un informe de evaluación de la migración de la base de datos.	Cree el informe de evaluación de la migración de la base de datos siguiendo los pasos de la documentación de AWS SCT.	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
Consultar del informe de evaluación.	Utilice la pestaña Resumen del informe de evaluación de la migración de la base de datos para ver el informe y analizar los datos. Este análisis le ayudará a determinar la complejidad de la migración. Para obtener más información, consulte la documentación de AWS SCT.	Ingeniero de migraciones
Convertir el esquema.	Para convertir su esquemas de base de datos de origen: 1. En la consola AWS SCT, elija Ver y, a continuación, Vista principal. 2. Seleccione el objeto o el nodo principal del esquema de origen, abra el menú contextual (haga clic con el botón derecho) y, a continuación, elija Convertir esquema. Para obtener más información, consulte la documentación de AWS SCT.	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
Aplicar el esquema de base de datos convertido a su instancia de base de datos de destino.	1. Seleccione el elemento del esquema del panel derecho del proyecto que indique el esquema previsto para su instancia de base de datos de destino. 2. Abra el menú contextual (clic con el botón secundario) del elemento del esquema y seleccione Aplicar a base de datos. Para obtener más información, consulte la documentación de AWS SCT.	Ingeniero de migraciones

Migrar datos

Tarea	Descripción	Habilidades requeridas
Configurar grupos de parámetros de base de datos y una VPC.	Configure grupos de parámetors de base de datos y una VPC, y configure las reglas y parámetros de entrada necesarios para la migración. Para obtener instrucciones, consulte la Documentación de AWS DMS. Para el grupo de seguridad de VPC, seleccione la instancia EC2 para Db2 y la instancia de base de datos compatible con Aurora PostgreSQL.	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	Esta instancia de replicación debe estar en la misma región que las instancias de base de datos de origen y de destino.	
Preparar las instancias de base de datos de origen y destino.	Prepare las instancias de base de datos de origen y destino para la migración. En un entorno de producción, la base de datos de origen ya existirá. En el caso de la base de datos de origen, el nombre del servidor debe ser el sistema de nombres de dominio (DNS) público de la instancia EC2 en la que se ejecuta Db2. Para el nombre de usuario, puede usar `db2inst1` seguido del puerto, que será 5000 para IBM Db2.	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
Crear un cliente y puntos de conexión de Amazon EC2.	1. Cree un cliente de Amazon EC2. Utilice este cliente para rellenar la base de datos de origen con datos que desee replicar. También utiliza este cliente para verificar la replicación mediante la ejecución de consultas en la base de datos de destino. 2. Cree puntos de conexión para la base de datos de origen y la instancia de base de datos de destino para utilizarlos en los siguientes pasos. Para obtener instrucciones, consulte la Documentación de AWS DMS. Debe crear puntos de conexión independientes para las bases de datos de origen y de destino. Para la versión 10.18 o posterior compatible con Aurora PostgreSQL, el puerto será 5432 y podrá obtener el nombre del servidor desde el punto de conexión de la instancia de base de datos.	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
Crear una instancia de replicación.	Cree una instancia de replicación mediante la consola de AWS DMS y especifique los puntos de conexión de origen y destino. La instancia de replicación realiza la migración de datos entre los puntos de conexión. Para obtener más información, consulte la documentación de AWS DMS.	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
Crear una tarea de AWS DMS para migrar los datos.	Cree una tarea para cargar las tablas de IBM Db2 de origen en la instancia de base de datos PostgreSQL de destino siguiendo los pasos de la documentación de AWS DMS. • Para el origen y el destino, utilice los nombres de los puntos de conexión de origen y destino. • El tipo de migración puede ser de carga completa. • Para la regla de esquema, puede usar el esquema `inst1` de la base de datos Db2. • Para el nombre de la tabla, especifique `%` si desea migrar todas las tablas. Cuando se complete la carga, verá que las tablas de Db2 del esquema `inst1` aparecen en la base de datos compatible con Aurora PostgreSQL.	Ingeniero de migraciones

Recursos relacionados

Referencias

- Documentación de Amazon Aurora
- Documentación del contenedor de datos externos (FDW) de PostgreSQL
- Documentación IMPORT FOREIGN SCHEMA de PostgreSQL

- Documentación de AWS DMS
- Documentación de AWS SCT

Tutoriales y videos

- Introducción a AWS DMS (guía)
- Introducción a Amazon EC2: Elastic Cloud Server y alojamiento con AWS (vídeo)

Migre de Oracle 8i o 9i a Amazon RDS para PostgreSQL mediante AWS DMS SharePlex

Creado por Kumar Babu P G (AWS)

Entorno: PoC o piloto	Origen: bases de datos: relacionales	Destino: Amazon RDS para PostgreSQL o Amazon Aurora (PostgreSQL).
Tipo R: renovar arquitectura	Carga de trabajo: Oracle	Tecnologías: migración; bases de datos
Servicios de AWS; Amazon RDS; Amazon Aurora		

Resumen

Este patrón describe cómo migrar una base de datos Oracle 8i o 9i en las instalaciones a una base de datos de Amazon Relational Database Service (Amazon RDS) para PostgreSQL o Amazon Aurora PostgreSQL. AWS Database Migration Service (AWS DMS) no admite Oracle 8i o 9i como fuente, por lo que Quest SharePlex replica los datos de una base de datos 8i o 9i local en una base de datos Oracle intermedia (Oracle 10g u 11g), que es compatible con AWS DMS.

Desde la instancia intermedia de Oracle, el esquema y los datos se migran a la base de datos PostgreSQL en AWS mediante la herramienta de conversión de esquemas de AWS (AWS SCT) y AWS DMS. Este método ayuda a lograr una transmisión continua de datos desde la base de datos Oracle de origen a la instancia de base de datos PostgreSQL de destino con un retraso de replicación mínimo. En esta implementación, el tiempo de inactividad se limita al tiempo que se tarda en crear o validar todas las claves, activadores y secuencias externas en la base de datos PostgreSQL de destino.

La migración utiliza una instancia de Amazon Elastic Compute Cloud (Amazon EC2) con Oracle 10g u 11g instalado para alojar los cambios de la base de datos de origen de Oracle. AWS DMS utiliza esta instancia intermedia de Oracle como fuente para transmitir los datos a Amazon RDS para PostgreSQL o Aurora PostgreSQL. La replicación de datos se puede pausar y reanudar desde la base de datos Oracle en las instalaciones a la instancia intermedia de Oracle. También se puede pausar y reanudar desde la instancia intermedia de Oracle hasta la base de datos PostgreSQL

de destino para que pueda validar los datos mediante la validación de datos de AWS DMS o una herramienta de validación de datos personalizada.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una base de datos Oracle 8i o 9i de origen en un centro de datos en las instalaciones
- AWS Direct Connect, configurado entre el centro de datos en las instalaciones y AWS
- Controladores de conectividad de bases de datos Java (JDBC) para conectores SCT de AWS instalados en una máquina local o en la instancia EC2 en la que está instalado AWS SCT
- Uso de una base de datos de Oracle como origen para AWS DMS
- Uso de una base de datos de PostgreSQL como destino para AWS DMS
- Familiaridad con la replicación de datos de Quest SharePlex

Limitaciones

- El límite de tamaño de la base de datos es de 64 TB
- La base de datos Oracle en las instalaciones debe ser Enterprise Edition

Versiones de producto

- Oracle 8i o 9i para la base de datos de origen
- Oracle 10g o 11g para la base de datos intermedia
- PostgreSQL 9.6 o posterior

Arquitectura

Pila de tecnología de origen

- Base de datos Oracle 8i o 9i
- Quest SharePlex

Pila de tecnología de destino

- Amazon RDS para PostgreSQL o Amazon Aurora PostgreSQL.

Arquitectura de origen y destino

Herramientas

- AWS DMS – AWS Database Migration Service (AWS DMS) ayuda a migrar los datos de forma rápida y segura a AWS. La base de datos de origen puede permanecer totalmente operativa durante la migración, minimizando así el tiempo de inactividad de las aplicaciones que dependen de ella. AWS DMS puede migrar sus datos desde y hasta las bases de datos comerciales y de código abierto más usadas.
- AWS SCT – La herramienta de conversión de esquemas de AWS (AWS SCT) simplifica las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado, incluidas las vistas, los procedimientos almacenados y las funciones, a un formato compatible con la base de datos de destino. Los objetos que no se conviertan automáticamente se marcan claramente para poder convertirlos manualmente con el objetivo de completar la migración. AWS SCT también puede analizar el código fuente de su aplicación en busca de instrucciones de SQL incrustadas y convertirlas como parte de un proyecto de conversión de esquemas de bases de datos. Durante este proceso, AWS SCT optimiza el código nativo en la nube al convertir las funciones heredadas de Oracle y SQL Server en sus equivalentes de AWS, para ayudarlo a modernizar sus aplicaciones mientras migra sus bases de datos. Una vez finalizada la conversión del esquema, AWS SCT puede ayudar a migrar datos de una variedad de almacenamiento de datos a Amazon Redshift mediante el uso de agentes de migración de datos integrados.
- Quest SharePlex: Quest SharePlex es una herramienta de replicación de datos de Oracle a Oracle para mover datos con un tiempo de inactividad mínimo y sin pérdida de datos.

Epics

Crear una instancia EC2 e instalar Oracle

Tarea	Descripción	Habilidades requeridas
Configure la red para Amazon EC2.	Creación de la nube privada virtual (VPC), subredes, puerta de enlace de Internet, tablas de enrutamiento y grupos de seguridad.	AWS SysAdmin
Crear la nueva instancia EC2	Seleccione la imagen de máquina de Amazon (AMI) para las instancia EC2. Elija el tamaño de la instancia y configura los detalles de la instancia: la cantidad de instancias (1), la VPC y la subred del paso anterior, la asignación automática de la IP pública y otras opciones. Agregue almacenamiento, configure grupos de seguridad y lance la instancia. Cuando se le pida, cree y guarde un par de claves para el siguiente paso.	AWS SysAdmin
Instale Oracle en la instancia EC2.	Adquiera las licencias y los binarios de Oracle necesarios e instale Oracle 10g u 11g en la instancia EC2.	Administrador de base de datos

Configure SharePlex en una instancia EC2 y configure la replicación de datos

Tarea	Descripción	Habilidades requeridas
Configurar. SharePlex	Cree una instancia de Amazon EC2 e instale los SharePlex binarios que sean compatibles con Oracle 8i o 9i.	AWS SysAdmin, administrador de bases de datos
Configure la replicación de datos.	Siga las prácticas SharePlex recomendadas para configura r la replicación de datos desde una base de datos Oracle 8i/9i local a una instancia Oracle 10g/11g.	Administrador de base de datos

Convertir el esquema de base de datos Oracle a PostgreSQL

Tarea	Descripción	Habilidades requeridas
Configure AWS SCT.	Cree un informe nuevo y, a continuación, conéctese a Oracle como origen y a PostgreSQL como destino. En la configuración del proyecto, abra la pestaña SQL Scripting y cambie el script SQL de destino a Varios archivos.	Administrador de base de datos
Convertir el esquema de base de datos Oracle.	En la pestaña Acción, elija Generar informe, Convertir esquema y, a continuación, Guardar como SQL.	Administrador de base de datos
Modifique los scripts SQL generados por AWS SCT.		Administrador de base de datos

Creación y configuración de la instancia de base de datos de Amazon RDS

Tarea	Descripción	Habilidades requeridas
Creación de una instancia de base de datos de Amazon RDS	En la consola de Amazon RDS, cree una nueva instancia de base de datos PostgreSQL.	AWS SysAdmin, administrador de bases de datos
Configure la instancia de base de datos.	Especifique la versión del motor de base de datos, la clase de instancia de base de datos, la implement ación Multi-AZ, el tipo de almacenamiento y el almacenamiento asignado. Introduzca el identificador de la instancia de base de datos, un nombre de usuario maestro y una contraseña maestra.	AWS SysAdmin, administrador de bases de datos
Configurar la red y la seguridad.	Especifique la VPC, el grupo de subredes, la accesibilidad pública, la preferencia de zona de disponibilidad y los grupos de seguridad.	AWS SysAdmin, administrador de bases de datos
Configurar las opciones de la base de datos.	Especifique el nombre, el puerto, el grupo de parámetro s, el cifrado y la clave maestra de la base de datos.	AWS SysAdmin, administrador de bases de datos
Configure copias de seguridad .	Especifique el período de retención de la copia de seguridad, la ventana de copia de seguridad, la hora de inicio, la duración y si desea copiar	AWS SysAdmin, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	las etiquetas a las instantán eas.	
Configure las opciones de monitoreo.	Habilite y desactive la monitorización mejorada de información sobre rendimien to.	AWS SysAdmin, administrador de bases de datos
Configurar las opciones de mantenimiento.	Especifique la actualización automática de la versión secundaria, el período de mantenimiento y el día, la hora y la duración de inicio.	AWS SysAdmin, administrador de bases de datos
Ejecute los scripts previos a la migración desde AWS SCT.	En la instancia de Amazon RDS, ejecute los siguientes scripts: reate_database.sql , create_sequence.sql, create_table.sql, create_vi ew.sql y create_function.sql.	AWS SysAdmin, administrador de bases de datos

Migre los datos mediante AWS DMS

Tarea	Descripción	Habilidades requeridas
Cree una instancia de replicaci ón en AWS DMS.	Complete los campos para el nombre, la clase de instancia , la VPC (igual que para la instancia EC2), la zona de disponibilidad múltiple y la accesibilidad pública. En la sección de configuración avanzada, especifique el almacenamiento asignado, el grupo de subredes, la zona de	AWS SysAdmin, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	disponibilidad, los grupos de seguridad de VPC y la clave raíz de AWS Key Managemen t Service (AWS KMS).	
Cree el punto de conexión de origen de la base de datos.	Especifique el nombre del punto de conexión, el tipo, el motor de origen (Oracle), el nombre del servidor (nombre de DNS privado de Amazon EC2), el puerto, el modo SSL, el nombre de usuario, la contraseña, el SID, la VPC (especifique la VPC que tiene la instancia de replicación) y la instancia de replicaci ón. Para probar la conexión, seleccione Run Test (Ejecutar prueba) y, a continuación, cree el punto de conexión. También puede configurar los siguientes ajustes avanzados : maxFileSize y numberDat aType Scale.	AWS SysAdmin, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
Cree una tarea de replicación de AWS DMS.	Especifique el nombre de la tarea, la instancia de replicación, los puntos de conexión de origen y destino y la instancia de replicaci ón. Para tipo de migración, seleccione la opción «Migrate existing data and replication ongoing changes» (Migrar datos existentes y cambios de replicación en curso). Desactive la casilla de verificación «Start task on create» (Iniciar la tarea al crearla).	AWS SysAdmin, administrador de bases de datos
Configure la configuración de la tarea de replicación de AWS DMS.	Para el modo de preparaci ón de la tabla de destino, elija «Do nothing» (No hacer nada). Detenga la tarea cuando se complete la carga completa para crear las claves principales. Especifique el modo LOB limitado o completo y habilite las tablas de control. Si lo desea, puede configurar la configuración CommitRate avanzada.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Configure las asignaciones de tablas.	En la sección Mapeos de tablas, cree una regla de Inclusión para todas las tablas de todos los esquemas incluidos en la migración y, a continuación, cree una regla de Exclusión. Agregue tres reglas de transformación para convertir los nombres del esquema, la tabla y las columnas a minúsculas y añada cualquier otra regla necesaria para esta migración específica.	Administrador de base de datos
Iniciar la tarea.	Iniciar la tarea de replicación. Asegúrese de que la carga completa está ejecutando. Ejecute ALTER SYSTEM SWITCH LOGFILE en la base de datos principal de Oracle para iniciar la tarea.	Administrador de base de datos
Ejecute los scripts de la migración intermedia desde AWS SCT.	En Amazon RDS para PostgreSQL, ejecute los siguientes scripts: create_index.sql y create_constraint.sql.	Administrador de base de datos
Reinicie la tarea para continuar con la captura de datos de cambio (CDC).	Ejecute VACUUM en la instancia de base de datos Amazon RDS para PostgreSQL y reinicie la tarea de AWS DMS para aplicar los cambios de CDC en caché.	Administrador de base de datos

Realizar la transición a la base de datos de PostgreSQL

Tarea	Descripción	Habilidades requeridas
Consulte los registros y las tablas de metadatos de AWS DMS.	Valide cualquier error y corríjalo si es necesario.	Administrador de base de datos
Detenga todas las dependencias de Oracle.	Cierre los oyentes de la base de datos de Oracle y ejecute ALTER SYSTEM SWITCH LOGFILE. Detenga la tarea de AWS DMS cuando no muestre actividad.	Administrador de base de datos
Ejecute los scripts posteriores a la migración desde AWS SCT.	En Amazon RDS para PostgreSQL, ejecute los siguientes scripts: create_foreign_key_constraint.sql y create_triggers.sql.	Administrador de base de datos
Complete los pasos adicionales de Amazon RDS para PostgreSQL.	Aumente las secuencias para que coincidan con las de Oracle si es necesario, ejecute VACUUM y ANALYZE y tome una instantánea para comprobar la conformidad.	Administrador de base de datos
Abra las conexiones hacia Amazon RDS para PostgreSQL.	Elimine los grupos de seguridad de AWS DMS de Amazon RDS para PostgreSQL, añada grupos de seguridad de producción y dirija sus aplicaciones a la nueva base de datos.	Administrador de base de datos
Limpie los recursos de AWS DMS.	Elimine los puntos de conexión, las tareas de	SysAdmin, DBA

Tarea	Descripción	Habilidades requeridas
	replicación, las instancias de replicación y la instancia EC2.	

Recursos relacionados

- Documentación de AWS DMS
- Documentación de AWS SCT
- Precio de Amazon RDS para PostgreSQL
- Uso de una base de datos de Oracle como origen para AWS DMS
- Uso de una base de datos de PostgreSQL como destino para AWS DMS
- Documentación de Quest SharePlex

Migre de Oracle 8i o 9i a Amazon RDS para PostgreSQL mediante la vista materializada y AWS DMS

Creado por Kumar Babu P G (AWS) y Pragnesh Patel (AWS)

Entorno: PoC o piloto	Origen: Oracle 8i o 9i	Destino: una base de datos compatible con Amazon RDS para PostgreSQL o Aurora PostgreSQL
Tipo R: renovar arquitectura	Carga de trabajo: Oracle	Tecnologías: migración; bases de datos
Servicios de AWS; Amazon RDS; Amazon Aurora		

Resumen

Este patrón describe cómo migrar una base de datos Oracle 8i o 9i en las instalaciones a una base de datos de Amazon Relational Database Service (Amazon RDS) para PostgreSQL o para una edición compatible de Amazon Aurora PostgreSQL.

AWS Database Migration Service (AWS DMS) no admite Oracle 8i o 9i como fuente, por lo que este patrón utiliza una instancia de base de datos Oracle intermedia que es compatible con AWS DMS, como Oracle 10g u 11g. También utiliza la característica de vistas materializadas para migrar los datos de la instancia 8i/9i de origen de Oracle a la instancia intermedia 10g/11g de Oracle.

La Herramienta de conversión de esquemas de AWS (AWS SCT) convierte el esquema de la base de datos y AWS DMS migra los datos a la base de datos PostgreSQL de destino.

Este patrón ayuda a los usuarios que desean migrar desde bases de datos Oracle heredadas con un tiempo de inactividad mínimo. En esta implementación, el tiempo de inactividad se limita al tiempo que se tarda en crear o validar todas las claves externas, activadores y secuencias en la base de datos de destino.

El patrón utiliza instancias de Amazon Elastic Compute Cloud (Amazon EC2) con una base de datos Oracle 10g/11g instalada para ayudar con la transmisión de datos a través de AWS DMS. Puede pausar temporalmente la replicación del streaming desde la base de datos Oracle en las

instalaciones a una instancia de Oracle para activar AWS DMS y ponerse al día con la validación de datos o para utilizar otra herramienta de validación de datos. La instancia de base de datos PostgreSQL y la base de datos intermedia de Oracle tendrán los mismos datos cuando AWS DMS haya terminado de migrar los cambios actuales.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una base de datos Oracle 8i o 9i de origen en un centro de datos en las instalaciones
- AWS Direct Connect, configurado entre el centro de datos en las instalaciones y AWS
- Controladores de conectividad de bases de datos Java (JDBC) para conectores SCT de AWS instalados en una máquina local o en la instancia EC2 en la que está instalado AWS SCT
- Uso de una base de datos de Oracle como origen para AWS DMS
- Uso de una base de datos de PostgreSQL como destino para AWS DMS

Limitaciones

- El límite de tamaño de la base de datos es de 64 TB

Versiones de producto

- Oracle 8i o 9i para la base de datos de origen
- Oracle 10g o 11g para la base de datos intermedia
- PostgreSQL 10.17 o posterior

Arquitectura

Pila de tecnología de origen

- Base de datos Oracle 8i o 9i

Pila de tecnología de destino

- Amazon RDS para PostgreSQL o Aurora PostgreSQL compatibles

Arquitectura de destino

Herramientas

- AWS DMS ayuda a migrar las bases de datos de forma rápida y segura. La base de datos de origen puede permanecer totalmente operativa durante la migración, minimizando así el tiempo de inactividad de las aplicaciones que dependen de ella. AWS DMS puede migrar sus datos desde y hasta las bases de datos comerciales y de código abierto más usadas.
- AWS SCT ayuda a convertir automáticamente el esquema de la base de datos de origen y la mayor parte de los objetos de código de la base de datos, incluidas las vistas, los procedimientos almacenados y las funciones, a un formato compatible con la base de datos de destino. Los objetos que no se conviertan automáticamente se marcan claramente para que puedan convertirse manualmente con el objetivo de completar la migración. AWS SCT también puede analizar el código fuente de su aplicación en busca de instrucciones de SQL incrustadas y convertirlas como parte de un proyecto de conversión de esquemas de bases de datos. Durante este proceso, AWS SCT optimiza el código nativo en la nube al convertir las funciones heredadas de Oracle y SQL Server en sus equivalentes de AWS, para ayudarlo a modernizar sus aplicaciones mientras migra sus bases de datos. Una vez finalizada la conversión del esquema, AWS SCT puede ayudar a migrar datos de una variedad de almacenamiento de datos a Amazon Redshift mediante el uso de agentes de migración de datos integrados.

Prácticas recomendadas

Para conocer las prácticas recomendadas para actualizar las vistas materializadas, consulte la siguiente documentación de Oracle:

- Actualización de vistas materializadas
- Actualización rápida para vistas materializadas

Epics

Instale Oracle en una instancia EC2 y cree vistas materializadas

Tarea	Descripción	Habilidades requeridas
Configure la red para la instancia EC2.	Creación de la nube privada virtual (VPC), subredes, puerta de enlace de Internet, tablas de enrutamiento y grupos de seguridad.	AWS SysAdmin
Crear la instancia EC2.	Seleccione la imagen de máquina de Amazon (AMI) para las instancia EC2. Elija el tamaño de la instancia y configura los detalles de la instancia: la cantidad de instancias (1), la VPC y la subred del paso anterior, la asignación automática de la IP pública y otras opciones. Agregue almacenamiento, configure grupos de seguridad y lance la instancia. Cuando se le pida, cree y guarde un par de claves para el siguiente paso.	AWS SysAdmin
Instale Oracle en la instancia EC2.	Adquiera las licencias y los binarios de Oracle necesarios e instale Oracle 10g u 11g en la instancia EC2.	Administrador de base de datos
Configure las redes de Oracle.	Modifique o añada entradas en `listener.ora` para conectarse a la base de datos Oracle 8i/9i de origen en las	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	instalaciones y, a continuación, cree los enlaces de la base de datos.	
Creación de vistas materializadas	Identifique los objetos de la base de datos que desee replicar en la base de datos Oracle 8i/9i de origen y, a continuación, cree vistas materializadas de todos los objetos mediante el enlace a la base de datos.	Administrador de base de datos
Implemente scripts para actualizar las vistas materializadas a los intervalos necesarios.	Desarrolle e implemente scripts para actualizar las vistas materializadas a los intervalos requeridos en la instancia Amazon EC2 Oracle 10g/11g. Utilice la opción de actualización incremental para refrescar las vistas materializadas.	Administrador de base de datos

Convertir el esquema de base de datos Oracle a PostgreSQL

Tarea	Descripción	Habilidades requeridas
Configure AWS SCT.	Cree un informe nuevo y, a continuación, conéctese a Oracle como origen y a PostgreSQL como destino. En la Configuración del proyecto, vaya a la pestaña SQL Scripting. Cambie el Script SQL de destino a	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Multiple Files (Varios archivos) . (AWS SCT no es compatibl e con las bases de datos Oracle 8i/9i, por lo que debe restaurar el volcado exclusivo del esquema en la instancia intermedia de Oracle 10g/11g y usarlo como fuente para AWS SCT).	
Convertir el esquema de base de datos Oracle.	En la pestaña Action (Acción), elija Generate Report (Generar informe), Convert Schema (Convertir esquema) y, a continuación, Save as SQL (Guardar como SQL).	Administrador de base de datos
Modifique los scripts SQL.	Realice las modificaciones en función de las mejores prácticas. Por ejemplo, cambie a los tipos de datos adecuados y desarrolle equivalentes de PostgreSQL para funciones específicas de Oracle.	Administrador de base de datos, DevDBA

Creación y configuración de la instancia de base de datos de Amazon RDS para alojar la base de datos convertida

Tarea	Descripción	Habilidades requeridas
Creación de una instancia de base de datos de Amazon RDS	En la consola de Amazon RDS, cree una nueva instancia de base de datos PostgreSQL.	AWS SysAdmin, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
Configure la instancia de base de datos.	Especifique la versión del motor de base de datos, la clase de instancia de base de datos, la implement ación Multi-AZ, el tipo de almacenamiento y el almacenamiento asignado. Introduzca el identificador de la instancia de base de datos, un nombre de usuario maestro y una contraseña maestra.	AWS SysAdmin, administrador de bases de datos
Configurar la red y la seguridad.	Especifique la VPC, el grupo de subredes, la accesibilidad pública, la preferencia de zona de disponibilidad y los grupos de seguridad.	DBA, SysAdmin
Configurar las opciones de la base de datos.	Especifique el nombre, el puerto, el grupo de parámetro s, el cifrado y la clave maestra de la base de datos.	ADMINISTRADOR DE BASES DE DATOS (DBA), AWS SysAdmin
Configure copias de seguridad .	Especifique el período de retención de la copia de seguridad, la ventana de copia de seguridad, la hora de inicio, la duración y si desea copiar las etiquetas a las instantán eas.	AWS SysAdmin, administrador de bases de datos
Configure las opciones de monitoreo.	Habilite y desactive la monitorización mejorada de información sobre rendimien to.	AWS SysAdmin, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
Configurar las opciones de mantenimiento.	Especifique la actualización automática de la versión secundaria, el período de mantenimiento y el día, la hora y la duración de inicio.	AWS SysAdmin, administrador de bases de datos
Ejecute los scripts previos a la migración desde AWS SCT.	En la instancia de Amazon RDS para PostgreSQL de destino, cree el esquema de base de datos mediante los scripts SQL de AWS SCT con otras modificaciones. Estas pueden incluir la ejecución de varios scripts e incluir la creación de usuarios, la creación de bases de datos, la creación de esquemas, tablas, vistas, funciones y otros objetos de código.	AWS SysAdmin, administrador de bases de datos

Migre los datos mediante AWS DMS

Tarea	Descripción	Habilidades requeridas
Cree una instancia de replicación en AWS DMS.	Complete los campos para el nombre, la clase de instancia, la VPC (igual que para la instancia EC2), la zona de disponibilidad múltiple y la accesibilidad pública. En la configuración avanzada, especifique el almacenamiento asignado, el grupo de subredes, la zona de disponibi	AWS SysAdmin, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	lidad, los grupos de seguridad de VPC y la clave de AWS Key Management Service (AWS KMS).	
Cree el punto de conexión de origen de la base de datos.	Especifique el nombre del punto de conexión, el tipo, el motor de origen (Oracle), el nombre del servidor (nombre de instancia privada de Amazon EC2), el puerto, el modo SSL, el nombre de usuario, la contraseña, el SID, la VPC (especifique la VPC que tiene la instancia de replicación) y la instancia de replicación. Para probar la conexión, seleccione Ejecutar prueba y, a continuación, cree el punto de conexión. También puede configurar los siguientes ajustes avanzados : maxFileSizey numberDat aTypeScale.	AWS SysAdmin, administrador de bases de datos
Conecte AWS DMS a Amazon RDS para PostgreSQL.	Cree un grupo de seguridad de migración para las conexiones entre las VPC, si su base de datos PostgreSQL está en otra VPC.	AWS SysAdmin, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
Cree puntos de conexión de base de datos de destino.	Especifique el nombre del punto de conexión, el tipo, el motor de origen (PostgreSQL), el nombre del servidor (punto de conexión de Amazon RDS), el puerto, el modo SSL, el nombre de usuario, la contraseña, el nombre de la base de datos, la VPC (especifique la VPC que tiene la instancia de replicación) y la instancia de replicación. Para probar la conexión, seleccione Ejecutar prueba y, a continuación, cree el punto de conexión. También puede configurar los siguientes ajustes avanzados: maxFileSizey numberDataTypeScale.	AWS SysAdmin, administrador de bases de datos
Cree una tarea de replicación de AWS DMS.	Especifique el nombre de la tarea, la instancia de replicación, los puntos de conexión de origen y destino y la instancia de replicación. Para tipo de migración, seleccione la opción Migrate existing data and replication ongoing changes (Migrar datos existentes y cambios de replicación en curso). Desactive la casilla Start task on create (Iniciar la tarea al crearla).	AWS SysAdmin, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
Configure la configuración de la tarea de replicación de AWS DMS.	Para el modo de preparación de la tabla de destino, elija No hacer nada. Detenga la tarea cuando se complete la carga completa para crear las claves principales. Especifique el modo LOB limitado o completo y habilite las tablas de control. Si lo desea, puede configura r la configuración CommitRat eavanzada.	Administrador de base de datos
Configure las asignaciones de tablas.	En la sección Table mappings (Mapeos de tabla), cree una regla de inclusión para todas las tablas de todos los esquemas incluidos en la migración y, a continuación, cree una regla de exclusión . Agregue tres reglas de transformación para convertir los nombres del esquema, la tabla y las columnas a minúsculas y añada cualquier otra regla necesaria para esta migración específica.	Administrador de base de datos
Iniciar la tarea.	Iniciar la tarea de replicación. Asegúrese de que la carga completa está ejecutand o. Ejecute `ALTER SYSTEM SWITCH LOGFILE` en la base de datos principal de Oracle para iniciar la tarea.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Ejecute los scripts de la migración intermedia desde AWS SCT.	En Amazon RDS para PostgreSQL, ejecute los siguientes scripts: `create_index.sql` y `create_constraint.sql` (si el esquema completo no se creó inicialmente).	Administrador de base de datos
Reanude la tarea para continuar con la captura de datos de cambio (CDC).	Ejecute `VACUUM` en la instancia de base de datos Amazon RDS para PostgreSQL y reinicie la tarea de AWS DMS para aplicar los cambios de CDC en caché.	Administrador de base de datos

Realizar la transición a la base de datos de PostgreSQL

Tarea	Descripción	Habilidades requeridas
Consulte los registros y las tablas de validación de AWS DMS.	Compruebe y corrija cualquier error de replicación o validación.	Administrador de base de datos
Deje de utilizar la base de datos de Oracle en las instalaciones y sus dependencias.	Detenga todas las dependencias de Oracle, cierre los oyentes de la base de datos de Oracle y ejecute `ALTER SYSTEM SWITCH LOGFILE`. Detenga la tarea de AWS DMS cuando no muestre actividad.	Administrador de base de datos
Ejecute los scripts posteriores a la migración desde AWS SCT.	En Amazon RDS para PostgreSQL, ejecute estos scripts: `create_fo`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`reign_key_constrai nt.sql and create_tr iggers.sql` . Asegúrese de que las secuencias estén actualizadas.	
Complete los pasos adicional es de Amazon RDS para PostgreSQL.	Aumente las secuencias para que coincidan con las de Oracle si es necesario, ejecute `VACUUM` y ANALYZE y `ANALYZE`, y tome una instantánea para comprobar la conformidad.	Administrador de base de datos
Abra las conexiones hacia Amazon RDS para PostgreSQ L.	Elimine los grupos de seguridad de AWS DMS de Amazon RDS para PostgreSQ L, añada grupos de seguridad de producción y dirija sus aplicaciones a la nueva base de datos.	Administrador de base de datos
Limpie los objetos de AWS DMS.	Elimine los puntos de conexión, las tareas de replicación, las instancias de replicación y la instancia EC2.	SysAdmin, DBA

Recursos relacionados

- Documentación de AWS DMS
- Documentación de AWS SCT
- Precio de Amazon RDS para PostgreSQL
- Uso de una base de datos de Oracle como origen para AWS DMS
- Uso de una base de datos de PostgreSQL como destino para AWS DMS

Migración de Oracle en Amazon EC2 a Amazon RDS para MySQL con AWS DMS y AWS SCT

Creado por Anil Kunapareddy (AWS) y Harshad Gohil

Entorno: PoC o piloto	Origen: bases de datos: relacionales	Destino: Amazon RDS para MySQL
Tipo R: renovar arquitectura	Carga de trabajo: Oracle	Tecnologías: migración; bases de datos
Servicios de AWS: Amazon RDS		

Resumen

La administración de bases de datos de Oracle en instancias de Amazon Elastic Compute Cloud (Amazon EC2) requiere recursos y puede resultar costosa. Mover estas bases de datos a una instancia de base de datos de Amazon Relational Database Service (Amazon RDS) para MySQL le facilitará el trabajo al optimizar el presupuesto global de TI. Amazon RDS para MySQL también ofrece funciones como Multi-AZ, escalabilidad y copias de seguridad automáticas.

Este patrón le guía a través de la migración de una base de datos de Oracle de origen en Amazon EC2 a una instancia de base de datos Amazon RDS para MySQL de destino. Utiliza AWS Database Migration Service (AWS DMS) para migrar los datos y la Herramienta de conversión de esquemas de AWS (AWS SCT) para convertir el esquema y los objetos de la base de datos de origen a un formato compatible con Amazon RDS para MySQL.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos fuente con servicios de instancia y escucha en ejecución, en modo ARCHIVELOG
- Una base de datos Amazon RDS para MySQL de destino, con suficiente almacenamiento para la migración de datos

Limitaciones

- AWS DMS no crea un esquema en la base de datos de destino; debe hacerlo usted. El nombre de esquema ya tiene que existir para el destino. Las tablas del esquema de origen se importan al usuario o esquema que AWS DMS utiliza para conectarse a la instancia de destino. Debe crear varias tareas de replicación si tiene que migrar varios esquemas.

Versiones de producto

- Todas las ediciones de las bases de datos de Oracle para las versiones 10.2 y posteriores, 11g y versiones posteriores a la 12.2 y 18c. Para ver la lista actualizada de versiones compatibles, consulte Uso de una base de datos de Oracle como fuente para AWS DMS y Uso de una base de datos compatible con MySQL como destino para AWS DMS. Le recomendamos utilizar la versión más reciente de AWS DMS para obtener el soporte más completo de versiones y características. Para obtener información sobre las versiones de bases de datos de Oracle compatibles con AWS SCT, consulte la documentación de AWS SCT.
- AWS DMS es compatible con las versiones 5.5, 5.6 y 5.7 de MySQL.

Arquitectura

Pila de tecnología de origen

- Una base de datos de Oracle en una instancia EC2

Pila de tecnología de destino

- Instancia de base de datos de Amazon RDS para MySQL

Arquitectura de migración de datos

Arquitectura de origen y destino

Herramientas

- AWS DMS: AWS Database Migration Service (AWS DMS) es un servicio web que puede utilizar para migrar datos de una base de datos en las instalaciones, de una instancia de base de datos de Amazon RDS o de una base de datos de una instancia EC2 a una base de datos de un servicio de AWS, como Amazon RDS para MySQL o una instancia EC2. Puede también migrar desde una base de datos de un servicio de AWS a otra base de datos local. Puede migrar datos entre motores de bases de datos heterogéneos u homogéneos.
- AWS SCT: la herramienta de conversión de esquemas de AWS (AWS SCT) hace más predecible las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado, incluidas las vistas, los procedimientos almacenados y las funciones, a un formato compatible con la base de datos de destino. Tras convertir el esquema de la base de datos y los objetos de código mediante AWS SCT, puede utilizar AWS DMS para migrar los datos de la base de datos de origen a la base de datos de destino para completar sus proyectos de migración.

Epics

Planificación de la migración

Tarea	Descripción	Habilidades requeridas
Identifique las versiones y motores de la base de datos de origen y destino.		Administrador de base de datos/desarrollador
Identifique la instancia de replicación de DMS.		Administrador de base de datos/desarrollador
Identifique los requisitos de almacenamiento, como el tipo y la capacidad de almacenam iento.		Administrador de base de datos/desarrollador
Identifique los requisitos de la red, como la latencia y el ancho de banda.		Administrador de base de datos/desarrollador

Tarea	Descripción	Habilidades requeridas
Identifique los requisitos de hardware para las instancia s del servidor de origen y destino (según la lista de compatibilidad de Oracle y los requisitos de capacidad).		Administrador de base de datos/desarrollador
Identifique requisitos de seguridad para acceder a la red de las bases de datos de origen y destino.		Administrador de base de datos/desarrollador
Instale los controladores AWS SCT y Oracle.		Administrador de base de datos/desarrollador
Determine una estrategia de copia de seguridad.		Administrador de base de datos/desarrollador
Determine los requisitos de disponibilidad.		Administrador de base de datos/desarrollador
Identifique la estrategia de migración y cambio de aplicaciones.		Administrador de base de datos/desarrollador
Seleccione el tipo de instancia de base de datos adecuado en función de la capacidad , el almacenamiento y las características de la red.		Administrador de base de datos/desarrollador

Configure el entorno

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC). El origen, el destino y la instancia de replicación deben estar en la misma VPC. También es bueno tenerlos en la misma zona de disponibilidad.		Desarrollador
Cree los grupos de seguridad necesarios para el acceso a la base de datos.		Desarrollador
Genere y configure un par de claves.		Desarrollador
Configure las subredes, las zonas de disponibilidad y los bloques CIDR.		Desarrollador

Configure la fuente: base de datos de Oracle en una instancia EC2

Tarea	Descripción	Habilidades requeridas
Instale Oracle Database en Amazon EC2 con los usuarios y roles necesarios.		Administrador de base de datos
Realice los tres pasos de la siguiente columna para acceder a Oracle desde fuera de la instancia EC2.	1. Cambie el host local en `tnsnames` al DNS público de Amazon EC2. 2. Cambie el host local en `listener` al DNS público de Amazon EC2.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	3. Detenga y vuelva a iniciar el oyente.	
Cuando se reinicia Amazon EC2, el DNS público cambia. Asegúrese de actualizar el DNS público de Amazon EC2 en “tnsnames” y “listener ” o utilice una dirección IP elástica.		Administrador de base de datos/desarrollador
Configure el grupo de seguridad de la instancia de EC2 para que la instancia de replicación y los clientes necesarios puedan acceder a la base de datos de origen.		Administrador de base de datos/desarrollador

Configure el destino: Amazon RDS para MySQL

Tarea	Descripción	Habilidades requeridas
Configure e inicie la instancia de base de datos de Amazon RDS para MySQL.		Desarrollador
Cree el espacio de tablas necesario en la instancia de base de datos de Amazon RDS para MySQL.		Administrador de base de datos
Configure el grupo de seguridad para que la instancia de replicación y los clientes necesarios puedan		Desarrollador

Tarea	Descripción	Habilidades requeridas
acceder a la base de datos de destino.		

Configure AWS SCT y cree un esquema en la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Instale los controladores AWS SCT y Oracle.		Desarrollador
Introduzca los parámetros adecuados y conéctese a la fuente y al destino.		Desarrollador
Genere un informe de conversión de esquemas.		Desarrollador
Corrija el código y el esquema según sea necesario, especialmente los espacios de tabla y las comillas, y ejecútelos en la base de datos de destino.		Desarrollador
Valide el esquema en el origen y en el destino antes de migrar los datos.		Desarrollador

Migración de datos utilizando AWS DMS

Tarea	Descripción	Habilidades requeridas
Para carga completa y la captura de datos de cambios (CDC) o simplemente para		Desarrollador

Tarea	Descripción	Habilidades requeridas
CDC, debe configurar un atributo de conexión adicional.		
Al usuario especificado en las definiciones de la base de datos de Oracle de origen de AWS DMS se le deben conceder todos los privilegios necesarios. Para ver una lista completa, consulte https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Source.Oracle.html#CHAP_Source.Oracle.Self-Managed.		Administrador de base de datos/desarrollador
Habilitar el registro suplementario en la base de datos de origen.		Administrador de base de datos/desarrollador
Para la captura completa de datos y cambios (CDC) o simplemente CDC, habilite el modo ARCHIVELOG en la base de datos de origen.		Administrador de base de datos
Cree puntos de conexión de origen y destino y pruebe las conexiones.		Desarrollador
Cuando los puntos de conexión estén conectados correctamente, cree una tarea de replicación.		Desarrollador

Tarea	Descripción	Habilidades requeridas
Seleccione solo CDC (o) carga completa más CDC en la tarea para capturar los cambios para la replicación continua únicamente (o) carga completa más los cambios en curso, respectivamente.		Desarrollador
Ejecute la tarea de replicación y supervise CloudWatch los registros de Amazon.		Desarrollador
Valide los datos en las bases de datos de origen y destino.		Desarrollador

Migración de su aplicación y cómo realizar la transición

Tarea	Descripción	Habilidades requeridas
Siga los pasos de su estrategia de migración de aplicaciones.		Administrador de base de datos, desarrollador, propietario de la aplicación
Siga los pasos de su estrategia de transición o cambio de aplicaciones.		Administrador de base de datos, desarrollador, propietario de la aplicación

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Valide el esquema y los datos en las bases de datos de origen y de destino.		Administrador de base de datos/desarrollador

Tarea	Descripción	Habilidades requeridas
Recopile métricas en función del tiempo de migración, el porcentaje de trabajo manual en comparación con el trabajo con herramientas, el ahorro de costos, etc.		DBA/Desarrollador/ AppOwner
Revise los documentos y artefactos del proyecto.		DBA/Desarrollador/ AppOwner
Cerrar los recursos temporales de AWS.		Administrador de base de datos/desarrollador
Cerrar el proyecto y enviar comentarios.		DBA/Desarrollador/ AppOwner

Recursos relacionados

- Documentación de AWS DMS
- Sitio web de AWS DMS
- Publicaciones del blog de AWS DMS
- Strategies for Migrating Oracle Database to AWS
- Preguntas frecuentes de Amazon RDS para Oracle
- Preguntas frecuentes sobre Oracle
- Amazon EC2
- Preguntas frecuentes sobre Amazon EC2
- Concesión de licencias de software de Oracle en el entorno de computación en la nube

Migración de Oracle a Amazon DocumentDB con AWS DMS

Tipo R: renovar arquitectura	Origen: bases de datos: relacionales	Destino: Amazon DocumentDB
Creado por: AWS	Entorno: PoC o piloto	Tecnologías: bases de datos; migración
Carga de trabajo: Oracle	Servicios de AWS: Amazon DocumentDB	

Resumen

Este patrón proporciona orientación para migrar una base de datos de Oracle a una base de datos de Amazon DocumentDB (con compatibilidad con MongoDB) mediante AWS Database Migration Service (AWS DMS). Este enfoque se puede aplicar a una base de datos de origen de Oracle en las instalaciones, así como a una instancia de base de datos de Amazon Relational Database Service (Amazon RDS) para Oracle. Este patrón utiliza como ejemplo una instancia de origen de base de datos de Oracle en Amazon RDS.

Amazon DocumentDB (con compatibilidad con MongoDB) es un servicio de base de datos de documentos totalmente gestionado y compatible con MongoDB que facilita el almacenamiento, la consulta y la indexación de datos JSON.

El caso de uso de este patrón es la one-to-one replicación de una tabla de base de datos de Oracle en una colección de Amazon DocumentDB. El patrón utiliza las tareas de replicación de AWS DMS para leer la estructura de tablas de la base de datos de Oracle, crear la colección correspondiente en Amazon DocumentDB y realizar una migración a carga completa. Puede ver y consultar sus datos en Amazon DocumentDB, de la misma forma que lo haría en MongoDB.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Familiaridad con el uso de bases de datos de Oracle

- Familiaridad con el uso de Amazon DocumentDB
- Para el usuario de Oracle, SELECCIONE CUALQUIER privilegio TABLE
- Para el uso de Amazon DocumentDB, el privilegio necesario para volcar datos

Limitaciones

Se aplican las siguientes restricciones al utilizar Amazon DocumentDB como destino de AWS DMS:

- En Amazon DocumentDB, los nombres de las colecciones no pueden incluir el símbolo del dólar ($). Además, los nombres de las bases de datos no pueden contener caracteres Unicode.
- AWS DMS no permite combinar varias tablas de origen en una sola colección de Amazon DocumentDB.
- Cuando AWS DMS procesa los cambios de una tabla de origen que no dispone de una clave principal, las columnas de cualquier objeto binario grande (LOB) en esa tabla se omiten.
- Si la opción Cambiar tabla está habilitada y AWS DMS encuentra una columna de origen llamada "_id", esa columna aparece como "__id" (con dos guiones bajos) en la tabla de cambios.
- Si elige Oracle como punto de conexión de origen, el origen de Oracle debe tener el registro suplementario completo habilitado. De lo contrario, si hay columnas en el origen que no han cambiado, los datos se cargan en Amazon DocumentDB como valores nulos.

Versiones de producto

- Amazon RDS para Oracle versión 11.2.0.3 o posterior
- AWS DMS versión 3.1.3 o posterior (para obtener información sobre la versión más reciente, consulte Uso de Amazon DocumentDB como destino para AWS DMS en la documentación de AWS DMS)

Arquitectura

Pila de tecnología de origen

- Instancia de base de datos de Amazon RDS para Oracle

Pila de tecnología de destino

- Amazon DocumentDB

Arquitectura de origen y destino

Herramientas

- AWS DMS: AWS Database Migration Service (AWS DMS) es un servicio web que puede utilizar para migrar datos de un almacén de datos de origen a otro de destino. La Guía del usuario de AWS DMS especifica las versiones y ediciones de la base de datos fuente de Oracle que se admiten para su uso con AWS DMS. Para obtener información adicional relacionada con este patrón, consulte Uso de Amazon DocumentDB como destino para AWS DMS.
- Amazon EC2: Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de AWS. El clúster de Amazon DocumentDB debe ejecutarse en su nube privada virtual (VPC) predeterminada. Para interactuar con el clúster de Amazon DocumentDB, debe lanzar una instancia EC2 en la VPC predeterminada, en la misma región de AWS en la que creó el clúster de Amazon DocumentDB. Para obtener más información, consulte Lanzamiento de una instancia de Amazon EC2 en la documentación de Amazon DocumentDB.

Epics

Planificación de la migración

Tarea	Descripción	Habilidades requeridas
Valide las versiones de las bases de datos de origen y de destino.		AWS Administrador
Elija el tipo de instancia apropiado (capacidad, características de almacenamiento y características de red).		AWS Administrador
Identifique los requisitos de seguridad de acceso a la red/host para las bases de datos de origen y destino.		AWS Administrador

Tarea	Descripción	Habilidades requeridas
Cree un grupo de seguridad saliente para las bases de datos de origen y destino.		AWS Administrador
Crear y configurar una instancia EC2 para Amazon DocumentDB.		AWS Administrador

Configurar la infraestructura

Tarea	Descripción	Habilidades requeridas
Creación de una VPC y de subredes.		AWS Administrador
Cree grupos de seguridad y listas de control de acceso (ACL) a la red.		AWS Administrador
Configure e inicie la instancia de Amazon RDS para Oracle de origen.		AWS Administrador
Configure e inicie la instancia de Amazon DocumentDB.		AWS Administrador

PreparE la base de datos de origen

Tarea	Descripción	Habilidades requeridas
Compruebe que la base de datos de Oracle se pueda conectar mediante los detalles de conexión.		AWS Administrador

Tarea	Descripción	Habilidades requeridas
Compruebe que el usuario de Oracle tiene el privilegio SELECT ANY TABLE.		AWS Administrador

Prepare la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Cree el clúster de Amazon DocumentDB eligiendo la clase de instancia y el número de instancias adecuados.		AWS Administrador

Configurar Amazon EC2

Tarea	Descripción	Habilidades requeridas
Para configurar la instancia EC2.	Para interactuar con el clúster de Amazon DocumentDB, debe lanzar una instancia EC2 en la VPC predeterminada, en la misma región de AWS en la que creó el clúster de Amazon DocumentDB. Configure la Región de AWS, las VPC, las zonas de disponibilidad y las subredes para la instancia EC2.	AWS Administrador
Configure el par de claves.	Par de claves públicas/ privadas que le permite conectarse de forma segura	AWS Administrador

Tarea	Descripción	Habilidades requeridas
	a la instancia EC2 una vez lanzada.	
Configure los rangos de CIDR de los hosts bastiones (opcional).	Configure el intervalo de direcciones IP de CIDR para el acceso Secure Shell (SSH) externo a las instancias del host bastión.	AWS Administrador

Migración de datos: carga completa

Tarea	Descripción	Habilidades requeridas
Cree una instancia de replicación de AWS DMS.		AWS Administrador
Cree puntos de conexión de origen y destino.		AWS Administrador
Cree tareas de replicación de AWS DMS para una carga completa.		AWS Administrador

Prueba de la migración de datos

Tarea	Descripción	Habilidades requeridas
Conéctese al clúster de Amazon DocumentDB a través de la instancia EC2.		AWS Administrador
Conectarse a un clúster mediante el intérprete de comandos de mongo.	Para obtener instrucciones, consulte los enlaces de Amazon DocumentDB en la sección Referencias y ayuda.	AWS Administrador

Tarea	Descripción	Habilidades requeridas
Verifique los resultados de la migración.		AWS Administrador

Recursos relacionados

- Cómo funciona AWS DMS
- Migración a Amazon DocumentDB
- Uso de Amazon DocumentDB como objetivo para AWS DMS
- Información general sobre Amazon DocumentDB
- Obtenga acceso y utilice su clúster de Amazon DocumentDB mediante el intérprete de comandos de mongo
- Migración de MongoDB a Amazon DocumentDB mediante el método offline (entrada del blog)
- Cómo utilizar Amazon DocumentDB (con compatibilidad con MongoDB) para crear y gestionar aplicaciones a escala (entrada del blog)

Migrar una base de datos Oracle de Amazon EC2 a Amazon RDS para MariaDB mediante AWS DMS y AWS SCT

Creado por Veeranjaneyulu Grandhi (AWS) y vinod kumar (AWS)

Entorno: PoC o piloto	Origen: bases de datos: relacionales	Destino: Amazon RDS para MariaDB
Tipo R: renovar arquitectura	Carga de trabajo: Oracle	Tecnologías: migración; bases de datos
Servicios de AWS: Amazon RDS		

Resumen

Este patrón le guía por los pasos para migrar una base de datos Oracle en una instancia de Amazon Elastic Compute Cloud (Amazon EC2) a una instancia de Amazon Relational Database Service (Amazon RDS) para la base de datos MariaDB. Este patrón utiliza AWS Data Migration Service (AWS DMS) y Herramienta de conversión de esquemas de AWS (AWS SCT) para la conversión de esquemas.

Administrar bases de datos de Oracle en instancias de EC2 requiere más recursos y es más costoso que usar una base de datos en Amazon RDS. Amazon RDS facilita la configuración, el funcionamiento y el escalado de una base de datos relacional en la nube. Amazon RDS proporciona una capacidad rentable y redimensionable a la vez que automatiza las tareas de administración que tanto tiempo consumen, como el aprovisionamiento de hardware, la configuración de la base de datos, la aplicación de parches y las copias de seguridad.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una base de datos Oracle de origen con servicios de instancia y escucha en funcionamiento. Esta base de datos debe estar en modo ARCHIVELOG.
- Estar familiarizado con Usar una base de datos de Oracle como origen para AWS DMS

- Familiaridad con el uso de Oracle como origen para AWS SCT.

Limitaciones

- Límite de tamaño de la base de datos: 64 TB

Versiones de producto

- Todas las ediciones de las bases de datos Oracle para las versiones 10.2 y posteriores, 11g y versiones posteriores a la 12.2 y 18c. Para ver la lista actualizada de versiones compatibles, consulte Uso de una base de datos Oracle como origen para AWS DMS y la tabla de versiones de AWS SCT en la documentación de AWS.
- Amazon RDS es compatible con las versiones 10.3, 10.4, 10.5 y 10.6 de MariaDB Server Community Server. Para ver la lista más reciente de las versiones admitidas, consulte la documentación de Amazon RDS.

Arquitectura

Pila de tecnología de origen

- Una base de datos Oracle en una instancia EC2

Pila de tecnología de destino

- Amazon RDS para MariaDB

Arquitectura de migración de datos

Arquitectura de destino

Herramientas

- La Herramienta de conversión de esquemas de AWS (AWS SCT) hace que las migraciones de bases de datos heterogéneas sean predecibles al convertir automáticamente el esquema de la

base de datos de origen y la mayoría de los objetos de código de la base de datos (incluidas las vistas, los procedimientos almacenados y las funciones) a un formato compatible con la base de datos de destino. Tras convertir el esquema de la base de datos y los objetos de código mediante AWS SCT, puede utilizar AWS DMS para migrar los datos de la base de datos de origen a la base de datos de destino para completar sus proyectos de migración. Para obtener más información, consulte Uso de Oracle como fuente de AWS SCT en la documentación de AWS SCT.

- AWS Database Migration Service (AWS DMS) le ayuda a migrar bases de datos a AWS de forma rápida y segura. La base de datos de origen permanece totalmente operativa durante la migración, minimizando así el tiempo de inactividad de las aplicaciones que dependen de ella. AWS DMS puede migrar sus datos desde y hasta las bases de datos comerciales y de código abierto más utilizadas. AWS DMS admite migraciones homogéneas, como de Oracle a Oracle, así como migraciones heterogéneas entre diferentes plataformas de bases de datos, como de Oracle o Microsoft SQL Server a Amazon Aurora. Para obtener más información sobre la migración de bases de datos de Oracle, consulte Uso de una base de datos de Oracle como origen para AWS DMS en la documentación de AWS DMS.

Epics

Planificar la migración

Tarea	Descripción	Habilidades requeridas
Identifique las versiones y los motores de bases de datos.	Identifique las versiones y motores de la base de datos de origen y destino.	Administrador de base de datos, desarrollador
Identifique la instancia de replicación.	Identifique la instancia de replicación de AWS DMS.	Administrador de base de datos, desarrollador
Identifique requisitos de almacenamiento.	Identifique el tipo y la capacidad de almacenam iento.	Administrador de base de datos, desarrollador
Identifique requisitos de red.	Identifique la latencia y el ancho de banda de la red.	Administrador de base de datos, desarrollador
Identifique los requisitos de hardware.	Identifique los requisitos de hardware para las instancia	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
	s del servidor de origen y destino (según la lista de compatibilidad de Oracle y los requisitos de capacidad).	
Identifique los requisitos de seguridad.	Identifique los requisitos de seguridad de acceso a la red de las bases de datos de origen y destino.	Administrador de base de datos, desarrollador
Instalar controladores.	Instale los controladores AWS SCT y Oracle más recientes.	Administrador de base de datos, desarrollador
Determine una estrategia de copia de seguridad.		Administrador de base de datos, desarrollador
Determine los requisitos de disponibilidad.		Administrador de base de datos, desarrollador
Elija una estrategia de migración/transición de aplicaciones.		Administrador de base de datos, desarrollador
Seleccione el tipo de instancia .	Seleccione el tipo de instancia adecuado en función de la capacidad, el almacenamiento y las características de la red.	Administrador de base de datos, desarrollador

Configure el entorno

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC).	Las instancias de origen, destino y replicación deben estar en la misma VPC y en la	Desarrollador

Tarea	Descripción	Habilidades requeridas
	misma zona de disponibilidad (recomendado).	
Creación de los grupos de seguridad.	Cree los grupos de seguridad necesarios para el acceso a la base de datos.	Desarrollador
Genere un par de claves.	Genere y configure un par de claves.	Desarrollador
Configure otros recursos.	Configure las subredes, las zonas de disponibilidad y los bloques CIDR.	Desarrollador

Configurar el origen

Tarea	Descripción	Habilidades requeridas
Lanzar la instancia EC2.	Para obtener instrucciones, consulte la documentación de Amazon EC2.	Desarrollador
Instalar la base de datos de Oracle.	Instale la base de datos Oracle en la instancia de EC2, con los usuarios y roles necesarios.	Administrador de base de datos
Siga los pasos de la descripción de la tarea para acceder a Oracle desde fuera de la instancia de EC2.	1. Cambie el host local en `tnsnames` al DNS público de Amazon EC2. 2. Cambie el host local en `listener` al DNS público de Amazon EC2. 3. Detenga y vuelva a iniciar el oyente.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Actualice el DNS público de Amazon EC2.	Una vez reiniciada la instancia de EC2, el DNS público cambia. Asegúrese de actualizar el DNS público de Amazon EC2 en `tnsnames` y `listener`, o utilice una dirección IP elástica.	Administrador de base de datos, desarrollador
Configurar el grupo de seguridad de instancias de EC2.	Configure el grupo de seguridad de la instancia de EC2 para que la instancia de replicación y los clientes necesarios puedan acceder a la base de datos de origen.	Administrador de base de datos, desarrollador

Configurar el entorno de destino de Amazon RDS para MariaDB

Tarea	Descripción	Habilidades requeridas
Inicie la instancia de base de datos de RDS.	Configure e inicie la instancia de la base de datos de Amazon RDS para MariaDB.	Desarrollador
Crear espacios de trabajo.	Cree los espacios de tabla necesarios en la base de datos MariaDB de Amazon RDS MariaDB.	Administrador de base de datos
Configurar un grupo de seguridad.	Configure un grupo de seguridad para que la instancia de replicación y los clientes necesarios puedan acceder a la base de datos de destino.	Desarrollador

Configurar AWS SCT

Tarea	Descripción	Habilidades requeridas
Instalar controladores.	Instale los controladores AWS SCT y Oracle más recientes.	Desarrollador
Connect (Conectar).	Introduzca los parámetros adecuados y, a continuac ión, conéctese al origen y al destino.	Desarrollador
Genere un informe de conversión de esquemas.	Genere un informe de conversión del esquemas de AWS SCT.	Desarrollador
Corrija el código y el esquema según sea necesario.	Realice las correcciones necesarias en el código y el esquema (especialmente los espacios de tabla y las comillas).	Administrador de base de datos, desarrollador
Valide el esquema.	Valide el esquema en el origen frente al de destino antes de cargar los datos.	Desarrollador

Migre datos utilizando AWS DMS

Tarea	Descripción	Habilidades requeridas
Defina un atributo de conexión.	Para cargar completamente y capturar datos de cambios (CDC) o simplemente para CDC, debe configurar un atributo de conexión adicional. Para obtener más información,	Desarrollador

Tarea	Descripción	Habilidades requeridas
	consulte la documentación de Amazon RDS.	
Habilitar el registro suplement ario.	Habilitar el registro suplement ario en la base de datos de origen.	Administrador de base de datos, desarrollador
Habilite el modo de registro de archivos.	Para los CDC de carga completa (o solo para los CDC), habilite el modo de registro de archivos en la base de datos de origen.	Administrador de base de datos
Cree y pruebe puntos de conexión.	Cree puntos de conexión de origen y destino y pruebe las conexiones. Para obtener más información, consulte la documentación de Amazon DMS.	Desarrollador
Cree una tarea de replicación.	Cuando los puntos de conexión estén conectados correctamente, cree una tarea de replicación. Para obtener más información, consulte la documentación de Amazon DMS.	Desarrollador
Elija el tipo de replicación.	Elija Solo CDC o Carga completa más CDC en la tarea para capturar los cambios solo para la replicación continua, o para carga completa y cambios continuos, respectiv amente.	Desarrollador

Tarea	Descripción	Habilidades requeridas
Inicie y monitoree la tarea.	Inicie la tarea de replicación y supervise CloudWatch los registros de Amazon. Para obtener más información, consulte la documentación de Amazon DMS.	Desarrollador
Valide los datos.	Valide los datos en las bases de datos de origen y destino.	Desarrollador

Migrar aplicaciones y hacer la transición a la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Siga la estrategia de migración de aplicaciones elegida.		Administrador de base de datos, propietario de la aplicación, desarrollador
Siga la estrategia de transició n/cambio de la aplicación elegida.		Administrador de base de datos, propietario de la aplicación, desarrollador

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Valide el esquema y los datos.	Asegúrese de que el esquema y los datos se validen correctamente en el origen frente al destino antes de cerrar el proyecto.	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
Recopile métricas.	Recopile métricas para tiempo de migración, porcentaj e de tareas manuales en comparación con las tareas de herramientas, ahorro de costos y otros criterios similares.	Administrador de base de datos, propietario de la aplicación, desarrollador
Revise la documentación.	Revise los documentos y artefactos del proyecto.	Administrador de base de datos, propietario de la aplicación, desarrollador
Cierre los recursos.	Cerrar los recursos temporale s de AWS.	Administrador de base de datos, desarrollador
Cierre el proyecto.	Cierre el proyecto de migración y envíe sus comentarios.	Administrador de base de datos, propietario de la aplicación, desarrollador

Recursos relacionados

- Información general sobre MariaDB de Amazon RDS
- Detalles del producto de Amazon RDS para MariaDB
- Uso de una base de datos de Oracle como origen para AWS DMS
- Estrategias para migrar bases de datos Oracle a AWS
- Concesión de licencias de software de Oracle en el entorno de computación en la nube
- Preguntas frecuentes de Amazon RDS para Oracle
- Información general sobre AWS DMS
- Publicaciones del blog de AWS DMS
- Información general sobre Amazon EC2
- Preguntas frecuentes sobre Amazon EC2
- Documentación de AWS SCT

Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para MySQL con AWS DMS y AWS SCT

Tipo R: renovar arquitectura	Origen: bases de datos: relacionales	Destino: Amazon RDS para MySQL
Creado por: AWS	Entorno: PoC o piloto	Tecnologías: bases de datos; migración
Carga de trabajo: Oracle	Servicios de AWS: Amazon RDS	

Resumen

Este patrón le guía a través de la migración de una base de datos de Oracle en las instalaciones a una Amazon Relational Database Service (Amazon RDS) para una instancia de base de datos de MySQL. Utiliza AWS Database Migration Service (AWS DMS) para migrar los datos y la Herramienta de conversión de esquemas de AWS (AWS SCT) para convertir el esquema y los objetos de la base de datos de origen a un formato compatible con Amazon RDS para MySQL.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos de origen de Oracle en un centro de datos en las instalaciones

Limitaciones

- Límite de tamaño de la base de datos: 64 TB

Versiones de producto

- Todas las ediciones de bases de datos de Oracle para las versiones 11g (versiones 11.2.0.3.v1 y posteriores) y hasta la 12.2, y 18c. Para ver la lista actualizada de versiones compatibles, consulte Uso de una base de datos de Oracle como origen para AWS DMS. Le recomendamos

utilizar la versión más reciente de AWS DMS para obtener el soporte más completo de versiones y características. Para obtener información sobre las versiones de bases de datos de Oracle compatibles con AWS SCT, consulte la Documentación de AWS SCT.

- AWS DMS es actualmente compatible con las versiones 5.5, 5.6 y 5.7 de MySQL. Para ver la lista actualizada de versiones compatibles, consulte Uso de una base de datos compatible con MySQL como destino para las versiones de AWS DMS en la documentación de AWS.

Arquitectura

Pila de tecnología de origen

- Base de datos de Oracle en las instalaciones

Pila de tecnología de destino

- Instancia de base de datos de Amazon RDS para MySQL

Arquitectura de migración de datos

Herramientas

- AWS DMS: AWS Database Migration Services (AWS DMS) facilita la migración de bases de datos relacionales, almacenamiento de datos, bases de datos NoSQL y otros tipos de almacenes de datos. Puede utilizar AWS DMS para migrar datos a la nube de AWS, entre instancias en las instalaciones (a través de una configuración de nube de AWS) o entre combinaciones de configuraciones en las instalaciones y en la nube.
- AWS SCT: la Herramienta de conversión de esquemas de AWS (AWS SCT) se utiliza para convertir su esquema de base de datos existente de un motor de base de datos a otro. El código personalizado que convierte la herramienta incluye vistas, procedimientos almacenados y funciones. Cualquier código que la herramienta no pueda convertir automáticamente está claramente marcado para que pueda convertirlo usted mismo.

Epics

Planificación de la migración

Tarea	Descripción	Habilidades requeridas
Valide la versión y el motor de la base de datos de origen y de destino.		Administrador de base de datos
Identifique los requisitos de hardware de la instancia del servidor de destino.		DBA, SysAdmin
Identifique los requisitos de almacenamiento (el tipo y la capacidad de almacenam iento).		DBA, SysAdmin
Elija el tipo de instancia adecuado en función de la capacidad, las características de almacenamiento y las características de red.		DBA, SysAdmin
Identifique los requisitos de seguridad de acceso a la red para las bases de datos de origen y destino.		DBA, SysAdmin
Identificar la estrategia de migración de aplicaciones.		DBA, propietario de la SysAdmin aplicación

Configuración de la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC) y subredes.		SysAdmin
Creación de grupos de seguridad y listas de control de acceso a la red (ACL).		SysAdmin
Configure e inicie una instancia de base de datos de Amazon RDS.		DBA, SysAdmin

Migración de datos

Tarea	Descripción	Habilidades requeridas
Migre el esquema de la base de datos mediante AWS SCT.		Administrador de base de datos
Migre los datos mediante AWS DMS.		Administrador de base de datos

Migración de la aplicación

Tarea	Descripción	Habilidades requeridas
Utilizar AWS SCT para analizar y convertir el código SQL dentro del código de la aplicación.	Para obtener más informaci ón, consulte https://docs.aws.a mazon.com/ SchemaCon version tool/latest/UserGuide/ chap_converting.app.html.	Propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Seguir la estrategia de migración de aplicaciones.		SysAdminDBA, propietario de la aplicación

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Cambie los clientes de la aplicación a la nueva infraestructura.		DBA, propietario de la SysAdmin aplicación

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cerrar los recursos temporales de AWS.		DBA, SysAdmin
Revise y valide los documentos del proyecto.		DBA, SysAdmin
Recopile métricas sobre el tiempo de migración, el porcentaje de migraciones manuales en comparación con las realizadas con herramientas, el ahorro de costos, etc.		DBA, SysAdmin
Cerrar el proyecto y enviar comentarios.		

Recursos relacionados

Referencias

- Documentación de AWS DMS
- Documentación de AWS SCT
- Precios de Amazon RDS

Tutoriales y videos

- Introducción a AWS DMS
- Introducción a Amazon RDS
- AWS DMS (video)
- Amazon RDS (video)

Migre una base de datos Oracle en las instalaciones a Amazon RDS para PostgreSQL mediante Oracle Bystander y AWS DMS

Creado por Cady Motyka (AWS)

Entorno: PoC o piloto	Origen: bases de datos: relacionales	Destino: Amazon RDS para PostgreSQL o Amazon Aurora (PostgreSQL).
Tipo R: renovar arquitectura	Carga de trabajo: Oracle	Tecnologías: migración; bases de datos
Servicios de AWS: Amazon RDS		

Resumen

Este patrón describe cómo puede migrar una base de datos Oracle en las instalaciones a cualquiera de los siguientes servicios de bases de datos de AWS compatibles con PostgreSQL con un tiempo de inactividad mínimo:

- Amazon Relational Database Service (Amazon RDS) para PostgreSQL
- Edición compatible con Amazon Aurora PostgreSQL

La solución utiliza AWS Database Migration Service (AWS DMS) para migrar los datos, la Herramienta de conversión de esquemas de AWS (AWS SCT) para convertir el esquema de la base de datos y una base de datos Oracle Bystander para ayudar a gestionar la migración. En esta implementación, el tiempo de inactividad se limita al tiempo necesario para crear o validar todas las claves externas de la base de datos.

La solución también utiliza instancias de Amazon Elastic Compute Cloud (Amazon EC2) con una base de datos Oracle Bystander para ayudar a controlar el flujo de datos a través de AWS DMS. Puede pausar temporalmente la replicación en streaming desde la base de datos Oracle en las instalaciones a Oracle Bystander para activar AWS DMS y ponerse al día con la validación de datos o para utilizar otra herramienta de validación de datos. La instancia de base de datos de Amazon RDS para PostgreSQL o la instancia de base de datos compatible con Aurora PostgreSQL y la base

de datos de bystander tendrán los mismos datos cuando AWS DMS termine de migrar los cambios actuales.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una base de datos de origen de Oracle en un centro de datos en las instalaciones con Active Data Guard configurado en modo de espera
- AWS Direct Connect, configurado entre el centro de datos en las instalaciones y AWS Secrets Manager para almacenar los secretos de la base de datos
- Controladores de conectividad de bases de datos Java (JDBC) para conectores SCT de AWS instalados en una máquina local o en la instancia EC2 en la que está instalado AWS SCT
- Uso de una base de datos de Oracle como origen para AWS DMS
- Uso de una base de datos de PostgreSQL como destino para AWS DMS

Limitaciones

- Límite de tamaño de la base de datos: 64 TB

Versiones de producto

- AWS DMS es compatible con todas las ediciones de bases de datos Oracle para las versiones 10.2 y posteriores (para versiones 10.x), 11g y hasta 12.2, 18c y 19c. Para ver la lista actualizada de versiones compatibles, consulte Uso de una base de datos Oracle como fuente para AWS DMS. Le recomendamos utilizar la versión más reciente de AWS DMS para obtener el soporte más completo de versiones y características. Para obtener información sobre las versiones de bases de datos Oracle compatibles con AWS SCT, consulte la documentación de AWS SCT.
- AWS DMS es compatible con PostgreSQL versión 9.4 y posterior (para las versiones 9.x), 10.x, 11.x, 12.x y 13.x Para obtener más información, consulte Uso de una base de datos PostgreSQL como destino para AWS DMS en la documentación de AWS.

Arquitectura

Pila de tecnología de origen

- Una base de datos Oracle en las instalaciones
- Una instancia EC2 que aloja a un bystander para la base de datos Oracle

Pila de tecnología de destino

- Instancia de Amazon RDS para PostgreSQL o Aurora PostgreSQL, PostgreSQL 9.3 y versiones posteriores

Arquitectura de destino

El siguiente diagrama muestra un ejemplo de flujo de trabajo para migrar una base de datos de Oracle a una base de datos de AWS compatible con PostgreSQL mediante AWS DMS y un bystander de Oracle:

Herramientas

- AWS Database Migration Service (AWS DMS) le permite migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones.
- La Herramienta de conversión de esquemas de AWS (AWS SCT) simplifica las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado, lo que incluye las vistas, los procedimientos almacenados y las funciones, a un formato compatible con la base de datos de destino.
- Amazon Relational Database Service (Amazon RDS) ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS.

Epics

Convertir el esquema de base de datos Oracle a PostgreSQL

Tarea	Descripción	Habilidades requeridas
Configure AWS SCT.	Cree un informe nuevo y conéctese a Oracle como origen y a PostgreSQL como destino. En la Configura ción del proyecto, vaya a	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	la pestaña SQL Scripting . Cambie el Script SQL de destino a Carios archivos. Estos archivos se utilizarán más adelante y se denominar án de la siguiente manera: • create_database.sql • create_sequence.sql • create_table.sql • create_view.sql • create_function.sql	
Convertir el esquema de base de datos Oracle.	En la pestaña Acción, elija Generar informe. A continuac ión, elija Convertir esquema y seleccione Guardar como SQL.	Administrador de base de datos
Modifique los scripts.	Por ejemplo, es posible que desee modificar el script si un número del esquema de origen se ha convertid o a formato numérico en PostgreSQL, pero prefiera utilizar BIGINT en su lugar para obtener un mejor rendimiento.	Administrador de base de datos

Creación y configuración de la instancia de base de datos de Amazon RDS

Tarea	Descripción	Habilidades requeridas
Creación de una instancia de base de datos de Amazon RDS	En la región de AWS correcta, cree una nueva instancia de base de datos de PostgreSQL. Para obtener más información, consulte Creación de una instancia de base de datos PostgreSQL y conexión a una base de datos en una instancia de base de datos PostgreSQL en la documentación de Amazon RDS.	AWS SysAdmin, administrador de bases de datos
Configure las especificaciones de la instancia de base de datos.	Especifique la versión del motor de base de datos, la clase de instancia de base de datos, la implementación Multi-AZ, el tipo de almacenamiento y el almacenamiento asignado. Introduzca el identificador de la instancia de base de datos, un nombre de usuario principal y una contraseña principal.	AWS SysAdmin, administrador de bases de datos
Configurar la red y la seguridad.	Especifique la nube privada virtual (VPC), el grupo de subredes, la accesibilidad pública, la preferencia de zona de disponibilidad y los grupos de seguridad.	DBA, SysAdmin

Tarea	Descripción	Habilidades requeridas
Configurar las opciones de la base de datos.	Especifique el nombre, el puerto, el grupo de parámetros, el cifrado y la clave KMS.	AWS SysAdmin, administrador de bases de datos
Configure copias de seguridad.	Especifique el período de retención de la copia de seguridad, la ventana de copia de seguridad, la hora de inicio, la duración y si desea copiar las etiquetas a las instantáneas.	AWS SysAdmin, administrador de bases de datos
Configure las opciones de monitoreo.	Active o desactive los conocimientos mejorados de supervisión y rendimiento.	AWS SysAdmin, administrador de bases de datos
Configurar las opciones de mantenimiento.	Especifique la actualización automática de versiones secundarias, el período de mantenimiento y el día, la hora y la duración de inicio.	AWS SysAdmin, administrador de bases de datos
Ejecute los scripts previos a la migración desde AWS SCT.	En la instancia de Amazon RDS, ejecute los siguientes scripts generados por AWS SCT: • create_database.sql • create_sequence.sql • create_table.sql • create_view.sql • create_function.sql	AWS SysAdmin, administrador de bases de datos

Configurar Oracle bystander en Amazon EC2

Tarea	Descripción	Habilidades requeridas
Configure la red para Amazon EC2.	Creación de la nueva VPC, subredes, puerta de enlace de Internet, tablas de enrutamie nto y grupos de seguridad.	AWS SysAdmin
Crear la instancia EC2.	En la región de AWS correspondiente, cree una nueva instancia de EC2. Seleccione la imagen de máquina de Amazon (AMI), elija el tamaño de la instancia y configure los detalles de la instancia: la cantidad de instancias (1), la VPC y la subred del paso anterior, la asignación automática de la IP pública y otras opciones. Agregue almacenamiento, configure grupos de seguridad y lance. Cuando se le pida, cree y guarde un par de claves para el siguiente paso.	AWS SysAdmin
Conecte la base de datos de origen de Oracle a la instancia EC2.	Copie la dirección IP pública IPv4 y el DNS en un archivo de texto y conéctese mediante SSH de la siguiente manera: ssh -i «your_file.pem» EC2-user@<your-IP - -DNS>. address-or-public	AWS SysAdmin
Configure el host inicial para un bystander en Amazon EC2.	Configure las claves SSH, el perfil bash, ORATAB y los	AWS SysAdmin, administrador de Linux

Tarea	Descripción	Habilidades requeridas
	enlaces simbólicos. Cree directorios Oracle.	
Configure la copia de la base de datos para un bystander en Amazon EC2.	Utilice RMAN para crear una copia de la base de datos, habilitar el registro adicional y crear el archivo de control en espera. Una vez completada la copia, coloque la base de datos en modo de recuperac ión.	AWS SysAdmin, administrador de bases de datos
Configurar Oracle Data Guard.	Modifique el archivo listener. ora e inicie el oyente. Configure un nuevo destino de archivo. Coloque al espectado r en modo de recuperac ión, sustituya los archivos temporales para evitar futuros daños, instale un crontab si es necesario para evitar que el directorio de archivos se quede sin espacio y edite el manage-trclog-files-oraclea rchivo.cfg para el archivo de origen y el modo de espera.	AWS SysAdmin, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
Prepare la base de datos de Oracle para sincronizar los envíos.	Añada los archivos de registro en espera y cambie el modo de recuperación. Cambie el envío de registros a SYNC AFFIRM tanto en la fuente principal como en la fuente en espera. Cambie los registros principales, confirme mediante el registro de alertas de bystander de Amazon EC2 que está utilizando los archivos de registro en espera y confirme que la retransmi sión se transmite en SYNC.	AWS SysAdmin, administrador de bases de datos

Migrar datos con AWS DMS

Tarea	Descripción	Habilidades requeridas
Cree una instancia de replicaci ón en AWS DMS.	Complete los campos para el nombre, la clase de instancia , la VPC (igual que para la instancia EC2), la zona de disponibilidad múltiple y la accesibilidad pública. En Avanzado, especifique el almacenamiento asignado, el grupo de subredes, la zona de disponibilidad, los grupos de seguridad de VPC y la clave de AWS Key Management Service (AWS KMS).	AWS SysAdmin, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
Cree el punto de conexión de origen de la base de datos.	Especifique el nombre del punto de conexión, el tipo, el motor de origen (Oracle), el nombre del servidor (nombre de DNS privado de Amazon EC2), el puerto, el modo SSL, el nombre de usuario, la contraseña, el SID, la VPC (especifique la VPC que tiene la instancia de replicación) y la instancia de replicación. Para probar la conexión, seleccione Ejecutar prueba y, a continuac ión, cree el punto de conexión. También puede configurar los siguientes ajustes avanzados : maxFileSizey numberDat aTypeScale.	AWS SysAdmin, administrador de bases de datos
Conecte AWS DMS a Amazon RDS para PostgreSQL.	Cree un grupo de seguridad de migración para las conexiones entre las VPC.	AWS SysAdmin, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
Cree puntos de conexión de base de datos de destino.	Especifique el nombre del punto de conexión, el tipo, el motor de origen (PostgreSQL), el nombre del servidor (punto de conexión de Amazon RDS), el puerto, el modo SSL, el nombre de usuario, la contraseña, el nombre de la base de datos, la VPC (especifique la VPC que tiene la instancia de replicación) y la instancia de replicación. Para probar la conexión, seleccione Ejecutar prueba y, a continuación, cree el punto de conexión. También puede configurar los siguientes ajustes avanzados: maxFileSize y numberDataTypeScale.	AWS SysAdmin, administrador de bases de datos
Cree una tarea de replicación de AWS DMS.	Especifique el nombre de la tarea, la instancia de replicación, los puntos de conexión de origen y destino y la instancia de replicación. Para tipo de migración, seleccione la opción Migrate existing data and replication ongoing changes (Migrar datos existentes y cambios de replicación en curso). Desactive la casilla de verificación Iniciar la tarea al crearla.	AWS SysAdmin, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
Configure la configuración de la tarea de replicación de AWS DMS.	Para el modo de preparación de la tabla de destino, elija No hacer nada. Detenga la tarea cuando se complete la carga completa (para crear las claves principales). Especifiq ue el modo LOB limitado o completo y habilite las tablas de control. Si lo desea, puede configurar la configuración CommitRateavanzada.	Administrador de base de datos
Configure el mapeo de tablas.	En la sección Table mappings (Mapeo de tablas), cree una regla de Inclusión para todas las tablas de todos los esquemas incluidos en la migración y, a continuación, cree una regla de Exclusión . Agregue tres reglas de transformación para convertir los nombres del esquema, la tabla y las columnas a minúsculas y añada cualquier otra regla necesaria para esta migración específica.	Administrador de base de datos
Iniciar la tarea.	Iniciar la tarea de replicación. Asegúrese de que la carga completa está ejecutando. Ejecute ALTER SYSTEM SWITCH LOGFILE en la base de datos principal de Oracle para iniciar la tarea.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Ejecute los scripts de la migración intermedia desde AWS SCT.	En Amazon RDS para PostgreSQL, ejecute los siguientes scripts generados por AWS SCT: • create_index.sql • create_constraint.sql	Administrador de base de datos
Reinicie la tarea para continuar con la captura de datos de cambio (CDC).	Ejecute VACUUM en la instancia de base de datos Amazon RDS para PostgreSQL y reinicie la tarea de AWS DMS para aplicar los cambios de CDC en caché.	Administrador de base de datos

Realizar la transición a la base de datos de PostgreSQL

Tarea	Descripción	Habilidades requeridas
Revise los registros y las tablas de validación de AWS DMS para ver si hay algún error.	Compruebe y corrija cualquier error de replicación o validación.	Administrador de base de datos
Detenga todas las dependencias de Oracle.	Detenga todas las dependencias de Oracle, cierre los oyentes de la base de datos de Oracle y ejecute ALTER SYSTEM SWITCH LOGFILE. Detenga la tarea de AWS DMS cuando no muestre actividad.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Ejecute los scripts posterior es a la migración desde AWS SCT.	En Amazon RDS para PostgreSQL, ejecute los siguientes scripts generados por AWS SCT: • create_foreign_key_constrai nt.sql • create_triggers.sql	Administrador de base de datos
Complete los pasos adicional es de Amazon RDS para PostgreSQL.	Aumente las secuencias para que coincidan con las de Oracle si es necesario, ejecute VACUUM y ANALYZE y tome una instantánea para comprobar la conformidad.	Administrador de base de datos
Abra las conexiones hacia Amazon RDS para PostgreSQ L.	Elimine los grupos de seguridad de AWS DMS de Amazon RDS para PostgreSQ L, añada grupos de seguridad de producción y dirija sus aplicaciones a la nueva base de datos.	Administrador de base de datos
Limpie los objetos de AWS DMS.	Elimine los puntos de conexión, las tareas de replicación, las instancias de replicación y la instancia EC2.	SysAdmin, DBA

Recursos relacionados

- Documentación de AWS DMS
- Documentación de AWS SCT
- Precio de Amazon RDS para PostgreSQL

Migre de Oracle Database a Amazon RDS for PostgreSQL mediante Oracle GoldenGate

Creado por Dhairya Jindani (AWS), Rajeshkumar Sabankar (AWS) y Sindhusha Paturu (AWS)

Entorno: PoC o piloto	Origen: bases de datos: relacionales	Destino: Amazon RDS para PostgreSQL
Tipo R: renovar arquitectura	Carga de trabajo: Oracle	Tecnologías: migración; bases de datos
Servicios de AWS: Amazon RDS		

Resumen

Este patrón muestra cómo migrar una base de datos Oracle a Amazon Relational Database Service (Amazon RDS) para PostgreSQL mediante Oracle Cloud Infrastructure (OCI). GoldenGate

Con Oracle GoldenGate, puede replicar datos entre la base de datos de origen y una o más bases de datos de destino con un tiempo de inactividad mínimo.

Nota: La base de datos de origen de Oracle puede estar ubicada en las instalaciones o en una instancia de Amazon Elastic Compute Cloud (Amazon EC2). Puede utilizar un procedimiento similar cuando utilice herramientas de replicación en las instalaciones.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una GoldenGate licencia de Oracle
- Controlador de Java Database Connectivity (JDBC) para conectarse a la base de datos PostgreSQL
- Esquema y tablas creados con la herramienta de conversión de esquemas de AWS (AWS SCT) en la base de datos Amazon RDS para PostgreSQL de destino

Limitaciones

- Oracle solo GoldenGate puede replicar los datos de las tablas existentes (carga inicial) y los cambios en curso (captura de datos de cambios)

Versiones de producto

- Oracle Database 10g Enterprise Edition o versiones más recientes
- Oracle GoldenGate 12.2.0.1.1 para Oracle o versiones más recientes
- Oracle GoldenGate 12.2.0.1.1 para PostgreSQL o versiones más recientes

Arquitectura

El siguiente diagrama muestra un ejemplo de flujo de trabajo para migrar una base de datos de Oracle a Amazon RDS for PostgreSQL mediante Oracle: GoldenGate

En el diagrama, se muestra el siguiente flujo de trabajo:

1. El proceso de GoldenGate extracción de Oracle se ejecuta en la base de datos de origen para extraer los datos.
2. El proceso de Oracle GoldenGate Replicat entrega los datos extraídos a la base de datos Amazon RDS for PostgreSQL de destino.

Herramientas

- Oracle le GoldenGate ayuda a diseñar, ejecutar, organizar y monitorear sus soluciones de procesamiento de datos y de replicación de datos en streaming en Oracle Cloud Infrastructure.
- Amazon Relational Database Service (Amazon RDS) para PostgreSQL lo ayuda a configurar, utilizar y escalar una base de datos relacional de PostgreSQL en la nube de AWS.

Epics

Descargue e instale Oracle GoldenGate

Tarea	Descripción	Habilidades requeridas
Descargue Oracle GoldenGate.	Descargue las siguientes versiones de Oracle GoldenGate: • Oracle GoldenGate 12.2.0.1.1 para Oracle o una versión más reciente • Oracle GoldenGate 12.2.0.1.1 para PostgreSQL o una versión más reciente Para descargar el software, consulte GoldenGate Descargas de Oracle en el sitio web de Oracle.	Administrador de base de datos
Instale Oracle GoldenGate for Oracle en el servidor de Oracle Database de origen.	Para obtener instrucciones, consulte la GoldenGate documentación de Oracle.	Administrador de base de datos
Instale la base de datos Oracle GoldenGate para PostgreSQL en la instancia Amazon EC2.	Para obtener instrucciones, consulte la documentación de Oracle. GoldenGate	Administrador de base de datos

Configure Oracle GoldenGate en las bases de datos de origen y destino

Tarea	Descripción	Habilidades requeridas
Configure Oracle GoldenGate for Oracle Database en la base de datos de origen.	Para obtener instrucciones, consulte la GoldenGate documentación de Oracle. Asegúrese de configurar lo siguiente: • Registro suplementario • GoldenGate Usuarios de Oracle • Cualquier concesión y permiso necesarios • Archivos de parámetros • Proceso de gestión • Directorio • Archivos GLOBALS • Monedero de Oracle	Administrador de base de datos
Configure Oracle GoldenGate para PostgreSQL en la base de datos de destino.	Para obtener instrucciones, consulte la Parte VI Uso de Oracle GoldenGate para PostgreSQL en el sitio web de Oracle. Asegúrese de configurar lo siguiente: • Proceso de gestión • Archivos GLOBALS • Monedero de Oracle	Administrador de base de datos

Configuración de la captura de datos

Tarea	Descripción	Habilidades requeridas
Configure el proceso de extracción en la base de datos de origen.	En la base de datos de Oracle de origen, cree un archivo de extracción para extraer los datos. Para obtener instrucciones, consulte ADD EXTRACT en la documentación de Oracle. Nota: El archivo de extracción incluye la creación del archivo de parámetros de extracción y el directorio de archivos de seguimiento.	Administrador de base de datos
Configure una bomba de datos para transferir el archivo de seguimiento de la base de datos de origen a la de destino.	Cree un archivo de parámetros EXTRACT y un directorio de archivos de seguimiento siguiendo las instrucciones que aparecen en PARFILE en Utilidades de bases de datos, en el sitio web de Oracle. Para obtener más información, consulte ¿Qué es una ruta? en Fusion Middleware Understanding Oracle GoldenGate en el sitio web de Oracle.	Administrador de base de datos
Instale la replicación en la instancia de Amazon EC2.	Cree un archivo de parámetros de replicación y un directorio de archivos de seguimiento.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Para obtener más información sobre la creación de archivos de parámetros de replicación, consulte la sección 3.5 Validación de un archivo de parámetros en la documentación de la base de datos de Oracle. Para obtener más información, consulte Creación de un registro de seguimiento en la documentación de CloudTrail. Importante: asegúrese de añadir una entrada en la tabla de puntos de control en el archivo GLOBALS del destino. Para obtener más información, consulte ¿Qué es un replicante? en Fusion Middleware Understanding Oracle GoldenGate en el sitio web de Oracle.	

Configure la replicación de datos

Tarea	Descripción	Habilidades requeridas
En la base de datos de origen, cree un archivo de parámetros para extraer los datos de la carga inicial.	Siga las instrucciones de la sección Creación de un archivo de parámetros en GGSCI en la documentación de Oracle Cloud.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Importante: asegúrese de que el administrador esté funcionando en el objetivo.	
En la base de datos de destino, cree un archivo de parámetros para replicar los datos de la carga inicial.	Siga las instrucciones de la sección Creación de un archivo de parámetros en GGSCI en la documentación de Oracle Cloud. Importante: asegúrese de añadir e iniciar el proceso de replicación.	Administrador de base de datos

Cambie a la base de datos de Amazon RDS para PostgreSQL

Tarea	Descripción	Habilidades requeridas
Detenga el proceso de replicación y asegúrese de que las bases de datos de origen y destino estén sincronizadas.	Compare los recuentos de filas entre las bases de datos de origen y destino para asegurarse de que la replicación de los datos se realizó correctamente.	Administrador de base de datos
Compatibilidad con el lenguaje de definición de datos (DDL) de configuración.	Ejecute el script DDL para crear activadores, secuencias, sinónimos y claves referenciales en PostgreSQL. Nota: Puede usar cualquier aplicación cliente de SQL estándar para conectarse al clúster de base de datos. Por ejemplo, puede usar pgAdmin	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	para conectarse a su instancia de base de datos.	

Recursos relacionados

- Amazon RDS para PostgreSQL en la Guía del usuario de Amazon RDS
- Documentación de Amazon EC2
- Oracle GoldenGate admitía métodos de procesamiento y bases de datos (documentación de Oracle)

Migración de una base de datos de Oracle a Amazon Redshift con AWS DMS y AWS SCT

Origen: Oracle	Destino: Redshift	Tipo R: renovar arquitectura
Entorno: producción	Tecnologías: migración; análisis; bases de datos	Carga de trabajo: Oracle
Servicios de AWS: Amazon Redshift; AWS DMS		

Resumen

Este patrón proporciona orientación para migrar las bases de datos de Oracle a un data warehouse en la nube de Amazon Redshift en la nube de Amazon Web Services (AWS) mediante AWS Database Migration Service (AWS DMS) y la Herramienta de conversión de esquemas de AWS (AWS SCT). El patrón cubre las bases de datos de Oracle de origen que se encuentran en las instalaciones o instaladas en una instancia de Amazon Elastic Compute Cloud (Amazon EC2). También incluye Amazon Relational Database Service (Amazon RDS) para bases de datos de Oracle.

Requisitos previos y limitaciones

Requisitos previos

- Una base de datos de Oracle que se ejecuta en un centro de datos en las instalaciones o en la nube de AWS
- Una cuenta de AWS activa
- Estar familiarizado con el uso de una base de datos de Oracle como origen para AWS DMS
- Familiaridad con el uso de una base de datos Amazon Redshift como objetivo para AWS DMS
- Conocimiento de Amazon RDS, Amazon Redshift, las tecnologías de bases de datos aplicables y SQL
- Controladores de conectividad de bases de datos Java (JDBC) para conectores de AWS SCT, donde está instalado AWS SCT

Versiones de producto

- Para las bases de datos de Oracle autogestionadas, AWS DMS admite todas las ediciones de bases de datos de Oracle para las versiones 10.2 y posteriores (para las versiones 10.x), 11g y hasta 12.2, 18c y 19c. En el caso de las bases de datos de Amazon RDS para Oracle que administra AWS, AWS DMS admite todas las ediciones de bases de datos de Oracle para las versiones 11g (versiones 11.2.0.4 y posteriores) y hasta 12.2, 18c y 19c. Le recomendamos utilizar la versión más reciente de AWS DMS para obtener el soporte más completo de versiones y características.

Arquitectura

Pila de tecnología de origen

Uno de los siguientes:

- Una base de datos de Oracle en las instalaciones
- Una base de datos de Oracle en una instancia EC2
- Una instancia de base de datos de Amazon RDS para Oracle

Pila de tecnología de destino

- Amazon Redshift

Arquitectura de destino

De una base de datos de Oracle que se ejecuta en la nube de AWS a Amazon Redshift:

Desde una base de datos de Oracle que se ejecuta en un centro de datos interno hasta Amazon Redshift:

Herramientas

- AWS DMS: AWS Database Migration Service (AWS DMS) le ayuda a migrar bases de datos a AWS de forma rápida y segura. La base de datos de origen permanece totalmente operativa

durante la migración, minimizando así el tiempo de inactividad de las aplicaciones que dependen de ella. AWS DMS puede migrar sus datos desde y hasta las bases de datos comerciales y de código abierto más usadas.

- AWS SCT: la herramienta de conversión de esquemas de AWS (AWS SCT) puede utilizarse para convertir su esquema de base de datos existente de un motor de base de datos a otro. Es compatible con varios motores de bases de datos, incluidos Oracle, SQL Server y PostgresSQL, como orígenes.

Epics

Preparación para la migración

Tarea	Descripción	Habilidades requeridas
Valide las versiones de las bases de datos.	Valide las versiones de las bases de datos de origen y destino y asegúrese de que son compatibles con AWS DMS. Para información sobre las versiones de bases de datos de Oracle compatibles, consulte Uso de una base de datos de Oracle como fuente para AWS DMS. Para obtener información acerca del uso de Amazon Redshift como destino, consulte Uso de una base de datos de Amazon Redshift como destino de AWS DMS.	Administrador de base de datos
Crear una VPC y un grupo de seguridad.	En su cuenta de AWS, cree una nube privada virtual (VPC), si no existe. Cree un grupo de seguridad para el tráfico saliente para las bases de datos de origen y	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	destino. Para más información, consulte la documentación de Amazon Virtual Private Cloud (Amazon VPC).	
Instale AWS SCT.	Descargue e instale la versión más reciente de AWS SCT y sus controladores correspondientes. Para más información, consulte Instalación, verificación y actualización de AWS SCT.	Administrador de base de datos
Cree un usuario para la tarea de AWS DMS.	Cree un usuario de AWS DMS en la base de datos de origen y concédale privilegios de LECTURA. AWS SCT y AWS DMS utilizarán este usuario.	Administrador de base de datos
Pruebe la conectividad de la base de datos.	Probar la conectividad con la instancia de base de datos de Oracle.	Administrador de base de datos
Cree un proyecto nuevo en AWS SCT.	Abra la herramienta AWS SCT y cree un proyecto nuevo.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Analice el esquema de Oracle que se va a migrar.	Utilice AWS SCT para analizar el esquema que se va a migrar y generar un informe de evaluación de la migración de la base de datos. Para obtener más información, consulte Creación de un informe de evaluación de la migración de bases de datos en la documentación de AWS SCT.	Administrador de base de datos
Revise el informe de evaluación.	Revise el informe para comprobar la viabilidad de la migración. Es posible que algunos objetos de base de datos requieran una conversión manual. Para más información sobre el informe, consulte Ver el informe de evaluación en la documentación de AWS SCT.	Administrador de base de datos

Prepare la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Crear un clúster de Amazon Redshift.	Cree un clúster de Amazon Redshift en la VPC que creó anteriormente. Para obtener más información, consulte Clústeres de Amazon Redshift en la documentación de Amazon Redshift.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree usuarios de bases de datos.	Extraiga la lista de usuarios, roles y concesiones de la base de datos de origen de Oracle. Cree usuarios en la base de datos Amazon Redshift de destino y aplique las funciones del paso anterior.	Administrador de base de datos
Evaluar los parámetros de la base de datos.	Revise las opciones, los parámetros, los archivos de red y los enlaces a las bases de datos de la base de datos de origen de Oracle y evalúe su aplicabilidad al destino.	Administrador de base de datos
Aplique cualquier configuración pertinente a la base de datos de destino.	Para obtener más información acerca de este paso, consulte Referencia de configuración en la documentación de Amazon Redshift.	Administrador de base de datos

Crear usuarios en la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Cree un usuario de AWS DMS en la base de datos de destino.	Cree un usuario de AWS DMS en la base de datos de destino y concédale privilegios de lectura y escritura. Valide la conectividad desde AWS SCT.	Administrador de base de datos
Convierta el esquema, revise el informe SQL y guarde los errores o advertencias.	Para obtener más información, consulte Convertir esquemas de bases de datos mediante	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	AWS SCT en la documenta ción de AWS SCT.	
Aplique los cambios de esquema a la base de datos de destino o guárdelos como un archivo .sql.	Para obtener instrucciones, consulte Guardar y aplicar el esquema convertido en AWS SCT en la documentación de AWS SCT.	Administrador de base de datos
Valide los objetos de la base de datos de destino.	Valide los objetos que se crearon en el paso anterior en la base de datos de destino. Reescriba o rediseñe los objetos que no se hayan convertido correctamente.	Administrador de base de datos
Deshabilite las claves y los desencadenadores externos.	Deshabilite cualquier clave y desencadenador externo. Esto puede provocar problemas de carga de datos durante el proceso de carga completa cuando se ejecuta AWS DMS.	Administrador de base de datos

Migración de datos utilizando AWS DMS

Tarea	Descripción	Habilidades requeridas
Cree una instancia de replicaci ón de AWS DMS.	Inicie sesión en la Consola de administración de AWS y abra la consola de AWS DMS. En el panel de navegació n, seleccione Instancias de replicación y Crear instancia de replicación. Para obtener instrucciones detalladas,	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	consulte el paso 1 de la Introducción a AWS DMS en la documentación de AWS DMS.	
Cree puntos de conexión de origen y destino.	Cree puntos de conexión de origen y destino, pruebe la conexión desde la instancia de replicación a los puntos de conexión de origen y destino. Para obtener instrucciones detalladas, consulte el paso 2 de la Introducción a AWS DMS en la documentación de AWS DMS.	Administrador de base de datos
Cree una tarea de replicación.	Cree una tarea de replicación y seleccione el método de migración adecuado. Para obtener instrucciones detalladas, consulte el paso 3 de la Introducción a AWS DMS en la documentación de AWS DMS.	Administrador de base de datos
Iniciar la tarea de replicación.	Inicie la tarea de replicación y supervise los registros para detectar cualquier error.	Administrador de base de datos

Migración de la aplicación

Tarea	Descripción	Habilidades requeridas
Cree servidores de aplicaciones.	Cree los nuevos servidores de aplicaciones en AWS.	Propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Migre el código de la aplicación.	Migre el código de la aplicación a los nuevos servidores.	Propietario de la aplicación
Configure los servidores de aplicaciones.	Configure el servidor de aplicaciones para los controladores y la base de datos de destino.	Propietario de la aplicación
Optimice el código de la aplicación.	Optimice el código de la aplicación para la base de datos de destino.	Propietario de la aplicación

Realizar la transición a la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Valide a los usuarios.	En la base de datos de Amazon Redshift de destino, valide a los usuarios y asígneles funciones y privilegios.	Administrador de base de datos
Valide que la aplicación esté bloqueada.	Asegúrese de que la aplicación esté bloqueada para evitar más cambios.	Propietario de la aplicación
Valide los datos.	Valide los datos de la base de datos Amazon Redshift de destino.	Administrador de base de datos
Habilite las claves y los desencadenadores externos.	Habilite las claves y los desencadenadores externos en la base de datos de Amazon Redshift de destino.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Conéctese a la nueva base de datos.	Configure la aplicación para conectarse a la nueva base de datos de Amazon Redshift.	Propietario de la aplicación
Realice las comprobaciones finales.	Realice una comprobación final y exhaustiva del sistema antes de la puesta en marcha.	Administrador de base de datos, propietario de la aplicación
Realice la puesta en marcha.	Póngalo en marcha con la base de datos de Amazon Redshift de destino.	Administrador de base de datos

Cerrar el proyecto de migración

Tarea	Descripción	Habilidades requeridas
Cerrar los recursos temporales de AWS.	Cierre los recursos temporales de AWS, como la instancia de replicación de AWS DMS y la instancia de EC2 utilizadas para AWS SCT.	Administrador de base de datos, administrador de sistemas
Revise los documentos.	Revise y valide los documentos del proyecto de migración.	Administrador de base de datos, administrador de sistemas
Recopile métricas.	Recopile información sobre el proyecto de migración, como el tiempo de migración, el porcentaje de tareas manuales en comparación con las tareas automatizadas y el ahorro total de costos.	Administrador de base de datos, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Cerrar el proyecto.	Cerrar el proyecto y enviar comentarios.	Administrador de base de datos, administrador de sistemas

Recursos relacionados

Referencias

- Guía del usuario de AWS DMS
- Guía del usuario de AWS SCT
- Guía de introducción a Amazon Redshift

Tutoriales y videos

- Conozca en profundidad AWS SCT y AWS DMS (presentación de AWS re:Invent 2019)
- Introducción a AWS Database Migration Service (AWS DMS)

Migrar una base de datos de Oracle a Aurora PostgreSQL con AWS DMS y AWS SCT

Creado por Senthil Ramasamy (AWS)

Entorno: PoC o piloto	Origen: base de datos de Oracle	Destino: Amazon Aurora compatible con PostgreSQL
Tipo R: renovar arquitectura	Carga de trabajo: Oracle	Tecnologías: Migración; bases de datos
Servicios de AWS: Amazon Aurora		

Resumen

Este patrón describe cómo migrar una base de datos de Oracle a una edición compatible con PostgreSQL de Amazon Aurora mediante AWS Data Migration Service (AWS DMS) y la la Herramienta de conversión de esquemas de AWS (AWS SCT).

El patrón abarca las bases de datos Oracle de origen que se encuentran en las instalaciones, las bases de datos Oracle que están instaladas en instancias de Amazon Elastic Compute Cloud (Amazon EC2) y Amazon Relational Database Service (Amazon RDS) para las bases de datos Oracle. El patrón convierte estas bases de datos en compatibles con Aurora PostgreSQL.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una base de datos de Oracle en un centro de datos en las instalaciones o en la nube de AWS.
- Los clientes de SQL se instalan en una máquina local o en una instancia EC2.
- Controladores de conectividad de bases de datos Java (JDBC) para conectores de AWS SCT instalados en un equipo local o en la instancia de EC2 en la que está instalado AWS SCT.

Limitaciones

- Límite de tamaño de la base de datos: 128 TB
- Si la base de datos de origen admite una aplicación comercial off-the-shelf (COTS) o es específica del proveedor, es posible que no pueda convertirla en otro motor de base de datos. Antes de usar este patrón, confirme que la aplicación es compatible con Aurora PostgreSQL.

Versiones de producto

- Para las bases de datos Oracle autogestionadas, AWS DMS admite todas las ediciones de bases de datos Oracle para las versiones 10.2 y posteriores (para las versiones 10.x), 11g y hasta 12.2, 18c y 19c. Para ver la lista más reciente de las versiones de las bases de datos de Oracle compatibles (tanto autogestionadas como de Amazon RDS para Oracle), consulte Uso de una base de datos Oracle como fuente para AWS DMS y Uso de una base de datos PostgreSQL como destino para AWS DMS.
- Le recomendamos utilizar la versión más reciente de AWS DMS para obtener el soporte más completo de versiones y características. Para obtener información sobre las versiones de bases de datos Oracle compatibles con AWS SCT, consulte la documentación de AWS SCT.
- Aurora es compatible con las versiones de PostgreSQL incluidas en las versiones de Amazon Aurora PostgreSQL y versiones del motor.

Arquitectura

Pila de tecnología de origen

Uno de los siguientes:

- Una base de datos Oracle en las instalaciones
- Una base de datos Oracle en una instancia EC2
- Una instancia de base de datos de Amazon RDS para Oracle

Pila de tecnología de destino

- Aurora compatible con PostgreSQL

Arquitectura de destino

Arquitectura de migración de datos

- Desde una base de datos de Oracle en ejecución en la nube de AWS

- Desde una base de datos de Oracle en ejecución en un centro de datos en las instalaciones

Herramientas

- AWS Database Migration Service (AWS DMS) le permite migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones.
- Herramienta de conversión de esquemas de AWS (AWS SCT) simplifica las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado a un formato compatible con la base de datos de destino.

Epics

Preparar la migración

Tarea	Descripción	Habilidades requeridas
Prepare la base de datos de origen.	Para preparar la base de datos de origen, consulte Uso de Oracle Database como un origen para AWS SCT en la documentación de AWS SCT.	Administrador de base de datos
Cree una instancia de EC2 para AWS SCT.	Cree y configure una instancia de EC2 para AWS SCT, si es necesario.	Administrador de base de datos
Descargue AWS SCT.	Descargue la versión más reciente de AWS SCT y los controladores asociados. Para obtener más información, consulte Instalación, verificac	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	ión y actualización de AWS SCT en la documentación de AWS SCT.	
Añada usuarios y permisos.	Agregue y valide los usuarios y permisos necesarios en la base de datos de origen.	Administrador de base de datos
Cree un proyecto de AWS SCT.	Cree un proyecto de AWS SCT para la carga de trabajo y conéctese a la base de datos de origen. Para obtener instrucciones, consulte Creación de un proyecto de AWS SCT y Adición de servidores de bases de datos en la documentación de AWS SCT.	Administrador de base de datos
Evalúe la viabilidad.	Genere un informe de evaluación que resuma las medidas a tomar en el caso de los esquemas que no se pueden convertir automátic amente y proporcione estimaciones de los esfuerzos de conversión manual. Para obtener más información, consulte Creación y revisión del informe de evaluación de la migración de bases de datos en la documentación de AWS SCT.	Administrador de base de datos

Prepare la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Crear una instancia de base de datos de Amazon RDS de destino.	Cree una instancia de base de datos de Amazon RDS de destino con Amazon Aurora como motor de base de datos. Para obtener más informaci ón, consulte Creación de una instancia de base de datos de Amazon RDS en la documentación de Amazon RDS.	Administrador de base de datos
Extraiga usuarios, roles y permisos.	Extraiga la lista de usuarios, roles y permisos de la base de datos de origen.	Administrador de base de datos
Asigne usuarios.	Asigne los usuarios existente s de la base de datos a los nuevos usuarios de la base de datos.	Propietario de la aplicación
Crear usuarios.	Cree usuarios en la base de datos de destino.	Administrador de base de datos, propietario de la aplicación
Aplique roles.	Aplique los roles del paso anterior a la base de datos de destino.	Administrador de base de datos
Compruebe las opciones, los parámetros, los archivos de red y los enlaces a las bases de datos.	Revise la base de datos de origen para ver las opciones, los parámetros, los archivos de red y los enlaces a la base de datos y, a continuación,	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	evalúe su aplicabilidad a la base de datos de destino.	
Aplique la configuración.	Aplique cualquier configura ción relevante a la base de datos de destino.	Administrador de base de datos

Transferir objetos

Tarea	Descripción	Habilidades requeridas
Configure la conectividad de AWS SCT.	Configure la conectividad de AWS SCT con la base de datos de destino.	Administrador de base de datos
Convierta el esquema con AWS SCT.	AWS SCT convierte automátic amente el esquema de la base de datos de origen y la mayor parte del código personalizado a un formato compatible con la base de datos de destino. El código que la herramienta no puede convertir automátic amente está marcado de forma clara para que pueda convertirlo manualmente.	Administrador de base de datos
Revise el informe.	Revise el informe SQL generado y guarde los errores y advertencias.	Administrador de base de datos
Aplique cambios de esquema automatizados.	Aplique los cambios de esquema automatizados a la base de datos de	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	destino o guárdelos como un archivo .sql.	
Valide objetos.	Valide que AWS SCT haya creado los objetos en el destino.	Administrador de base de datos
Gestione los elementos que no se hayan convertido.	Reescriba, rechace o rediseñe manualmente cualquier elemento que no se haya podido convertir automátic amente.	Administrador de base de datos, propietario de la aplicación
Aplique permisos de usuario y rol.	Aplique los permisos de usuario y rol generados, y revise las excepciones.	Administrador de base de datos

Migrar datos

Tarea	Descripción	Habilidades requeridas
Determine el método.	Determine el método para migrar los datos.	Administrador de base de datos
Crear una instancia de replicación.	Cree una instancia de replicaci ón desde la consola de AWS DMS. Para obtener más información, consulte Trabajar con una instancia de replicación de AWS DMS en la documentación de AWS DMS.	Administrador de base de datos
Cree los puntos de conexión de origen y de destino.	Para crear puntos de conexión, siga las instrucci ones de Creación de puntos de conexión de origen y	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	destino en la documentación de AWS DMS.	
Cree una tarea de replicación.	Para crear una tarea, consulte Trabajar con tareas de AWS DMS en la documentación de AWS DMS.	Administrador de base de datos
Inicie la tarea de replicación y supervise los registros.	Para obtener más informaci ón sobre este paso, consulte Monitorización de las tareas de AWS DMS en la documentación de AWS DMS.	Administrador de base de datos

Migrar la aplicación

Tarea	Descripción	Habilidades requeridas
Analice y convierta los elementos SQL en el código de la aplicación.	Use AWS SCT para analizar y convertir los elementos de SQL en el código de la aplicación. Al convertir su esquema de base de datos de un motor a otro, también deberá actualizar el código SQL de las aplicaciones para interactuar con el nuevo motor de base de datos en lugar del antiguo. Puede ver, analizar, editar y guardar el código SQL convertido.	Propietario de la aplicación
Cree servidores de aplicacio nes.	Cree los nuevos servidores de aplicaciones en AWS.	Propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Migre el código de la aplicació n.	Migre el código de la aplicació n a los nuevos servidores.	Propietario de la aplicación
Configure los servidores de aplicaciones.	Configure los servidores de aplicaciones para los controladores y la base de datos de destino.	Propietario de la aplicación
Corrija el código.	Corrija cualquier código específico del motor de base de datos de origen de su aplicación.	Propietario de la aplicación
Optimice el código.	Optimice el código de su aplicación para el motor de base de datos de destino.	Propietario de la aplicación

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Realizar la transición a la base de datos de destino.	Realice la transición a la nueva base de datos.	Administrador de base de datos
Bloquee la aplicación.	Bloquee la aplicación frente a cualquier cambio.	Propietario de la aplicación
Valide los cambios.	Valide que todos los cambios se hayan propagado a la base de datos de destino.	Administrador de base de datos
Redirigir a la base de datos de destino.	Apunte los nuevos servidores de la aplicación hacia la base de datos de destino.	Propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Compruebe todo.	Realice una verificación final y exhaustiva del sistema.	Propietario de la aplicación
Realice la puesta en marcha	Complete las tareas finales de la transición.	Propietario de la aplicación

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cerrar los recursos temporales de AWS.	Cierre los recursos temporales de AWS, como la instancia de replicación de AWS DMS y la instancia de EC2 utilizadas para AWS SCT.	Administrador de base de datos, propietario de la aplicación
Actualice los comentarios.	Actualice los comentarios sobre el proceso de AWS DMS para los equipos internos.	Administrador de base de datos, propietario de la aplicación
Revise el proceso y las plantillas.	Revise el proceso de AWS DMS y mejore la plantilla si es necesario.	Administrador de base de datos, propietario de la aplicación
Valide los documentos.	Revise y valide los documentos del proyecto.	Administrador de base de datos, propietario de la aplicación
Recopile métricas.	Recopile métricas para evaluar el tiempo de migración, el porcentaje de esfuerzo manual frente al automatizado, el ahorro de costos, etc.	Administrador de base de datos, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Cierre el proyecto.	Cierre el proyecto de migración y envíe comentarios a las partes interesadas.	Administrador de base de datos, propietario de la aplicación

Recursos relacionados

Referencias

- Uso de una base de datos de Oracle como origen para AWS DMS
- Utilizar una base de datos PostgreSQL como objetivo para el servicio de migración de bases de datos de AWS
- Manual de migración de Oracle Database 11g/12c a Amazon Aurora con compatibilidad con PostgreSQL (9.6.x)
- Manual de migración de Oracle Database 19c a Amazon Aurora con compatibilidad con PostgreSQL (12.4)
- Migración de una base de datos de Amazon RDS para Oracle a una edición compatible con Amazon Aurora PostgreSQL
- AWS Data Migration Service
- Schema Conversion Tool de AWS
- Migre de Oracle a Amazon Aurora
- Precios de Amazon RDS

Tutoriales y videos

- Explicación paso a paso de Database Migration
- Introducción a AWS DMS
- Introducción a Amazon RDS
- AWS Data Migration Service (vídeo)
- Migración de una base de datos Oracle a PostgreSQL (vídeo)

Información adicional

.

Migre datos de una base de datos Oracle en las instalaciones a Aurora PostgreSQL

Creado por Michelle Deng (AWS) y Shunan Xiang (AWS)

Entorno: PoC o piloto	Origen: Oracle	Destino: Aurora (compatible con PostgreSQL)
Tipo R: renovar arquitectura	Carga de trabajo: Oracle	Tecnologías: Migración; bases de datos
Servicios de AWS: Amazon Aurora; AWS DMS; AWS SCT		

Resumen

Este patrón proporciona orientación para la migración de datos de una base de datos Oracle en las instalaciones a una edición de Amazon Aurora compatible con PostgreSQL. Se basa en una estrategia de migración de datos en línea con un tiempo de inactividad mínimo para bases de datos Oracle de varios terabytes que contienen tablas grandes con un alto nivel de actividad de lenguaje de manipulación de datos (DML). Emplea una base de datos en espera de Oracle Active Data Guard como fuente para reducir la migración de datos de la base de datos principal. La replicación de la base de datos principal de Oracle a la base de datos en espera se puede suspender durante la carga completa para evitar errores ORA-01555.

Las columnas de tabla de claves principales (PK) o claves externas (FK), con el tipo de dato NUMBER, se usan habitualmente para almacenar números enteros en Oracle. Le recomendamos que los convierta a INT o BIGINT en PostgreSQL para obtener un mejor rendimiento. Puede usar la Herramienta de conversión de esquemas de AWS (AWS SCT) para cambiar la asignación de tipos de datos por defecto en las columnas PK y FK. (Para obtener más información, consulte la publicación del blog de AWS Convertir el tipo de datos NUMBER de Oracle a PostgreSQL). La migración de datos de este patrón usa AWS Database Migration Service (AWS DMS) tanto para la captura de datos a carga completa como para la captura de datos de cambios (CDC).

También puede usar este patrón para migrar una base de datos Oracle en las instalaciones a Amazon Relational Database Service (Amazon RDS) para PostgreSQL, o bien una base de datos

Oracle alojada en Amazon Elastic Compute Cloud (Amazon EC2) a Amazon RDS para PostgreSQL o Aurora compatible con PostgreSQL.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos de origen de Oracle en un centro de datos en las instalaciones con Active Data Guard configurado en modo de espera
- AWS Direct Connect, configurado entre el centro de datos en las instalaciones y la nube de AWS
- Estar familiarizado con mediante una base de datos de Oracle como origen para AWS DMS
- Uso de una base de datos de PostgreSQL como destino para AWS DMS

Limitaciones

- Los clústeres de bases de datos de Amazon Aurora se pueden crear con hasta 128 TiB de almacenamiento. Las instancias de bases de datos de Amazon RDS para PostgreSQL se pueden crear con hasta 64 TiB de almacenamiento. Para obtener la información de almacenamiento más reciente, consulte Almacenamiento y fiabilidad de Amazon Aurora y Almacenamiento de instancias de base de datos de Amazon RDS en la documentación de AWS.

Versiones de producto

- AWS DMS es compatible con todas las ediciones de bases de datos Oracle para las versiones 10.2 y posteriores (para versiones 10.x), 11g y hasta 12.2, 18c y 19c. Para ver la lista actualizada de versiones compatibles, consulte Uso de una base de datos de Oracle como origen para AWS DMS en la documentación de AWS.

Arquitectura

Pila de tecnología de origen

- Bases de datos Oracle en las instalaciones con Oracle Active Data Guard standby configurado

Pila de tecnología de destino

- Aurora compatible con PostgreSQL

Arquitectura de migración de datos

Herramientas

- AWS DMS: AWS Database Migration Service (AWS DMS) admite varios tipos de bases de datos de origen y destino. Consulte Uso de una base de datos de Oracle como fuente para AWS DMS, en la documentación de AWS DMS, para obtener una lista de las versiones y ediciones de bases de datos de origen y destino de Oracle compatibles. Si AWS DMS no admite la base de datos de origen, debe seleccionar otro método para migrar los datos en la fase 6 (en la sección Epics). Nota importante: dado que se trata de una migración heterogénea, primero debe comprobar si la base de datos admite una aplicación comercial off-the-shelf (COTS). Si la aplicación es COTS, consulte al proveedor para confirmar que es compatible con Aurora PostgreSQL antes de continuar. Para obtener más información, consulte los Tutoriales de migración paso a paso de AWS DMS en la documentación de AWS.
- AWS SCT: la Herramienta de conversión de esquemas de AWS (AWS SCT) facilita las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado a un formato compatible con la base de datos de destino. El código personalizado que convierte la herramienta incluye vistas, procedimientos almacenados y funciones. Cualquier código que la herramienta no pueda convertir automáticamente está claramente marcado para que pueda convertirlo manualmente.

Epics

Planificar la migración

Tarea	Descripción	Habilidades requeridas
Valide las versiones de las bases de datos de origen y de destino.		Administrador de base de datos
Instale AWS SCT y los controladores.		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Agregue y valide la base de datos de origen de concesion es y usuarios de requisitos previos de AWS SCT.		Administrador de base de datos
Cree un proyecto de AWS SCT para la carga de trabajo y conéctese a la base de datos de origen.		Administrador de base de datos
Genere un informe de evaluación y evalúe la viabilidad.		Administrador de base de datos, propietario de la aplicación

Prepare la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Cree una base de datos de destino de Aurora compatible con PostgreSQL.		Administrador de base de datos
Extraiga la lista de concesion es, usuarios y roles de la base de datos de origen.		Administrador de base de datos
Asigne los usuarios existente s de la base de datos a los nuevos usuarios de la base de datos.		Propietario de aplicación
Cree usuarios en la base de datos de destino.		Administrador de base de datos
Aplique los roles del paso anterior a la base de datos		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
de Aurora compatible con PostgreSQL de destino.		
Revise las opciones, los parámetros, los archivos de red y los enlaces de la base de datos de origen, y evalúe su aplicabilidad a la base de datos de destino.		Administrador de base de datos, propietario de la aplicación
Aplique cualquier configura ción relevante a la base de datos de destino.		Administrador de base de datos

Prepare para la conversión del código de objetos de la base de datos

Tarea	Descripción	Habilidades requeridas
Configure la conectividad de AWS SCT con la base de datos de destino.		Administrador de base de datos
Convierta el esquema en AWS SCT y guarde el código convertido como archivo .sql.		Administrador de base de datos, propietario de la aplicación
Convierta manualmente cualquier objeto de base de datos que no se haya podido convertir automáticamente.		Administrador de base de datos, propietario de la aplicación
Optimice la conversión del código de la base de datos.		Administrador de base de datos, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Divida el archivo .sql en varios archivos .sql según el tipo de objeto.		Administrador de base de datos, propietario de la aplicación
Valide los scripts SQL en la base de datos de destino.		Administrador de base de datos, propietario de la aplicación

Prepárese para la migración de datos

Tarea	Descripción	Habilidades requeridas
Cree una instancia de replicación de AWS DMS.		Administrador de base de datos
Crear los puntos de conexión de origen y de destino.	Si el tipo de datos de los PK y FK se convierte de NUMBER en Oracle a BIGINT en PostgreSQL, considere la posibilidad de especificar el atributo de conexión `numberDataTypeScale=-2` al crear el punto de conexión de origen.	Administrador de base de datos

Migre los datos: carga completa

Tarea	Descripción	Habilidades requeridas
Cree el esquema y las tablas en la base de datos de destino.		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree tareas de carga completa de AWS DMS agrupando tablas o dividiendo una tabla grande en función de su tamaño.		Administrador de base de datos
Detenga las aplicaciones en las bases de datos Oracle de origen durante un breve período.		Propietario de aplicación
Compruebe que la base de datos en espera de Oracle esté sincronizada con la base de datos principal y detenga la replicación de la base de datos principal a la base de datos en espera.		Administrador de base de datos, propietario de la aplicación
Inicie las aplicaciones en la base de datos Oracle de origen.		Propietario de aplicación
Inicie las tareas de carga completa de AWS DMS en paralelo desde la base de datos en espera de Oracle hasta la base de datos de Aurora compatible con PostgreSQL.		Administrador de base de datos
Cree los PK y los índices secundarios una vez finalizada la carga completa.		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Valide los datos.		Administrador de base de datos

Migre datos — CDC

Tarea	Descripción	Habilidades requeridas
Cree tareas de replicación continua de AWS DMS especificando la hora de inicio de CDC o el número de cambio de sistema (SCN) personalizados cuando el modo de espera de Oracle se sincronizó con la base de datos principal y antes de que se reiniciaran las aplicaciones en la tarea anterior.		Administrador de base de datos
Inicie las tareas de AWS DMS en paralelo para replicar los cambios en curso de la base de datos en espera Oracle a la base de datos Aurora compatible con PostgreSQL.		Administrador de base de datos
Restablezca la replicación de la base de datos principal de Oracle a la base de datos en espera.		Administrador de base de datos
Supervise los registros y detenga las aplicaciones en la base de datos de Oracle cuando la base de datos de		Administrador de base de datos, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
destino de Aurora compatibl e con PostgreSQL esté casi sincronizada con la base de datos Oracle de origen.		
Detenga las tareas de AWS DMS cuando el destino esté completamente sincronizado con la base de datos Oracle de origen.		Administrador de base de datos
Cree los FK y valide los datos en la base de datos de destino.		Administrador de base de datos
Cree funciones, vistas, desencadenantes, secuencia s y otros tipos de objetos en la base de datos de destino.		Administrador de base de datos
Aplique las concesiones de funciones en la base de datos de destino.		Administrador de base de datos

Migrar la aplicación

Tarea	Descripción	Habilidades requeridas
Use AWS SCT para analizar y convertir las instrucciones SQL del código de la aplicació n.		Propietario de aplicación
Cree nuevos servidores de aplicaciones en AWS.		Propietario de aplicación

Tarea	Descripción	Habilidades requeridas
Migre el código de la aplicación a los nuevos servidores.		Propietario de aplicación
Configure el servidor de aplicaciones para los controladores y la base de datos de destino.		Propietario de aplicación
Corrija cualquier código específico del motor de base de datos de origen de la aplicación.		Propietario de aplicación
Optimice el código de la aplicación para la base de datos de destino.		Propietario de aplicación

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Apunte el nuevo servidor de la aplicación hacia la base de datos de destino.		Administrador de base de datos, propietario de la aplicación
Realice comprobaciones de estado.		Administrador de base de datos, propietario de la aplicación
Realice la puesta en marcha		Administrador de base de datos, propietario de la aplicación

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cerrar los recursos temporales de AWS.		Administrador de base de datos, administrador de sistemas
Revise y valide los documentos del proyecto.		Administrador de base de datos, propietario de la aplicación
Recopile métricas sobre el tiempo necesario para migrar, el porcentaje de uso manual frente al uso de herramientas, el ahorro de costos y datos similares.		Administrador de base de datos, propietario de la aplicación
Cerrar el proyecto y enviar comentarios.		Administrador de base de datos, propietario de la aplicación

Recursos relacionados

Referencias

- Base de datos Oracle a Aurora compatible con PostgreSQL: manual de procedimientos para la migración
- Migración de una base de datos de Amazon RDS para Oracle a Amazon Aurora MySQL
- Sitio web de AWS DMS
- Documentación de AWS DMS
- Sitio web de AWS SCT
- Documentación de AWS SCT
- Migre de Oracle a Amazon Aurora

Tutoriales

- Introducción a AWS DMS
- Introducción a Amazon RDS
- Explicación paso a paso de AWS Database Migration Service (AWS DMS)

Migración de SAP ASE a Amazon RDS para SQL Server utilizando AWS DMS

Creado por Amit Kumar (AWS)

Entorno: PoC o piloto	Origen: SAP ASE	Destino: Amazon RDS para SQL Server
Tipo R: renovar arquitectura	Carga de trabajo: SAP	Tecnologías: Migración; Bases de datos; Moderniza ción
Servicios de AWS: Amazon RDS; AWS DMS		

Resumen

Este patrón proporciona orientación para migrar una base de datos de SAP Adaptive Server Enterprise (ASE) a una instancia de base de datos de Amazon Relational Database Service (Amazon RDS) que ejecute Microsoft SQL Server. La base de datos de origen puede estar ubicada en un centro de datos en las instalaciones o en una instancia de Amazon Elastic Compute Cloud (Amazon EC2). El patrón utiliza AWS Database Migration Service (AWS DMS) para migrar datos y (de forma opcional) herramientas de ingeniería de software asistida por computadora (CASE) para convertir el esquema de base de datos.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos SAP ASE en un centro de datos en las instalaciones o en una instancia EC2
- Una base de datos de Amazon RDS para SQL Server de destino que esté en funcionamiento

Limitaciones

- Límite de tamaño de la base de datos: 64 TB

Versiones de producto

- Solo para SAP ASE, versión 15.7 o 16.x. Para obtener la información más reciente, consulte Uso de una base de datos de SAP como origen para AWS DMS.
- Para las bases de datos de destino de Amazon RDS, AWS DMS admite las versiones de Microsoft SQL Server en Amazon RDS para las ediciones Enterprise, Standard, Web y Express. Para obtener la información más reciente sobre las versiones compatibles, consulte la documentación de AWS DMS. Le recomendamos utilizar la versión más reciente de AWS DMS para obtener el soporte más completo de versiones y características.

Arquitectura

Pila de tecnología de origen

- Una base de datos de SAP ASE que se encuentra en las instalaciones o en una instancia de Amazon EC2

Pila de tecnología de destino

- Instancia de base de datos de Amazon RDS para SQL Server

Arquitectura de origen y destino

Desde una base de datos de SAP ASE en Amazon EC2 a una instancia de base de datos de Amazon RDS para SQL Server:

De una base de datos SAP ASE en las instalaciones a una instancia de base de datos de Amazon RDS para SQL Server:

Herramientas

- AWS Database Migration Service (AWS DMS) es un servicio web que puede utilizar para migrar datos de una base de datos en las instalaciones, de una instancia de base de datos de Amazon RDS o de una base de datos de una instancia EC2 a una base de datos de un servicio de AWS,

como Amazon RDS para SQL Server o una instancia EC2. Puede también migrar desde una base de datos de un servicio de AWS a otra base de datos local. Puede migrar datos entre motores de bases de datos heterogéneos u homogéneos.

- Para las conversiones de esquemas, puede utilizar opcionalmente erwin Data Modeler o SAP. PowerDesigner

Epics

Planificación de la migración

Tarea	Descripción	Habilidades requeridas
Valide las versiones de las bases de datos de origen y de destino.		Administrador de base de datos
Identifique los requisitos de almacenamiento (el tipo y la capacidad de almacenam iento).		DBA, SysAdmin
Elija el tipo de instancia adecuado en función de la capacidad, las características de almacenamiento y las características de red.		DBA, SysAdmin
Identifique los requisitos de seguridad de acceso a la red para las bases de datos de origen y destino.		DBA, SysAdmin
Identificar la estrategia de migración de aplicaciones.		DBA, propietario de la SysAdmin aplicación

Configuración de la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC) y subredes.		SysAdmin
Cree grupos de seguridad y listas de control de acceso (ACL) a la red.		SysAdmin
Configure e inicie una instancia de base de datos de Amazon RDS.		SysAdmin

Migración de datos: opción 1

Tarea	Descripción	Habilidades requeridas
Migre el esquema de la base de datos manualmente o utilice una herramienta CASE como Erwin Data Modeler o SAP. PowerDesigner		Administrador de base de datos

Migración de datos: opción 2

Tarea	Descripción	Habilidades requeridas
Migre datos utilizando AWS DMS.		Administrador de base de datos

Migración de la aplicación

Tarea	Descripción	Habilidades requeridas
Seguir la estrategia de migración de aplicaciones.		DBA, SysAdmin propietario de la aplicación

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Cambie los clientes de la aplicación a la nueva infraestructura.		DBA, propietario de la SysAdmin aplicación

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cerrar los recursos temporales de AWS.		DBA, SysAdmin
Revise y valide los documentos del proyecto.		DBA, propietario de la SysAdmin aplicación
Recopile métricas como el tiempo de migración, el porcentaje de esfuerzo manual en comparación con el automatizado y el ahorro de costos.		DBA, propietario de la SysAdmin aplicación
Cerrar el proyecto y enviar comentarios.		DBA, propietario de la SysAdmin aplicación

Recursos relacionados

Referencias

- Sitio web de AWS DMS
- Precios de Amazon RDS
- Uso de una base de datos SAP ASE como origen para AWS DMS
- Limitaciones de RDS Custom for SQL Server

Tutoriales y videos

- Introducción a AWS DMS
- Introducción a Amazon RDS
- AWS DMS (video)
- Amazon RDS (video)

Migre una base de datos de Microsoft SQL Server en las instalaciones a Amazon Redshift mediante AWS DMS

Creado por Marcelo Fernandes (AWS)

Entorno: PoC o piloto	Origen: Microsoft SQL Server	Destino: Amazon Redshift
Tipo R: renovar arquitectura	Carga de trabajo: Microsoft	Tecnologías: migración; bases de datos
Servicios de AWS: Amazon Redshift		

Resumen

Este patrón proporciona orientación para migrar una base de datos de Microsoft SQL Server en las instalaciones a Amazon Redshift mediante AWS Data Migration Service (AWS DMS).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos de origen de Microsoft SQL Server en un centro de datos en las instalaciones
- Requisitos previos cumplidos para usar una base de datos de Amazon Redshift como destino para AWS DMS, tal y como se describe en la documentación de AWS DMS

Versiones de producto

- Ediciones SQL Server 2005-2019, Enterprise, Standard, Workgroup, Developer y Web. Para ver la lista actualizada de versiones compatibles, consulte Usar una base de datos de Microsoft SQL Server como origen de AWS DMS en la documentación de AWS.

Arquitectura

Pila de tecnología de origen

- Base de datos de Microsoft SQL Server en las instalaciones

Pila de tecnología de destino

- Amazon Redshift

Arquitectura de migración

Herramientas

- AWS DMS es un servicio de migración de datos que admite varios tipos de bases de datos de origen y destino. Para obtener información sobre las versiones y ediciones de bases de datos de Microsoft SQL Server que se admiten para su uso con AWS DMS, consulte Uso de una base de datos de Microsoft SQL Server como fuente de AWS DMS en la documentación de AWS DMS. Si AWS DMS no es compatible con su base de datos de origen, debe seleccionar un método alternativo para la migración de datos.

Epics

Planificar la migración

Tarea	Descripción	Habilidades requeridas
Validar la versión y el motor de la base de datos de origen y de destino.		Administrador de base de datos
Identifique los requisitos de hardware de la instancia del servidor de destino.		Administrador de base de datos, administrador de sistemas
Identificar los requisitos de almacenamiento (el tipo y la capacidad de almacenam iento).		Administrador de base de datos, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Elegir el tipo de instancia correcto en función de la capacidad, las características de almacenamiento y las características de la red.		Administrador de base de datos, administrador de sistemas
Identifique los requisitos de seguridad para acceder a la red de las bases de datos de origen y destino.		Administrador de base de datos, administrador de sistemas
Identificar la estrategia de migración de aplicaciones.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Configure la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC).	Para obtener más informaci ón, consulte Trabajar con una instancia de base de datos en una VPC en la documentación de AWS.	Administrador de sistemas
Creación de los grupos de seguridad.		Administrador de sistemas
Configure e inicie un clúster de Amazon Redshift.	Para obtener más información, consulte Crear un clúster de muestra de Amazon Redshift en la documentación de Amazon Redshift.	Administrador de base de datos, administrador de sistemas

Migrar datos

Tarea	Descripción	Habilidades requeridas
Migre los datos de la base de datos de Microsoft SQL Server mediante AWS DMS.		Administrador de base de datos

Migrar la aplicación

Tarea	Descripción	Habilidades requeridas
Seguir la estrategia de migración de aplicaciones.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Cambiar los clientes de la aplicación a la nueva infraestructura.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cierre los recursos temporales.		Administrador de base de datos, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Revise y valide los documentos del proyecto.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas
Recopile métricas como el tiempo de migración, el porcentaje de esfuerzo manual frente al automatizado y el ahorro de costos.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas
Cerrar el proyecto y enviar comentarios.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Recursos relacionados

Referencias

- Documentación de AWS DMS
- Documentación de Amazon Redshift
- Precios de Amazon Redshift

Tutoriales y videos

- Introducción a AWS DMS
- Introducción a Amazon Redshift
- Uso de una base de datos de Amazon Redshift como objetivo de AWS Database Migration Service (AWS DMS)
- AWS DMS (vídeo)

Migre una base de datos en las instalaciones de Microsoft SQL Server a Amazon Redshift mediante agentes de extracción de datos de AWS SCT

Creado por Neha Thakur (AWS)

Entorno: PoC o piloto	Origen: Microsoft SQL Server	Destino: Amazon Redshift
Tipo R: renovar arquitectura	Carga de trabajo: Microsoft	Tecnologías: migración; bases de datos
Servicios de AWS: Amazon Redshift; AWS SCT		

Resumen

Este patrón describe los pasos para migrar una base de datos de origen de Microsoft SQL Server en las instalaciones a una base de datos de destino de Amazon Redshift mediante los agentes de extracción de datos de la herramienta de conversión de esquemas de AWS (AWS SCT). Un agente es un programa externo que se integra con AWS SCT, pero que lleva a cabo la transformación de datos en otro lugar e interactúa con otros servicios de AWS en su nombre.

Requisitos previos y limitaciones

Requisitos previos

- Una base de datos de origen de Microsoft SQL Server utilizada para la carga de trabajo del almacenamiento de datos en un centro de datos en las instalaciones
- Una cuenta de AWS activa.

Versiones de producto

- Microsoft SQL Server versión 2008 o posterior. Consulte la documentación de AWS SCT para ver una lista de las versiones compatibles más reciente..

Arquitectura

Pila de tecnología de origen

- Una base de datos de Microsoft SQL Server en las instalaciones

Pila de tecnología de destino

- Amazon Redshift

Arquitectura de migración

Herramientas

- La Herramienta de conversión de esquemas de AWS (AWS SCT) gestiona las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado a un formato compatible con la base de datos de destino. Cuando las bases de datos de origen y destino son muy diferentes, puede utilizar un agente SCT de AWS para realizar una transformación de datos adicional. Para obtener más información, consulte Migrar datos de un almacén de datos en las instalaciones a Amazon Redshift en la documentación de AWS.

Prácticas recomendadas

- Prácticas recomendadas para AWS SCT
- Prácticas recomendadas para Amazon Redshift

Epics

Para preparar la migración

Tarea	Descripción	Habilidades requeridas
Valide las versiones de las bases de datos de origen y de destino.		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Identifique los requisitos de hardware del servidor de destino.		DBA, SysAdmin
Identifique los requisitos de almacenamiento (como el tipo y la capacidad de almacenam iento).		DBA, SysAdmin
Elija el tipo de instancia de destino en función de la capacidad, las características de almacenamiento y las características de red.		DBA, SysAdmin
Identifique los requisitos de seguridad de acceso a la red de las bases de datos de origen y destino.		DBA, SysAdmin
Elija una estrategia de migración de aplicaciones.		DBA, propietario de la SysAdmin aplicación

Configurar la infraestructura

Tarea	Descripción	Habilidades requeridas
Creación de una nube privada virtual (VPC) y subredes.		SysAdmin
Cree los grupos de seguridad.		SysAdmin
Configure e inicie el clúster de Amazon Redshift.		SysAdmin

Migrar datos

Tarea	Descripción	Habilidades requeridas
Migre los datos con los agentes de extracción de datos de AWS SCT.		Administrador de base de datos

Migración de aplicaciones

Tarea	Descripción	Habilidades requeridas
Siga la estrategia de migración de aplicaciones elegida.		DBA, propietario de la SysAdmin aplicación

Realizar la transición a la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Cambie las aplicaciones cliente a la nueva infraestr uctura.		DBA, propietario de la SysAdmin aplicación

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cerrar los recursos temporale s de AWS.		DBA, SysAdmin
Revise y valide los documento s del proyecto.		DBA, propietario de la SysAdmin aplicación
Recopile métricas como el tiempo de migración,		DBA, propietario de la SysAdmin aplicación

Tarea	Descripción	Habilidades requeridas
el porcentaje de esfuerzo manual frente al automatiz ado, el ahorro de costos, etc.		
Cierre el proyecto y envíe sus comentarios.		DBA, propietario de la SysAdmin aplicación

Recursos relacionados

Referencias

- Guía del usuario de AWS SCT
- Uso de agentes de extracción de datos
- Precios de Amazon Redshift

Tutoriales y videos

- Introducción a la Herramienta de conversión de esquemas de AWS
- Introducción a Amazon Redshift

Migración de una base de datos de Teradata a Amazon Redshift con los agentes de extracción de datos de AWS SCT

Tipo R: renovar arquitectura	Origen: bases de datos: relacionales	Destino: Amazon Redshift
Creado por: AWS	Entorno: PoC o piloto	Tecnologías: bases de datos; migración
Servicios de AWS: Amazon Redshift		

Resumen

Este patrón muestra los pasos para migrar una base de datos de Teradata, utilizada como almacenamiento de datos en un centro de datos en las instalaciones a una base de datos de Amazon Redshift. El patrón utiliza agentes de extracción de datos de la Herramienta de conversión de esquemas de AWS (AWS SCT). Un agente es un programa externo que se integra en AWS SCT, pero que lleva a cabo la transformación de datos en otro lugar e interactúa con otros servicios de AWS en nombre del usuario.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos Teradata de origen en un centro de datos en las instalaciones

Versiones de producto

- Teradata versión 13 y posteriores. Para ver la lista más reciente de las versiones compatibles, consulte la documentación de AWS SCT.

Arquitectura

Pila de tecnología de origen

- Base de datos Teradata en las instalaciones

Pila de tecnología de destino

- Clúster de Amazon Redshift

Arquitectura de migración de datos

Herramientas

- AWS SCT: la Herramienta de conversión de esquemas de AWS (AWS SCT) gestiona las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado a un formato compatible con la base de datos de destino. Cuando las bases de datos de origen y destino son muy diferentes entre sí, puede utilizar un agente SCT de AWS para realizar una transformación de datos adicional. Para obtener más información, consulte Migración de datos de un almacén de datos en las instalaciones a Amazon Redshift en la documentación de AWS.

Epics

Preparación para la migración

Tarea	Descripción	Habilidades requeridas
Valide las versiones de las bases de datos de origen y de destino.		Administrador de base de datos
Identifique los requisitos de hardware de la instancia del servidor de destino.		DBA, SysAdmin
Identifique los requisitos de almacenamiento (como el tipo y la capacidad de almacenam iento).		DBA, SysAdmin

Tarea	Descripción	Habilidades requeridas
Elija el tipo de instancia apropiado (capacidad, características de almacenamiento y características de red).		DBA, SysAdmin
Identifique los requisitos de seguridad de acceso a la red de las bases de datos de origen y destino.		DBA, SysAdmin
Elija una estrategia de migración de aplicaciones.		DBA, propietario de la SysAdmin aplicación

Configurar la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC) y subredes.		SysAdmin
Cree grupos de seguridad.		SysAdmin
Configure e inicie el clúster de Amazon Redshift.		SysAdmin

Migración de datos

Tarea	Descripción	Habilidades requeridas
Migre los datos con los agentes de extracción de datos de AWS SCT.	Para obtener información detallada sobre el uso de los agentes de extracción de datos de AWS SCT, consulte	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	los enlaces de la sección Referencias y Ayuda.	

Migración de aplicaciones

Tarea	Descripción	Habilidades requeridas
Siga la estrategia de migración de aplicaciones elegida.		DBA, propietario de la SysAdmin aplicación

Realizar la transición a la base de datos de Amazon Redshift de destino

Tarea	Descripción	Habilidades requeridas
Cambie las aplicaciones cliente a la nueva infraestr uctura.		DBA, propietario de la SysAdmin aplicación

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cerrar los recursos temporale s de AWS.		DBA, SysAdmin
Revise y valide los documento s del proyecto.		DBA, propietario de la SysAdmin aplicación
Recopile métricas sobre el tiempo de migración , el porcentaje de tareas manuales en comparación con		DBA, propietario de la SysAdmin aplicación

Tarea	Descripción	Habilidades requeridas
las tareas automatizadas, el ahorro de costos, etc.		
Cierre el proyecto y envíe sus comentarios.		

Recursos relacionados

Referencias

- Guía del usuario de AWS SCT
- Uso de agentes de extracción de datos
- Precios de Amazon Redshift
- Convert the Teradata RESET WHEN feature to Amazon Redshift SQL (Convertir la característica RESET WHEN de Teradata a Amazon Redshift (Recomendaciones de AWS)
- Convert the Teradata NORMALIZE temporal feature to Amazon Redshift SQL (Convertir la característica temporal NORMALIZE a Amazon Redshift SQL) (Recomendaciones de AWS)

Tutoriales

- Introducción a la Herramienta de conversión de esquemas de AWS
- Introducción a Amazon Redshift

Migración de una base de datos Vertica en las instalaciones a Amazon Redshift con los agentes de extracción de datos de AWS SCT

Tipo R: renovar arquitectura	Origen: bases de datos: relacionales	Destino: Amazon Redshift
Creado por: AWS	Entorno: PoC o piloto	Tecnologías: bases de datos; migración
Servicios de AWS: Amazon Redshift		

Resumen

Este patrón proporciona orientación para migrar una base de datos Vertica en las instalaciones a un clúster de Amazon Redshift mediante los agentes de extracción de datos de la herramienta de conversión de esquemas de AWS (AWS SCT). Un agente es un programa externo que se integra con AWS SCT, pero que lleva a cabo la transformación de datos en otro lugar e interactúa con otros servicios de AWS en su nombre.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos de origen de Vertica que se utiliza para la carga de trabajo del almacenamiento de datos en un centro de datos en las instalaciones.
- Un clúster de destino de Amazon Redshift.

Versiones de producto

- Vertica (versión 7.2.2 y posterior). Para ver la lista más reciente de las versiones compatibles, consulte la documentación de AWS SCT.

Arquitectura

Pila de tecnología de origen

- Una base de datos de Vertica en las instalaciones

Pila de tecnología de destino

- Un clúster de Amazon Redshift

Arquitectura de migración de datos

Herramientas

- AWS SCT: la herramienta de conversión de esquemas de AWS (AWS SCT) gestiona las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado a un formato compatible con la base de datos de destino. Cuando las bases de datos de origen y destino son muy diferentes entre sí, puede utilizar un agente SCT de AWS para realizar una transformación de datos adicional. Para obtener más información, consulte Migración de datos de un almacén de datos en las instalaciones a Amazon Redshift en la documentación de AWS.

Epics

Preparación para la migración

Tarea	Descripción	Habilidades requeridas
Valide las versiones de las bases de datos de origen y de destino.		Administrador de base de datos
Identifique los requisitos de almacenamiento (como el tipo		DBA, SysAdmin

Tarea	Descripción	Habilidades requeridas
y la capacidad de almacenam iento).		
Elija el tipo de instancia apropiado (capacidad, características de almacenam iento y características de red).		DBA, SysAdmin
Identifique los requisitos de seguridad de acceso a la red para las bases de datos de origen y destino.		DBA, SysAdmin
Elija una estrategia de migración de aplicaciones.		DBA, propietario de la SysAdmin aplicación

Configurar la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC) y subredes.		SysAdmin
Cree grupos de seguridad.		SysAdmin
Configure e inicie un clúster de Amazon Redshift.		SysAdmin

Migración de datos

Tarea	Descripción	Habilidades requeridas
Migre los datos con los agentes de extracción de datos de AWS SCT.	Para obtener información detallada sobre el uso de los agentes de extracción de	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	datos de AWS SCT, consulte los enlaces de la sección Referencias y Ayuda.	

Migración de aplicaciones

Tarea	Descripción	Habilidades requeridas
Siga la estrategia de migración de aplicaciones elegida.		DBA, propietario de la SysAdmin aplicación

Realizar la transición a la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Cambie las aplicaciones cliente a la nueva infraestr uctura.		DBA, propietario de la SysAdmin aplicación

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cerrar los recursos temporale s de AWS.		DBA, SysAdmin
Revise y valide los documento s del proyecto.		DBA, propietario de la SysAdmin aplicación
Recopile métricas sobre el tiempo de migración , el porcentaje de tareas manuales en comparación con		DBA, propietario de la SysAdmin aplicación

Tarea	Descripción	Habilidades requeridas
las tareas automatizadas, el ahorro de costos, etc.		
Cierre el proyecto y envíe sus comentarios.		

Recursos relacionados

Referencias

- Guía del usuario de AWS SCT
- Uso de agentes de extracción de datos
- Precios de Amazon Redshift

Tutoriales y videos

- Introducción a la Herramienta de conversión de esquemas de AWS
- Introducción a Amazon Redshift

Migre aplicaciones heredadas de Oracle Pro*C a ECPG

Creado por Sai Parthasaradhi (AWS) y Mahesh Balumuri (AWS)

Entorno: PoC o piloto	Origen: Oracle	Destino: PostgreSQL
Tipo R: renovar arquitectura	Carga de trabajo: Oracle	Tecnologías: Migración; bases de datos

Resumen

La mayoría de las aplicaciones antiguas que tienen código SQL integrado utilizan el precompilador Pro*C de Oracle para acceder a la base de datos. Al migrar estas bases de datos de Oracle a Amazon Relational Database Service (Amazon RDS) para PostgreSQL o a una edición compatible con Amazon Aurora PostgreSQL, debe convertir el código de la aplicación a un formato que sea compatible con el precompilador de PostgreSQL, que se denomina ECPG. Este patrón describe cómo convertir el código de Oracle Pro*C a su equivalente en PostgreSQL ECPG.

Para obtener más información sobre Pro*C, consulte la documentación de Oracle. Para obtener una breve introducción al ECPG, consulte la sección Información adicional.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una base de datos compatible con Amazon RDS para PostgreSQL o Aurora PostgreSQL
- Una base de datos Oracle que se ejecuta en las instalaciones

Herramientas

- Los paquetes de PostgreSQL que se enumeran en la siguiente sección.
- AWS CLI: la Interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto para interactuar con los servicios de AWS mediante comandos en el intérprete de comandos de línea de comandos. Con una configuración mínima, puede ejecutar comandos de la CLI de AWS que implementan una funcionalidad equivalente a la proporcionada por la consola de administración de AWS basada en navegador desde un símbolo del sistema.

Epics

Configurar el entorno de compilación en CentOS o RHEL

Tarea	Descripción	Habilidades requeridas
Instale los paquetes de PostgreSQL.	Instale los paquetes PostgreSQL necesarios utilizando los siguientes comandos. `yum update -y` `yum install -y yum-utils` `rpm -ivh https://download.postgresql.org/pub/repos/yum/reporpms/EL-8-x86_64/pgdg-redhat-repo-latest.noarch.rpm` `dnf -qy module disable postgresql`	Desarrollador de aplicaciones, DevOps ingeniero
Instale los archivos de encabezado y las bibliotecas.	Instale el paquete `postgresql12-devel` , que contiene bibliotecas y archivos de encabezado, mediante los siguientes comandos. Instale el paquete tanto en el entorno de desarrollo como en el de tiempo de ejecución para evitar errores en el entorno de ejecución. `dnf -y install postgresql12-devel` `yum install ncompress zip ghostscript jq unzip wget git -y`	Desarrollador de aplicaciones, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Solo para el entorno de desarrollo, ejecute también los siguientes comandos. `yum install zlib-devel make -y` `ln -s /usr/pgsql-12/bin/ecpg /usr/bin/`	
Configure la variable de ruta del entorno.	Establezca la ruta del entorno para las bibliotecas cliente de PostgreSQL. `export PATH=$PATH:/usr/pgsql-12/bin`	Desarrollador de aplicaciones, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Instale software adicional según sea necesario.	Si es necesario, instale PGLoader como reemplazo de SQL*Loader en Oracle. `wget -O /etc/yum.repos.d/pgloader-ccl.repo https://dl.packager.io/srv/opf/pgloader-ccl/master/installer/el/7.repo` `yum install pgloader-ccl -y` `ln -s /opt/pgloader-ccl/bin/pgloader /usr/bin/` Si llama a alguna aplicación Java desde un módulo Pro*C, instale Java. `yum install java -y` Instale ant para compilar el código Java. `yum install ant -y`	Desarrollador de aplicaciones, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Instale la AWS CLI.	Instale la CLI de AWS para ejecutar comandos que interactúen con servicios de AWS de como AWS Secrets Manager y Amazon Simple Storage Service (Amazon S3) desde sus aplicaciones. `cd /tmp/` `curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"` `unzip awscliv2.zip` `./aws/install -i /usr/local/aws-cli -b /usr/local/bin --update`	Desarrollador de aplicaciones, DevOps ingeniero
Identifique los programas que se convertirán.	Identifique las aplicaciones que desea convertir de Pro*C a ECPG.	Desarrollador de aplicaciones, propietario de la aplicación

Convertir el código Pro*C a ECPG

Tarea	Descripción	Habilidades requeridas
Elimine los encabezados no deseados.	Elimine los encabezados `include` que no sean necesarios en PostgreSQL, como `oci.h`, `oratypes` y `sqlda`.	Propietario de la aplicación, desarrollador de la aplicación
Actualice las declaraciones de variables.	Agregue instrucciones `EXEC SQL` para todas las declaraciones de variables que se	Desarrollador de aplicaciones, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	utilizan como variables de host. Elimine de la aplicación las declaraciones `EXEC SQL VAR` como las siguientes. `EXEC SQL VAR query IS STRING(2048);`	

Tarea	Descripción	Habilidades requeridas
Actualice la funcionalidad ROWNUM.	La función `ROWNUM` no está disponible en PostgreSQL. Sustituya esto con la función de ventana `ROW_NUMBER` en las consultas SQL. Código Pro*C: `SELECT SUBSTR(RT RIM(FILE_NAME,'.tx t'),12) INTO :gcpclFil eseq FROM (SELECT FILE_NAME FROM DEMO_FILES_TABLE WHERE FILE_NAME LIKE '%POC%' ORDER BY FILE_NAME DESC) FL2 WHERE ROWNUM <=1 ORDER BY ROWNUM;` Código ECPG: `SELECT SUBSTR(RT RIM(FILE_NAME,'.tx t'),12) INTO :gcpclFil eseq FROM (SELECT FILE_NAME , ROW_NUMBE R() OVER (ORDER BY FILE_NAME DESC) AS ROWNUM FROM demo_sche ma.DEMO_FILES_TABLE WHERE FILE_NAME LIKE '%POC%' ORDER BY FILE_NAME DESC) FL2`	Desarrollador de aplicaciones, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	`WHERE ROWNUM <=1 ORDER BY ROWNUM;`	
Actualice los parámetros de la función para usar variables de alias.	En PostgreSQL, los parámetros de las funciones no se pueden usar como variables de host. Sobrescríbalos mediante una variable de alias. Código Pro*C: `int processData(int referenceId){ EXEC SQL char col_val[100]; EXEC SQL select column_name INTO :col_val from table_name where col=:referenceId; }` Código ECPG: `int processData(int referenceIdParam){ EXEC SQL int referenceId = referenceIdParam; EXEC SQL char col_val[100]; EXEC SQL select column_name INTO :col_val from table_name where col=:referenceId; }`	Desarrollador de aplicaciones, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Actualice los tipos de estructura.	Defina los tipos de `struct` en los boques `EXEC SQL BEGIN` y `END` con `typedef` si las variables de tipo `struct` se utilizan como variables de host. Si los tipos de `struct` están definidos en los archivos de encabezado (`.h`), incluya los archivos con instrucciones `EXEC SQL include`. Código Pro*C: Archivo de encabezado (`demo.h`) `struct s_partition_ranges { char sc_table_group[31]; char sc_table_name[31]; char sc_range_value[10]; }; struct s_partition_ranges_ind { short ss_table_group; short ss_table_name; short ss_range_value; };` Código ECPG:	Desarrollador de aplicaciones, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	Archivo de encabezado (`demo.h`) `EXEC SQL BEGIN DECLARE SECTION;` `typedef struct` `{` `  char  sc_table_group[31];` `  char  sc_table_name[31];` `  char  sc_range_value[10];` `} s_partition_ranges;` `typedef struct` `{` `  short  ss_table_group;` `  short  ss_table_name;` `  short  ss_range_value;` `} s_partition_ranges_ind;` `EXEC SQL END DECLARE SECTION;` Archivo Pro*C (`demo.pc`) `#include "demo.h"` `struct s_partition_ranges gc_partition_data[MAX_PART_TABLE] ;` `struct s_partition_ranges_ind gc_partition_data_ind[MAX_PART_TABLE] ;` Archivo ECPG (`demo.pc`)	

Tarea	Descripción	Habilidades requeridas
	`exec sql include "demo.h"` `EXEC SQL BEGIN DECLARE SECTION;` `s_partition_ranges gc_partition_data[MAX_PART_TABLE] ;` `s_partition_ranges_ind gc_partition_data_ind[MAX_PART_TABLE] ;` `EXEC SQL END DECLARE SECTION;`	

Tarea	Descripción	Habilidades requeridas
Modifique la lógica para extraerla de los cursores.	Para obtener varias filas de los cursores mediante variables de matriz, cambie el código que se va a utilizar `FETCH FORWARD`. Código Pro*C: `EXEC SQL char  aPoeFiles [MAX_FILES][FILENA ME_LENGTH]; EXEC SQL FETCH filename_ cursor into :aPoeFile s;` Código ECPG: `EXEC SQL char  aPoeFiles [MAX_FILES][FILENA ME_LENGTH]; EXEC SQL int fetchSize =  MAX_FILES; EXEC SQL FETCH  FORWARD :fetchSiz e filename_cursor  into :aPoeFiles;`	Desarrollador de aplicaciones, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Modifique las llamadas a paquetes que no tienen valores de retorno.	Las funciones de los paquetes de Oracle que no tienen valores de retorno se deben llamar con una variable indicadora. Si la aplicació n incluye varias funciones que tienen el mismo nombre o si las funciones de tipo desconocido generan errores de tiempo de ejecución, clasifique los valores en los tipos de datos. Código Pro*C: `void ProcessData (char *data , int id) { EXEC SQL EXECUTE BEGIN pkg_demo. process_data (:data, :id); END; END-EXEC; }` Código ECPG: `void ProcessData (char *dataParam, int idParam ) { EXEC SQL char *data = dataParam;`	Desarrollador de aplicaciones, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	`EXEC SQL int id = idParam;` `EXEC SQL short rowInd;` `EXEC SQL short rowInd = 0;` `EXEC SQL SELECT pkg_demo.process_data (` `inp_data => :data::text,` `inp_id => :id )` `INTO :rowInd;` `}`	

Tarea	Descripción	Habilidades requeridas
Reescriba las variables SQL_CURSOR.	Reescriba la variable `SQL_CURSOR` y su implementación. Código Pro*C: `/* SQL Cursor */` `SQL_CU` `RSOR demo_cursor;` `EXEC SQL` `ALLOCATE :demo_cursor;` `EXEC SQL EXECUTE` `BEGIN` `pkg_demo.` `get_cursor(` `demo_cur=` `>:demo_cursor` `);` `END;` `END-EXEC;` Código ECPG: `EXEC SQL DECLARE` `demo_cursor CURSOR FOR` `SELECT` `* from` `pkg_demo.open_file` `name_rc(` `demo_cur=` `>refcursor` `) ;` `EXEC SQL char open_file` `name_rcInd[100];` `# As the below function` `returns cursor_name` `as` `# return we need to` `use char[] type as` `indicator.`	Desarrollador de aplicaciones, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	`EXEC SQL SELECT pkg_demo.get_cursor ( demo_cur= >'demo_cursor' ) INTO :open_filename_rcInd;`	

Tarea	Descripción	Habilidades requeridas
Aplique patrones de migración comunes.	• Cambie las consultas SQL para que sean compatibles con PostgreSQL. • Mueva los bloques anónimos a la base de datos cuando no estén admitidos en ECPG. • Elimine la lógica `dbms_application_info` , que no admite PostgreSQL. • Mueva las instrucciones `EXEC SQL COMMIT` después de cerrar el cursor. Si realiza consultas mientras está en el bucle para recuperar los registros del cursor, el cursor se cierra y se muestra un error que indica que el cursor no existe. • Para obtener información sobre la gestión de excepciones en ECPG y códigos de error, consulte Gestión de errores en la documentación de PostgreSQL.	Desarrollador de aplicaciones, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Habilite la depuración, si fuera necesario.	Para ejecutar el programa ECPG en modo de depuración, añada el siguiente comando dentro del bloque de funciones principal. `ECPGdebug(1, stderr);`	Desarrollador de aplicaciones, propietario de la aplicación

Compilar programas ECPG

Tarea	Descripción	Habilidades requeridas
Cree un archivo ejecutable para ECPG.	Si tiene un archivo fuente de SQL C incrustado denominado `prog1.pgc` , puede crear un programa ejecutable mediante el siguiente Script. `ecpg prog1.pgc` `cc -I/usr/local/pgsql/include -c prog1.c` `cc -o prog1 prog1.o -L/usr/local/pgsql/lib -lecpg`	Desarrollador de aplicaciones, propietario de la aplicación
Cree un archivo de creación para su compilación.	Cree un archivo make para compilar el programa ECPG, tal como se muestra en el siguiente archivo de ejemplo. `CFLAGS ::= $(CFLAGS) -I/usr/pgsql-12/include -g -Wall` `LDFLAGS ::= $(LDFLAGS) -L/usr/pgsql-12/li`	Desarrollador de aplicaciones, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	`b -Wl,-rpath,/usr/pgsql-12/lib` `LDLIBS ::= $(LDLIBS) -lecpg` `PROGRAMS = test` `.PHONY: all clean` `%.c: %.pgc` `ecpg $<` `all: $(PROGRAMS)` `clean:` `rm -f $(PROGRAMS) $(PROGRAMS:%=%.c) $(PROGRAMS:%=%.o)`	

Pruebe la aplicación

Tarea	Descripción	Habilidades requeridas
Pruebe el código.	Pruebe el código de la aplicación que se convertirá para asegurarse de que funciona correctamente.	Desarrollador de aplicaciones, propietario de la aplicación, ingeniero de pruebas

Recursos relacionados

- ECPG: SQL integrado en C (documentación de PostgreSQL)
- Gestión de errores (documentación de PostgreSQL)
- Por qué utilizar el precompilador Pro*C/C++ de Oracle (documentación de Oracle)

Información adicional

PostgreSQL tiene un precompilador SQL integrado, ECPG, que es equivalente al precompilador Pro*C de Oracle. El ECPG convierte los programas en C que tienen instrucciones SQL incorporadas en código C estándar sustituyendo las llamadas SQL por llamadas a funciones especiales. Luego,

los archivos de salida se pueden procesar con cualquier cadena de herramientas del compilador de C.

Archivos de entrada y salida

ECPG convierte cada archivo de entrada que especifique en la línea de comandos en el archivo de salida C correspondiente. Si el nombre de un archivo de entrada no tiene una extensión de archivo, se asume la extensión .pgc. La extensión del archivo se sustituye por `.c` para construir el nombre del archivo de salida. Sin embargo, puede anular el nombre del archivo de salida predeterminado utilizando la opción `-o`.

Si utiliza un guión (`-`) como nombre del archivo de entrada, ECPG lee el programa desde la entrada estándar y escribe en la salida estándar, a menos que lo anule mediante la opción `-o`.

Archivos de encabezado

Cuando el compilador de PostgreSQL compila los archivos de código C preprocesados, busca los archivos de cabecera ECPG en el directorio de PostgreSQL `include`. Por lo tanto, puede que tenga que usar la opción `-I` para dirigir el compilador al directorio correcto (por ejemplo, `-I/usr/local/pgsql/include`).

Bibliotecas

Los programas que utilizan código C con SQL incorporado tienen que estar enlazados a la biblioteca `libecpg`. Por ejemplo, puede utilizar las opciones `-L/usr/local/pgsql/lib -lecpg` del enlazador.

Las aplicaciones ECPG convertidas llaman a las funciones de la biblioteca `libpq` a través de la biblioteca SQL integrada (`ecpglib`) y se comunican con el servidor PostgreSQL mediante el protocolo frontend/backend estándar.

Migre columnas generadas de forma virtual de Oracle a PostgreSQL

Creado por Veeranjaneyulu Grandhi (AWS), Rajesh Madiwale (AWS) y Ramesh Pathuri (AWS)

Entorno: producción	Origen: base de datos de Oracle	Destino: Amazon RDS para PostgreSQL o Aurora compatible con PostgreSQL
Tipo R: renovar arquitectura	Carga de trabajo: Oracle	Tecnologías: migración; bases de datos
Servicios de AWS: Amazon Aurora; Amazon RDS; AWS DMS		

Resumen

En la versión 11 y anteriores, PostgreSQL no proporciona una característica que sea directamente equivalente a una columna virtual de Oracle. Gestionar las columnas generadas de forma virtual al migrar de Oracle Database a la versión 11 o anterior de PostgreSQL resulta difícil por dos motivos:

- Las columnas virtuales no están visibles durante la migración.
- PostgreSQL no admite la expresión `generate` antes de la versión 12.

Sin embargo, existen soluciones alternativas para emular una funcionalidad similar. Cuando utilice AWS Database Migration Service (AWS DMS) para migrar datos desde Oracle Database a la versión 11 y anteriores de PostgreSQL, puede utilizar las funciones de activación para rellenar los valores de las columnas generadas de forma virtual. Este patrón proporciona ejemplos de código PostgreSQL y Oracle Database que puede utilizar para este fin. En AWS, puede utilizar Amazon Relational Database Service (Amazon RDS) para PostgreSQL o la Edición compatible con PostgreSQL de Amazon Aurora para la base de datos de PostgreSQL.

A partir de la versión 12 de PostgreSQL, se admiten las columnas generadas. Las columnas generadas pueden calcularse sobre la marcha a partir de otros valores de columna o calcularse y almacenarse. Las columnas generadas por PostgreSQL son similares a las columnas virtuales de Oracle.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Base de datos de origen de Oracle
- Bases de datos PostgreSQL de destino (en Amazon RDS para PostgreSQL o Aurora compatible con PostgreSQL)
- Experiencia en codificación PL/pgSQL

Limitaciones

- Solo se aplica a las versiones de PostgreSQL anteriores a la versión 12.
- Se aplica a la versión 11g o posterior de Oracle Database.
- Las columnas virtuales no se admiten en las herramientas de migración de datos.
- Solo se aplica a las columnas definidas en la misma tabla.
- Si una columna generada de forma virtual hace referencia a una función determinista definida por el usuario, no se puede utilizar como columna clave de partición.
- El resultado de la expresión debe ser un valor escalar. No puede devolver un tipo de datos proporcionado por Oracle, un tipo definido por el usuario, `LOB` o `LONG RAW`.
- Los índices que se definen en columnas virtuales equivalen a los índices basados en funciones en PostgreSQL.
- Se deben recopilar las estadísticas de las tablas.

Herramientas

- pgAdmin 4 es una herramienta de gestión de código abierto para PostgreSQL. Esta herramienta proporciona una interfaz gráfica que simplifica la creación, el mantenimiento y el uso de los objetos de la base de datos.
- Oracle SQL Developer es un entorno de desarrollo integrado y gratuito para trabajar con SQL en bases de datos de Oracle, tanto en implementaciones tradicionales como en la nube.

Epics

Cree tablas de bases de datos de origen y destino

Tarea	Descripción	Habilidades requeridas
Cree una tabla de base de datos Oracle de origen.	En Oracle Database, cree una tabla con columnas generadas de forma virtual mediante la siguiente declaración. `CREATE TABLE test.generated_column ( CODE NUMBER, STATUS VARCHAR2(12) DEFAULT 'PreOpen', FLAG CHAR(1) GENERATED ALWAYS AS (CASE UPPER(STATUS) WHEN 'OPEN' THEN 'N' ELSE 'Y' END) VIRTUAL VISIBLE );` En esta tabla de origen, los datos de la columna `STATUS` se migran a través de AWS DMS a la base de datos de destino. Sin embargo, la columna `FLAG` se rellena mediante la funcionalidad `generate by`, por lo que AWS DMS no podrá verla durante la migración. Para implementar la funcionalidad de `generated by`, debe utilizar activadores y funciones de la base de datos de destino para rellenar los valores	Administrador de base de datos, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	de la columna FLAG, como se muestra en la siguiente epopeya.	
Cree una tabla PostgreSQL de destino en AWS.	Cree una tabla de PostgreSQL en AWS con la siguiente instrucción. `CREATE TABLE test.generated_column ( code integer not null, status character varying(12) not null , flag character(1) );` En esta tabla, la columna `status` es una columna estándar. La columna `flag` será una columna generada en función de los datos de la columna `status`.	Administrador de base de datos, desarrollador de aplicaciones

Cree una función de activación para gestionar la columna virtual en PostgreSQL

Tarea	Descripción	Habilidades requeridas
Cree un activador de PostgreSQL.	En PostgreSQL, cree un activador. `CREATE TRIGGER tgr_gen_column AFTER INSERT OR UPDATE OF status ON test.generated_column`	Administrador de base de datos, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`` FOR EACH ROW EXECUTE FUNCTION test.tgf_gen_colum n(); ```	

Tarea	Descripción	Habilidades requeridas
Cree una función de activación de PostgreSQL.	En PostgreSQL, cree una función para el activador. Esta función rellena una columna virtual que la aplicación o AWS DMS insertan o actualizan y valida los datos. `CREATE OR REPLACE FUNCTION test.tgf_gen_column() RETURNS trigger AS $VIRTUAL_COL$ BEGIN IF (TG_OP = 'INSERT') THEN IF (NEW.flag IS NOT NULL) THEN RAISE EXCEPTION 'ERROR: cannot insert into column "flag"' USING DETAIL = 'Column "flag" is a generated column.'; END IF; END IF; IF (TG_OP = 'UPDATE') THEN IF (NEW.flag::VARCHAR != OLD.flag::varchar) THEN RAISE EXCEPTION 'ERROR: cannot update column "flag"' USING DETAIL = 'Column "flag" is a generated column.'; END IF; END IF; IF TG_OP IN ('INSERT','UPDATE') THEN`	Administrador de base de datos, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`IF (old.flag is NULL) OR (coalesce(old.status,'') != coalesce(new.status,'')) THEN UPDATE test.generated_column SET flag = (CASE UPPER(status) WHEN 'OPEN' THEN 'N' ELSE 'Y' END) WHERE code = new.code; END IF; END IF; RETURN NEW; END $VIRTUAL_COL$ LANGUAGE plpgsql;`	

Pruebe la migración de datos mediante AWS DMS

Tarea	Descripción	Habilidades requeridas
Crear una instancia de replicación.	Para crear una instancia de replicación, siga las instrucciones de la documentación de AWS DMS. La instancia de replicación debe estar en la misma nube privada virtual (VPC) que las bases de datos de origen y destino.	Administrador de base de datos, desarrollador de aplicaciones
Crear los puntos de conexión de origen y de destino.	Para crear los puntos de conexión, siga las instrucciones de la documentación de AWS DMS.	Administrador de base de datos, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Probar los puntos de conexión.	Puede probar las conexiones de conexión especificando la VPC y la instancia de replicación y seleccionando Ejecutar prueba.	Administrador de base de datos, desarrollador de aplicaciones
Cree e inicie una tarea de carga completa.	Para obtener instrucciones, consulte Creación de una tarea y Configuración de tareas de carga completa en la documentación de AWS DMS.	Administrador de base de datos, desarrollador de aplicaciones
Valide los datos de la columna virtual.	Compare los datos de la columna virtual en las bases de datos de origen y destino. Puede validar los datos manualmente o escribir un script para este paso.	Administrador de base de datos, desarrollador de aplicaciones

Recursos relacionados

- Introducción a AWS Database Migration Service (AWS DMS) (documentación de AWS DMS)
- Uso de una base de datos de Oracle como fuente para AWS DMS (documentación de AWS DMS)
- Uso de una base de datos PostgreSQL como destino para AWS DMS (documentación de AWS DMS)
- Columnas generadas en PostgreSQL (documentación de PostgreSQL)
- Funciones de activación (documentación de PostgreSQL)
- Columnas virtuales en Oracle Database (documentación de Oracle)

Configure la funcionalidad UTL_FILE de Oracle en Aurora compatible con PostgreSQL

Creado por Rakesh Raghav (AWS) y anuradha chintha (AWS)

Entorno: PoC o piloto	Origen: Oracle	Destino: Aurora PostgreSQL
Tipo R: renovar arquitectura	Carga de trabajo: Oracle	Tecnologías: migración; infraestructura; bases de datos
Servicios de AWS: Amazon S3; Amazon Aurora		

Resumen

Como parte de su migración de Oracle a una edición compatible con PostgreSQL de Amazon Aurora en la nube de Amazon Web Services (AWS), es posible que se enfrente a varios desafíos. Por ejemplo, migrar el código que se basa en la utilidad de Oracle `UTL_FILE` siempre es un desafío. En Oracle PL/SQL, el paquete `UTL_FILE` se utiliza para operaciones de archivos, como lectura y escritura, junto con el sistema operativo subyacente. La utilidad `UTL_FILE` funciona tanto para los sistemas de servidor como para los de máquinas cliente.

Amazon Aurora PostgreSQL es una oferta de bases de datos administradas. Por este motivo, no es posible acceder a los archivos del servidor de la base de datos. Este patrón le guía a través de la integración de Amazon Simple Storage Service (Amazon S3) y Amazon Aurora PostgreSQL para lograr un subconjunto de funciones de `UTL_FILE`. Con esta integración, podemos crear y consumir archivos sin utilizar herramientas o servicios de extracción, transformación y carga (ETL) de terceros.

Si lo desea, puede configurar la CloudWatch supervisión de Amazon y las notificaciones de Amazon SNS.

Recomendamos probar exhaustivamente esta solución antes de implementarla en un entorno de producción.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Experiencia en AWS Database Migration Service (AWS DMS)
- Experiencia en codificación PL/pgSQL
- Clúster de Amazon Aurora compatible con PostgreSQL
- Un bucket de S3

Limitaciones

Este patrón no proporciona la funcionalidad necesaria para reemplazar la utilidad de Oracle `UTL_FILE`. Sin embargo, los pasos y el código de muestra se pueden mejorar aún más para lograr sus objetivos de modernización de la base de datos.

Versiones de producto

- Edición 11.9 de Amazon Aurora compatible con PostgreSQL

Arquitectura

Pila de tecnología de destino

- Amazon Aurora compatible con PostgreSQL
- Amazon CloudWatch
- Amazon Simple Notification Service (Amazon SNS)
- Amazon S3

Arquitectura de destino

En el siguiente diagrama se muestra una representación de alto nivel de la solución.

1. Los archivos se cargan de la aplicación en el bucket S3.
2. La extensión `aws_s3` accede a los datos mediante PL/pgSQL y los carga en una aplicación compatible con Aurora PostgreSQL.

Herramientas

- Compatible con Amazon Aurora PostgreSQL: Amazon Aurora PostgreSQL Edition es un motor de bases de datos relacionales, completamente administrado, compatible con PostgreSQL y conforme a ACID. Combina la velocidad y la fiabilidad de las bases de datos comerciales de gama alta con la rentabilidad de las bases de datos de código abierto.
- AWS CLI: la interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta unificada para administrar los servicios de AWS. Con una única herramienta para descargar y configurar, podrá controlar varios servicios de AWS desde la línea de comando y automatizarlos mediante scripts.
- Amazon CloudWatch: Amazon CloudWatch supervisa los recursos y el uso de Amazon S3.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet. En este patrón, Amazon S3 proporciona una capa de almacenamiento para recibir y almacenar archivos para su consumo y transmisión hacia y desde el clúster compatible con Aurora PostgreSQL.
- aws_s3: la extensión `aws_s3` integra Amazon S3 y Aurora compatible con PostgreSQL.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) coordina y administra la entrega o el envío de mensajes entre publicadores y clientes. En este patrón, Amazon SNS se usa para enviar notificaciones.
- pgAdmin: pgAdmin es una herramienta de administración de código abierto para Postgres. pgAdmin 4 proporciona una interfaz gráfica para crear, mantener y utilizar objetos de bases de datos.

Código

Para lograr la funcionalidad requerida, el patrón crea varias funciones con nombres similares a `UTL_FILE`. La sección de información adicional contiene el código base de estas funciones.

En el código, sustituya `testaurorabucket` por el nombre del bucket S3 de prueba. Sustituya `us-east-1` por la región de AWS de donde está ubicado su bucket S3 de prueba.

Epics

Integre Amazon S3 y Aurora PostgreSQL

Tarea	Descripción	Habilidades requeridas
Configurar políticas de IAM.	Cree una política de AWS Identity and Access Management (políticas de IAM) que conceda acceso a un bucket de S3 y sus objetos. Para ver el código, consulte la sección de información adicional.	Administrador de AWS, Administrador de base de datos
Añada funciones de acceso de Amazon S3 a Aurora PostgreSQL.	Cree dos roles de IAM: un rol para el acceso de lectura y otro para el acceso de escritura a Amazon S3. Adjunte los dos roles al clúster compatible con Aurora PostgreSQL: • Un rol para la característica S3Export • Un rol para la característica S3Import Para obtener más informaci ón, consulte la documenta ción compatible con Aurora PostgreSQL sobre la importaci ón y la exportación de datos a Amazon S3.	Administrador de AWS, Administrador de base de datos

Configurar las extensiones en Aurora PostgreSQL

Tarea	Descripción	Habilidades requeridas
Cree la extensión aws_commons.	La extensión `aws_commons` es una dependencia de la extensión `aws_s3`.	Administrador de base de datos, desarrollador
Cree la extensión aws_s3.	La extensión `aws_s3` interactúa con Amazon S3.	Administrador de base de datos, desarrollador

Valide la integración compatible con Amazon S3 y Aurora PostgreSQL

Tarea	Descripción	Habilidades requeridas
Prueba de importación de archivos de Amazon S3 en Aurora PostgreSQL.	Para probar la importación de archivos a un entorno compatible con Aurora PostgreSQL, cree un archivo CSV de muestra y cárguelo en el bucket S3. Cree una definición de tabla basada en el archivo CSV y cargue el archivo en la tabla mediante la función `aws_s3.table_import_from_s3` .	Administrador de base de datos, desarrollador
Pruebe a exportar archivos de Aurora PostgreSQL a Amazon S3.	Para probar la exportación de archivos compatibles con Aurora PostgreSQL, cree una tabla de prueba, llénela con datos y, a continuación, exporte los datos mediante la función `aws_s3.query_export_to_s3` .	Administrador de base de datos, desarrollador

Para imitar la utilidad UTL_FILE, cree funciones envolventes

Tarea	Descripción	Habilidades requeridas
Cree el esquema utl_file_utility.	El esquema mantiene unidas las funciones envolventes. Ejecute el siguiente comando para crear el esquema. `CREATE SCHEMA utl_file_utility;`	Administrador de base de datos, desarrollador
Cree el tipo file_type.	Para crear el tipo `file_type` , utilice el siguiente código. `CREATE TYPE utl_file_utility.file_type AS ( p_path character varying(30), p_file_name character varying );`	Administrador de base de datos/desarrollador
Cree la función init.	La función `init` inicializa una variable común como `bucket` o `region`. Para ver el código, consulte la sección de información adicional.	Administrador de base de datos/desarrollador
Cree las funciones.	Cree las funciones envolvent es `fopen`, `put_line`, y `fclose`. Para ver el código, consulte la sección de información adicional.	Administrador de base de datos, desarrollador

Pruebe las funciones de la capa

Tarea	Descripción	Habilidades requeridas
Pruebe las funciones del contenedor en modo escritura.	Para probar las funciones del contenedor en modo de escritura, utilice el código que se proporciona en la sección Información adicional.	Administrador de base de datos, desarrollador
Pruebe las funciones del contenedor en el modo de adición.	Para probar las funciones del contenedor en el modo de adición, utilice el código proporcionado en la sección Información adicional.	Administrador de base de datos, desarrollador

Recursos relacionados

- Integración de Amazon S3
- Amazon S3
- Aurora
- Amazon CloudWatch
- Amazon SNS

Información adicional

Configurar políticas de IAM

Cree las políticas siguientes.

Nombre de la política	JSON
S3 IntRead	`{ "Version": "2012-10-17", "Statement": [ {`

```
            "Sid": "S3integrationtest
",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
         "arn:aws:s3:::testaurorabuc
ket/*",
         "arn:aws:s3:::testaurorabuc
ket"
            ]
        }
    ]
}
```

S3 IntWrite

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3integrationtest
",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",

                "s3:ListBucket"
            ],
            "Resource": [
    "arn:aws:s3:::testaurorabucket/
*",               "arn:aws:s3:::test
aurorabucket"
            ]
        }
    ]
}
```

Creación de la función init

Para inicializar variables comunes, como `bucket` o `region`, cree la función `init` mediante el siguiente código.

```
CREATE OR REPLACE FUNCTION utl_file_utility.init(
    )
    RETURNS void
    LANGUAGE 'plpgsql'

    COST 100
    VOLATILE
AS $BODY$
BEGIN
      perform set_config
      ( format( '%s.%s','UTL_FILE_UTILITY', 'region' )
      , 'us-east-1'::text
      , false );

      perform set_config
      ( format( '%s.%s','UTL_FILE_UTILITY', 's3bucket' )
      , 'testaurorabucket'::text
      , false );
END;
$BODY$;
```

Cree las funciones envolventes

Cree las funciones envolventes `fopen`, `put_line` y `fclose`.

fopen

```
CREATE OR REPLACE FUNCTION utl_file_utility.fopen(
    p_file_name character varying,
    p_path character varying,
    p_mode character DEFAULT 'W'::bpchar,
    OUT p_file_type utl_file_utility.file_type)
    RETURNS utl_file_utility.file_type
    LANGUAGE 'plpgsql'

    COST 100
    VOLATILE
AS $BODY$
declare
    v_sql character varying;
```

```
    v_cnt_stat integer;
    v_cnt integer;
    v_tabname character varying;
    v_filewithpath character varying;
    v_region character varying;
    v_bucket character varying;

BEGIN
    /*initialize common variable */
    PERFORM utl_file_utility.init();
    v_region := current_setting( format( '%s.%s', 'UTL_FILE_UTILITY', 'region' ) );
    v_bucket :=  current_setting( format( '%s.%s', 'UTL_FILE_UTILITY', 's3bucket' ) );

    /* set tabname*/
    v_tabname := substring(p_file_name,1,case when strpos(p_file_name,'.') = 0 then
 length(p_file_name) else strpos(p_file_name,'.') - 1 end );
    v_filewithpath := case when NULLif(p_path,'') is null then p_file_name else
 concat_ws('/',p_path,p_file_name) end ;
    raise notice 'v_bucket %, v_filewithpath % , v_region %', v_bucket,v_filewithpath,
 v_region;

    /* APPEND MODE HANDLING; RETURN EXISTING FILE DETAILS IF PRESENT ELSE CREATE AN
 EMPTY FILE */
    IF p_mode = 'A' THEN
        v_sql := concat_ws('','create temp table if not exists ', v_tabname,' (col1
 text)');
        execute v_sql;

        begin
        PERFORM aws_s3.table_import_from_s3
            ( v_tabname,
            '',
            'DELIMITER AS ''#''',
            aws_commons.create_s3_uri
            (     v_bucket,
                v_filewithpath ,
                v_region)
            );
        exception
            when others then
             raise notice 'File load issue ,%',sqlerrm;
             raise;
        end;
        execute concat_ws('','select count(*) from ',v_tabname) into v_cnt;
```

```
        IF v_cnt > 0
        then
            p_file_type.p_path := p_path;
            p_file_type.p_file_name := p_file_name;
        else
            PERFORM aws_s3.query_export_to_s3('select ''''',
                           aws_commons.create_s3_uri(v_bucket, v_filewithpath,
 v_region)
                             );

            p_file_type.p_path := p_path;
            p_file_type.p_file_name := p_file_name;
        end if;
        v_sql := concat_ws('','drop table ', v_tabname);
        execute v_sql;
    ELSEIF p_mode = 'W' THEN
            PERFORM aws_s3.query_export_to_s3('select ''''',
                           aws_commons.create_s3_uri(v_bucket, v_filewithpath,
 v_region)
                             );
            p_file_type.p_path := p_path;
            p_file_type.p_file_name := p_file_name;
    END IF;

EXCEPTION
        when others then
            p_file_type.p_path := p_path;
            p_file_type.p_file_name := p_file_name;
            raise notice 'fopenerror,%',sqlerrm;
            raise;
END;
$BODY$;
```

put_line

```
CREATE OR REPLACE FUNCTION utl_file_utility.put_line(
    p_file_name character varying,
    p_path character varying,
    p_line text,
    p_flag character DEFAULT 'W'::bpchar)
    RETURNS boolean
    LANGUAGE 'plpgsql'
```

```
    COST 100
    VOLATILE
AS $BODY$
/*****************************************************************************
* Write line, p_line in windows format to file, p_fp - with carriage return
* added before new line.
*****************************************************************************/
declare
    v_sql varchar;
    v_ins_sql varchar;
    v_cnt INTEGER;
    v_filewithpath character varying;
    v_tabname  character varying;
    v_bucket character varying;
    v_region character varying;

BEGIN
 PERFORM utl_file_utility.init();

/* check if temp table already exist */

 v_tabname := substring(p_file_name,1,case when strpos(p_file_name,'.') = 0 then
 length(p_file_name) else strpos(p_file_name,'.') - 1 end );

 v_sql := concat_ws('','select count(1) FROM pg_catalog.pg_class c LEFT JOIN
 pg_catalog.pg_namespace n ON n.oid = c.relnamespace where n.nspname like ''pg_temp_
%'''
                         ,' AND pg_catalog.pg_table_is_visible(c.oid) AND
 Upper(relname) = Upper( '''
                         ,  v_tabname ,''' ) ');

 execute v_sql into v_cnt;

  IF v_cnt = 0 THEN
        v_sql := concat_ws('','create temp table ',v_tabname,' (col text)');
       execute v_sql;
       /* CHECK IF APPEND MODE */
       IF upper(p_flag) = 'A' THEN
           PERFORM utl_file_utility.init();
           v_region := current_setting( format( '%s.%s', 'UTL_FILE_UTILITY',
 'region' ) );
           v_bucket :=  current_setting( format( '%s.%s', 'UTL_FILE_UTILITY',
 's3bucket' ) );
```

```
            /* set tabname*/
            v_filewithpath := case when NULLif(p_path,'') is null then p_file_name else
 concat_ws('/',p_path,p_file_name) end ;

            begin
               PERFORM aws_s3.table_import_from_s3
                     ( v_tabname,
                          '',
                       'DELIMITER AS ''#''',
                        aws_commons.create_s3_uri
                           ( v_bucket,
                               v_filewithpath,
                               v_region    )
                     );
            exception
                when others then
                    raise notice  'Error Message : %',sqlerrm;
                    raise;
            end;
        END IF;
    END IF;
    /* INSERT INTO TEMP TABLE */
    v_ins_sql := concat_ws('','insert into ',v_tabname,' values(''',p_line,''')');
    execute v_ins_sql;
    RETURN TRUE;
    exception
            when others then
                raise notice  'Error Message : %',sqlerrm;
                raise;
END;
$BODY$;
```

fclose

```
CREATE OR REPLACE FUNCTION utl_file_utility.fclose(
    p_file_name character varying,
    p_path character varying)
    RETURNS boolean
    LANGUAGE 'plpgsql'

    COST 100
    VOLATILE
```

```
AS $BODY$
DECLARE
    v_filewithpath character varying;
    v_bucket character varying;
    v_region character varying;
    v_tabname character varying;
    v_sql character varying;
BEGIN
      PERFORM utl_file_utility.init();

    v_region := current_setting( format( '%s.%s', 'UTL_FILE_UTILITY', 'region' ) );
    v_bucket :=  current_setting( format( '%s.%s', 'UTL_FILE_UTILITY', 's3bucket' ) );

    v_tabname := substring(p_file_name,1,case when strpos(p_file_name,'.') = 0 then
 length(p_file_name) else strpos(p_file_name,'.') - 1 end );
    v_filewithpath := case when NULLif(p_path,'') is null then p_file_name else
 concat_ws('/',p_path,p_file_name) end ;

    raise notice 'v_bucket %, v_filewithpath % , v_region %', v_bucket,v_filewithpath,
 v_region ;

    /* exporting to s3 */
    perform aws_s3.query_export_to_s3
        (concat_ws('','select * from ',v_tabname,'  order by ctid asc'),
            aws_commons.create_s3_uri(v_bucket, v_filewithpath, v_region)
        );
    v_sql := concat_ws('','drop table ', v_tabname);
    execute v_sql;
    RETURN TRUE;
EXCEPTION
       when others then
     raise notice 'error fclose %',sqlerrm;
     RAISE;
END;
$BODY$;
```

Pruebe sus funciones de configuración y envoltura

Utilice los siguientes bloques de código anónimos para comprobar su configuración.

Pruebe el modo de escritura

El siguiente código escribe un archivo llamado `s3inttest` en el bucket S3.

```
do $$
declare
l_file_name varchar := 's3inttest' ;
l_path varchar := 'integration_test' ;
l_mode char(1) := 'W';
l_fs utl_file_utility.file_type ;
l_status boolean;

begin
select * from
utl_file_utility.fopen( l_file_name, l_path , l_mode ) into l_fs ;
raise notice 'fopen : l_fs : %', l_fs;

select * from
utl_file_utility.put_line( l_file_name, l_path ,'this is test file:in s3bucket: for
 test purpose', l_mode ) into l_status ;
raise notice 'put_line : l_status %', l_status;

select * from utl_file_utility.fclose( l_file_name , l_path ) into l_status ;
raise notice 'fclose : l_status %', l_status;

end;
$$
```

Pruebe el modo de adición

El siguiente código añade líneas al archivo `s3inttest` que se creó en la prueba anterior.

```
do $$
declare
l_file_name varchar := 's3inttest' ;
l_path varchar := 'integration_test' ;
l_mode char(1) := 'A';
l_fs utl_file_utility.file_type ;
l_status boolean;

begin
select * from
utl_file_utility.fopen( l_file_name, l_path , l_mode ) into l_fs ;
raise notice 'fopen : l_fs : %', l_fs;


select * from
```

```
utl_file_utility.put_line( l_file_name, l_path ,'this is test file:in s3bucket: for
 test purpose : append 1', l_mode ) into l_status ;
raise notice 'put_line : l_status %', l_status;

select * from
utl_file_utility.put_line( l_file_name, l_path ,'this is test file:in s3bucket : for
 test purpose : append 2', l_mode ) into l_status ;
raise notice 'put_line : l_status %', l_status;

select * from utl_file_utility.fclose( l_file_name , l_path ) into l_status ;
raise notice 'fclose : l_status %', l_status;

end;
$$
```

Notificaciones de Amazon SNS

Si lo desea, puede configurar la CloudWatch supervisión de Amazon y las notificaciones de Amazon SNS en el bucket de S3. Para obtener más información, consulte Supervisión de Amazon S3 y Configuración de las notificaciones de Amazon SNS.

Validar los objetos de la base de datos después de migrar de Oracle a Amazon Aurora PostgreSQL

Creado por Venkatramana Chintha (AWS) y Eduardo Valentim (AWS)

Tipo R: renovar arquitectura	Origen: relacional	Destino: Amazon Aurora PostgreSQL, Amazon RDS para PostgreSQL
Creado por: AWS	Entorno: PoC o piloto	Tecnologías: bases de datos; migración
Carga de trabajo: Oracle	Servicios de AWS: Amazon Aurora	

Resumen

Este patrón describe un step-by-step enfoque para validar objetos después de migrar una base de datos de Oracle a una edición compatible con PostgreSQL de Amazon Aurora.

Este patrón describe los escenarios de uso y los pasos para la validación de objetos de bases de datos; para obtener información más detallada, consulte Validación de objetos de bases de datos después de la migración con AWS SCT y AWS DMS en el blog sobre bases de datos de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una base de datos Oracle local que se migró a una base de datos compatible con Aurora PostgreSQL.
- Credenciales de inicio de sesión a las que se ha aplicado la DataFullAccess política de AmazonRDS para la base de datos Aurora compatible con PostgreSQL.
- Este patrón utiliza el editor de consultas para los clústeres de bases de datos Aurora Serverless, que está disponible en la consola de Amazon Relational Database Service (Amazon RDS). Sin embargo, puede utilizar este patrón con cualquier otro editor de consultas.

Limitaciones

- Los objetos SYNONYM de Oracle no están disponibles en PostgreSQL, pero se pueden validar parcialmente mediante vistas o consultas SET search_path.
- El editor de consultas de Amazon RDS solo está disponible en determinadas regiones de AWS y para determinadas versiones de MySQL y PostgreSQL.

Arquitectura

Herramientas

Herramientas

- Edición compatible con Amazon Aurora PostgreSQL: Aurora PostgreSQL-Compatible es un motor de bases de datos relacionales, completamente administrado, compatible con PostgreSQL y conforme a ACID, que combina la velocidad y la fiabilidad de las bases de datos comerciales de tecnología avanzada con la sencillez y la rentabilidad de las bases de datos de código abierto.
- Amazon RDS: Amazon Relational Database Service (Amazon RDS) facilita la configuración, el funcionamiento y el escalado de una base de datos relacional en la nube de AWS. Proporciona una capacidad rentable y de tamaño ajustable para una base de datos relacional estándar y se ocupa de las tareas de administración de bases de datos comunes.
- Editor de consultas para Aurora Severless: el editor de consultas le ayuda a ejecutar consultas SQL en la consola de Amazon RDS. Puede ejecutar cualquier declaración SQL válida en el clúster de base de datos de Aurora Serverless, incluidas las declaraciones de manipulación y definición de datos.

Para validar los objetos, utilice los scripts completos del archivo «Script de validación de objetos» de la sección «Adjuntos». Utilice la siguiente tabla como referencia.

Objeto de Oracle	Script a utilizar
Paquetes	Consulta 1
Tablas	Consulta 3

Vistas	Consulta 5
Secuencias	Consulta 7
Desencadenadores	Consulta 9
Claves principales	Consulta 11
Índices	Consulta 13
Restricciones de comprobación	Consulta 15
Claves externas	Consulta 17

Objeto PostgreSQL	Script a utilizar
Paquetes	Consulta 2
Tablas	Consulta 4
Vistas	Consulta 6
Secuencias	Consulta 8
Desencadenadores	Consulta 10
Claves principales	Consulta 12
Índices	Consulta 14
Restricciones de comprobación	Consulta 16
Claves externas	Consulta 18

Epics

Valide los objetos de la base de datos Oracle de origen

Tarea	Descripción	Habilidades requeridas
Ejecute la consulta de validación de «paquetes» en la base de datos Oracle de origen.	Descargue y abra el archivo «Scripts de validación de objetos» de la sección «Adjuntos». Conéctese a la base de datos Oracle de origen a través de su programa cliente. Ejecute el script de validaciones «Consulta 1» desde el archivo «Scripts de validació n de objetos». Importante: Introduzca su nombre de usuario de Oracle en lugar de «your_schema» en las consultas. Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos
Ejecute la consulta de validación de las «tablas».	Ejecute el script «Consulta 3» desde el archivo «Scripts de validación de objetos». Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos
Ejecute la consulta de validación de «vistas».	Ejecute el script «Consulta 5» desde el archivo «Scripts de validación de objetos». Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos
Ejecute la validación del recuento de «secuencias».	Ejecute el script «Consulta 7» desde el archivo «Script	Desarrollador, administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	de validación de objetos». Asegúrese de registrar los resultados de la consulta.	
Ejecute la consulta de validación «activadores».	Ejecute el script «Consulta 9» desde el archivo «Scripts de validación de objetos». Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos
Ejecute la consulta de validación de las «claves principales».	Ejecute el script «Consulta 11» desde el archivo «Scripts de validación de objetos». Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos
Ejecute la consulta de validación de los «índices».	Ejecute el script de validación «Consulta 13» desde el archivo «Script de validación de objetos». Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos
Ejecute la consulta de validación «comprobar las restricciones».	Ejecute el script «Consulta 15» desde el archivo «Scripts de validación de objetos». Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos
Ejecute la consulta de validación de «claves externas».	Ejecute el script de validación «Consulta 17» desde el archivo «Script de validación de objetos». Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos

Validar objetos en la base de datos compatible con Aurora PostgreSQL de destino

Tarea	Descripción	Habilidades requeridas
Conectar a la base de datos Aurora compatibl e con PostgreSQL de destino mediante el editor de consultas.	Iniciar sesión en la Consola de administración de AWS y abrir la consola de Amazon RDS. En la esquina superior derecha, elija la región de AWS en la que creó la base de datos Aurora PostgreSQ L. En el panel de navegación, elija «Bases de datos» y elija la base de datos compatibl e con Aurora PostgreSQL de destino. En «Acciones », seleccione «Consulta ». Importante: si no se ha conectado a la base de datos antes, se abre la página «Conectarse a la base de datos». A continuación, debe introducir la información de la base de datos, como el nombre de usuario y la contraseña.	Desarrollador, administrador de base de datos
Ejecute la consulta de validación de los «paquetes».	Ejecute el script «Consulta 2» desde el archivo «Script de validación de objetos» de la sección «Adjuntos». Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos
Ejecute la consulta de validación de las «tablas».	Vuelva al editor de consultas de la base de datos compatibl e con Aurora PostgreSQL y	Desarrollador, administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	ejecute el script «Consulta 4» desde el archivo «Scripts de validación de objetos». Asegúrese de registrar los resultados de la consulta.	
Ejecute la consulta de validación de «vistas».	Vuelva al editor de consultas de la base de datos compatible con Aurora PostgreSQL y ejecute el script «Consulta 6» desde el archivo «Scripts de validación de objetos». Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos
Ejecute la validación del recuento de «secuencias».	Vuelva al editor de consultas de la base de datos compatible con Aurora PostgreSQL y ejecute el script «Consulta 8» desde el archivo «Scripts de validación de objetos». Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos
Ejecute la consulta de validación «activadores».	Vuelva al editor de consultas de la base de datos compatible con Aurora PostgreSQL y ejecute el script «Consulta 10» desde el archivo «Scripts de validación de objetos». Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Ejecute la consulta de validación de las «claves principales».	Vuelva al editor de consultas de la base de datos compatible con Aurora PostgreSQL y ejecute el script «Consulta 12» desde el archivo «Scripts de validación de objetos». Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos
Ejecute la consulta de validación de los «índices».	Vuelva al editor de consultas de la base de datos compatible con Aurora PostgreSQL y ejecute el script «Consulta 14» desde el archivo «Scripts de validación de objetos». Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos
Ejecute la consulta de validación «comprobar las restricciones».	Ejecute el script «Consulta 16» desde el archivo «Scripts de validación de objetos». Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos
Ejecute la consulta de validación de «claves externas».	Ejecute el script de validación «Consulta 18» desde el archivo «Script de validación de objetos». Asegúrese de registrar los resultados de la consulta.	Desarrollador, administrador de base de datos

Compare los registros de validación de las bases de datos de origen y destino

Tarea	Descripción	Habilidades requeridas
Compare y valide los resultados de ambas consultas.	Compare los resultados de las consultas de las bases de datos compatibles con Oracle y Aurora PostgreSQL para validar todos los objetos. Si todos coinciden, significa que todos los objetos se han validado correctamente.	Desarrollador, administrador de base de datos

Recursos relacionados

- Validación de objetos de bases de datos después de una migración mediante AWS SCT y AWS DMS
- Características de Amazon Aurora: edición compatible con PostgreSQL

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Volver a alojar

Temas

- Configure una infraestructura Multi-AZ para una FCI Always On de SQL Server mediante Amazon FSx
- Utilice las consultas de BMC Discovery para extraer datos de migración para planificar la migración

Acelere el descubrimiento y la migración de las cargas de trabajo de Microsoft a AWS

Creado por Ali Alzand

Entorno: producción	Fuente: carga de trabajo de Microsoft que se ejecuta en las instalaciones o en otros proveedores de servicios en la nube	Destino: Amazon EC2 Windows
Tipo R: volver a alojar	Carga de trabajo: Microsoft	Tecnologías: migración
Servicios de AWS: Amazon EC2		

Resumen

Este patrón le muestra cómo usar el PowerShell módulo Migration Validator Toolkit para detectar y migrar sus cargas de trabajo de Microsoft a AWS. El módulo funciona realizando múltiples comprobaciones y validaciones para tareas comunes asociadas a cualquier carga de trabajo de Microsoft. Por ejemplo, el módulo busca instancias que puedan tener varios discos conectados o instancias que usen muchas direcciones IP. Para ver una lista completa de las comprobaciones que puede realizar el módulo, consulta la sección Comprobaciones de la GitHub página del módulo.

El PowerShell módulo Migration Validator Toolkit puede ayudar a su organización a reducir el tiempo y el esfuerzo necesarios para descubrir qué aplicaciones y servicios se ejecutan en sus cargas de trabajo de Microsoft. El módulo también puede servirle de ayuda para identificar las configuraciones de sus cargas de trabajo para que pueda averiguar si sus configuraciones son compatibles con AWS. El módulo también proporciona recomendaciones sobre los próximos pasos y las acciones de mitigación, de modo que puede evitar cualquier error de configuración antes, durante o después de la migración.

Requisitos previos y limitaciones

Requisitos previos

- Cuenta de administrador local
- PowerShell 4.0

Limitaciones

- Funciona solo en Microsoft Windows Server 2012 R2 o posterior

Herramientas

Herramientas

- PowerShell 4.0

Repositorio de códigos

El PowerShell módulo Migration Validator Toolkit para este patrón está disponible en el GitHub migration-validator-toolkit-for repositorio -microsoft-workloads.

Epics

Ejecute el módulo Migration Validator Toolkit en un único destino PowerShell

Tarea	Descripción	Habilidades requeridas
Descargue, extraiga, importe e invoque el módulo.	Elija uno de los siguientes métodos para descargar e implementar el módulo: • Ejecute el PowerShell script • Descargue y extraiga el archivo.zip • Clona el repositorio GitHub Ejecute el PowerShell script En PowerShell, ejecute el siguiente código de ejemplo:	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	`#MigrationValidatorToolkit` `$uri = 'https://github.com/aws-samples/migration-validator-toolkit-for-microsoft-workloads/archive/refs/heads/main.zip'` `$destination = (Get-Location).Path` `if ((Test-Path -Path "$destination\MigrationValidatorToolkit.zip" -PathType Leaf) -or (Test-Path -Path "$destination\MigrationValidatorToolkit")) {` `write-host "File $destination\MigrationValidatorToolkit.zip or folder $destination\MigrationValidatorToolkit found, exiting"` `}else {` `Write-host "Enable TLS 1.2 for this PowerShell session only."` `[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12` `$webClient = New-Object System.Net.WebClient`	

Tarea	Descripción	Habilidades requeridas
	<pre> Write-host "Downloading Migration ValidatorToolkit.zip" $webClient.Downloa dFile($uri, "$destina tion\MigrationVali datorToolkit.zip") Write-host "MigrationValidato rToolkit.zip download successfully" Add-Type -Assembly "system.io.compres sion.filesystem" [System.IO.Compres sion.ZipFile]::Ext ractToDirectory("$ destination\Migrat ionValidatorToolki t.zip","$destinati on\MigrationValida torToolkit") Write-host "Extracting Migration ValidatorToolkit.zip complete successfully" Import-Module "$destination\Migr ationValidatorToolkit \migration-validator- toolkit-for-microsoft -workloads-main\Mi grationValidatorTo olkit.psm1"; Invoke- MigrationValidatorTo olkit }</pre> El código descarga el módulo de un archivo.zip. A continuac	

Tarea	Descripción	Habilidades requeridas
	ión, el código extrae, importa e invoca el módulo. Descargue y extraiga el archivo.zip 1. Descargue el archivo.zip (descarga). 2. Descomprima el archivo .zip. 3. Siga los pasos de la historia sobre cómo invocar el módulo manualmente de esta guía. Clona el repositorio GitHub 1. Para clonar el repositorio GitHub migration-validator-toolkit-for-microsoft-workloads, ejecuta el siguiente comando Git en una ventana de terminal: `git clone https://github.com/aws-samples/migration-validator-toolkit-for-microsoft-workloads.git` 2. Sigue los pasos de la historia sobre cómo invocar el módulo manualmente de esta guía.	

Tarea	Descripción	Habilidades requeridas
Invoque el módulo manualmente.	1. Vaya al directorio en el que está almacenado el módulo descargado. 2. Para generar el resultado que desee, ejecute uno de los siguientes comandos como administrador en PowerShell: Formato de tabla de formatos: `Import-Module .\MigrationValidatorToolkit.psm1;Invoke-MigrationValidatorToolkit` Formato de lista de formatos: `Import-Module .\MigrationValidatorToolkit.psm1;Invoke-MigrationValidatorToolkit -List` Formato de salida: GridView `Import-Module .\MigrationValidatorToolkit.psm1;Invoke-MigrationValidatorToolkit -GridView` ConvertTo-Formato CSV: `Import-Module .\MigrationValidatorToolkit`	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	`.psm1;Invoke-Migra tionValidatorToolkit -csv`	

Ejecute el módulo Migration Validator Toolkit PowerShell en varios objetivos

Tarea	Descripción	Habilidades requeridas
Descargue el archivo.zip o clone el repositorio. GitHub	Elija una de las opciones siguientes: • Descarga el archivo zip. (descargar). • Para clonar el repositorio GitHub migration-validator-toolkit-for-microsoft-workloads, ejecuta el siguiente comando Git en una ventana de terminal: `git clone https://github.com/aws-samples/migration-validator-toolkit-for-microsoft-workloads.git`	Administrador de sistemas
Actualiza la lista de archivos server.csv.	Si descargaste el archivo.zip, sigue estos pasos: 1. Descomprima el archivo .zip. 2. Vaya al directorio `MigrationValidator Toolkit\Inputs\` .	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	3. Actualice `serverlist.csv` con el nombre de host de los ordenadores de destino.	
Invoque el módulo.	Puede utilizar cualquier equipo del dominio que utilice un usuario del dominio que tenga acceso de administrador a los ordenadores de destino. 1. Descargue el código fuente como un archivo.zip y extraiga el archivo. 2. Como administrador PowerShell, ejecute el siguiente comando: `Import-Module .\MigrationValidatorToolkit.psm1;Invoke-DomainComputers` El archivo .csv de salida se guarda `Migration ValidatorToolkit \Outputs\folder` con el nombre del prefijo. `DomainComputers_MigrationAutomations_YYYY-MM-DDTHH-MM-SS`	Administrador de sistemas

Solución de problemas

Problema	Solución
`MigrationValidatorToolkit` escribe información sobre las ejecuciones, los comandos y los errores en los archivos de registro del host en ejecución.	Puede ver los archivos de registro manualmente en la siguiente ubicación: 1. Vaya al directorio `MigrationValidatorToolkit\logs\` . 2. Localice el archivo de registro. El formato del nombre del archivo de registro es: `ComputerName_MigrationValidatorToolkit_YYYY-MM-SSTHH-MM-SS.log`

Recursos relacionados

- Opciones, herramientas y prácticas recomendadas para migrar cargas de trabajo de Microsoft a AWS (AWS Prescriptive Guidance)
- Patrones de migración de Microsoft (AWS Prescriptive Guidance)
- Servicios gratuitos de migración a la nube en AWS (documentación de AWS)
- Acciones predefinidas posteriores al lanzamiento (documentación de marketing de la aplicación)

Información adicional

Preguntas frecuentes

¿Dónde puedo ejecutar el módulo Migration Validator Toolkit? PowerShell

Puede ejecutar el módulo en Microsoft Windows Server 2012 R2 o posterior.

¿Cuándo ejecuto este módulo?

Le recomendamos que ejecute el módulo durante la fase de evaluación del proceso de migración.

¿El módulo modifica mis servidores actuales?

No. Todas las acciones de este módulo son de solo lectura.

¿Cuánto tiempo se tarda en ejecutar el módulo?

La ejecución del módulo suele tardar entre 1 y 5 minutos, pero depende de la asignación de recursos del servidor.

¿Qué permisos necesita el módulo para ejecutarse?

Debe ejecutar el módulo desde una cuenta de administrador local.

¿Puedo ejecutar el módulo en servidores físicos?

Sí, siempre que el sistema operativo sea Microsoft Windows Server 2012 R2 o posterior.

¿Cómo puedo ejecutar el módulo a escala para varios servidores?

Para ejecutar el módulo a escala en varios ordenadores unidos a un dominio, siga los pasos del PowerShell módulo Ejecute the Migration Validator Toolkit en varios destinos, que se incluye en esta guía. En el caso de ordenadores que no estén unidos a un dominio, utilice una invocación remota o ejecute el módulo de forma local siguiendo los pasos del módulo Ejecute el kit de herramientas PowerShell de validación de migración en un solo destino, épica de esta guía.

Automatización de las actividades previas a la ingesta de cargas de trabajo para AWS Managed Services en Windows

Creado por Jacob Zhang (AWS), Calvin Yeh (AWS) y Dwayne Bordelon (AWS)

Repositorio de código: GitHub	Entorno: producción	Origen: servidores Windows
Destino: AWS Managed Services	Tipo R: volver a alojar	Tecnologías: migración
Servicios de AWS: AWS CloudFormation; AWS Managed Services; AWS Systems Manager; Amazon S3		

Resumen

En la nube de Amazon Web Services (AWS), AWS Managed Services (AMS) utiliza la ingesta de cargas de trabajo de AMS (WIGS) para trasladar las cargas de trabajo existentes a una VPC gestionada por AMS. Este patrón describe una solución para automatizar las actividades habituales previas a la ingesta de cargas de trabajo, como la actualización de.NET y Windows PowerShell y la ejecución de la validación previa a la ingestión del WIGS de Windows mantenida por AMS. El patrón también proporciona una interfaz de usuario unificada para los resultados de la ejecución. Incluye un documento de AWS Systems Manager Command, que realiza las actividades previas a la ingesta, en una plantilla de AWS CloudFormation . La plantilla se puede implementar repetidamente sin requerir acceso al propio Systems Manager ni entrar en conflicto con las automatizaciones de AMS.

Experiencia empresarial

Las migraciones a AMS requieren el aprovisionamiento de instancias nuevas de Amazon Elastic Compute Cloud (Amazon EC2) mediante Imágenes de máquina de Amazon (AMI) administradas por AMS y que incluyen componentes de AMS. Todas las cargas de trabajo o aplicaciones que se ejecuten en los centros de datos existentes se deben volver a implementar en instancias EC2 nuevas lanzadas desde estas AMI de AMS. Para evitar la enorme cantidad de trabajo manual que supone el proceso, el equipo de AMS creó el flujo de trabajo de ingesta de cargas de trabajo de AMS (WIGS) para incorporar sus imágenes personalizadas a AMS.

Las instancias de Windows deben cumplir algunos requisitos previos antes de que se lleve a cabo el proceso de WIGS. Los PowerShell scripts de Windows se suelen utilizar para realizar los preparativos necesarios (preparación para el WIGS) y comprobar si las instancias están preparadas para el WIGS (validación previa a la ingestión del WIGS). Los procesos de preparación y validación requieren que un ingeniero dedique de 15 a 30 minutos a cada servidor, inicie sesión manualmente y ejecute los scripts uno por uno.

Impulsor empresarial

Tradicionalmente, con Systems Manager, puede automatizar las tareas operativas, como la ejecución de PowerShell scripts de Windows. Sin embargo, debido a los riesgos elevados y a los frecuentes conflictos entre las automatizaciones de AMS y las de los usuarios, AMS no suele conceder a sus usuarios acceso a Systems Manager.

En el caso de las migraciones masivas mediante AWS Application Migration Service (AWS MGN), los PowerShell scripts de Windows `C:\Program Files (x86)\AWS Replication Agent \post_launch folder` suelen ejecutarse automáticamente cuando se lanza una instancia de prueba o transición. Sin embargo, estos scripts, si se ejecutan inmediatamente durante el lanzamiento de una instancia, suelen entrar en conflicto con las automatizaciones de AMS. Como resultado, es posible que se produzca un error en el lanzamiento sin proporcionar los resultados de ejecución necesarios para solucionar el error.

Este patrón resuelve estos problemas y proporciona una solución automatizada y funcional.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa con la incorporación de AMS completada.
- Cree un bucket de Amazon Simple Storage Service (Amazon S3) en la cuenta de AWS. Si no hay ningún bucket de S3 sobre el que tenga control en la cuenta, utilice una solicitud de cambio (RFC) para crear uno.
- La plantilla Prewigs_CFN.json descargada del repositorio. ams-auto-prewigs-windows
- El servidor al que aplique este patrón debe cumplir los siguientes requisitos:
  - Ejecutar Windows Server 2012 o posterior.
  - Se ha lanzado o está listo para lanzarse en la subred de migración de VPC de entorno aislado.
  - Tenga instalado un AWS Systems Manager Agent (SSM Agent).

- Tener adjunto un perfil de instancia de AWS Identity and Access Management (IAM). El perfil de instancia debe tener permisos para descargar archivos de buckets de S3 en la misma cuenta de AWS. Por lo general, un perfil de instancia que cumple el requisito mencionado anteriormente ya estaba establecido durante las configuraciones anteriores de una migración.
- Se puede ver desde Administrador de flotas de AWS Systems Manager.

Limitaciones

- Las actividades previas al WIGS varían en función del entorno y de los requisitos empresariales. Es posible que necesite realizar pequeñas modificaciones en este patrón para que se adapte mejor a sus necesidades específicas.

Versiones de producto

- El patrón se prueba con Windows Server 2012, 2012 R2, 2016 y 2019. En teoría, funciona con versiones posteriores de Windows. No funciona con versiones anteriores de Windows.

Arquitectura

En el siguiente diagrama se muestra la arquitectura:

1. Una VPC de entorno aislado con una subred de migración que contiene servidores que no se han preparado.
2. El depósito de S3 que almacena los scripts que utiliza la plantilla. CloudFormation
3. La CloudFormation plantilla despliega el documento de comandos de Systems Manager. El proceso se repite hasta que se completen los pasos.
4. Se preparan las instancias y se crean las RFC para el WIGS.
5. En la VPC gestionada por AMS, la subred gestionada por AMS contiene los servidores tras la ingesta de carga de trabajo.

Cómo funciona

- Este patrón se incluye en una CloudFormation plantilla de AWS que permite las implementaciones repetibles de infraestructura como código (IaC). Debe implementar esta plantilla solo una vez para cada cuenta de AWS que requiera esta automatización.
- La automatización se aplica a todas las instancias de EC2 con una clave de etiqueta AutoPreWiGS en la cuenta de AWS en la que se implementa este patrón. La primera vez que se inicia una instancia de Amazon EC2 para Windows con la clave de etiqueta AutoPreWiGS, la automatización realiza las siguientes tareas.
  1. Actualiza Windows PowerShell a la versión 5.1 y .NET a la versión 4.5.2. Es posible que la instancia se reinicie varias veces, en función de las versiones de Windows PowerShell y .NET existentes. Después de cada reinicio, las actualizaciones continúan hasta que se completen. En este paso se utiliza el código incrustado en la CloudFormation plantilla modificado a partir de un PowerShell script de Windows, así como una guía específica de Systems Manager sobre los reinicios del servidor.
  2. Descarga desde Amazon S3 y ejecuta un PowerShell script de Windows que ha personalizado para preparar la instancia de Windows de Amazon EC2 para WIGS. Para obtener más información, consulte la sección Epics.
  3. Instala el módulo PowerShell de validación previa a la ingesta WIGS de Windows desde AWS.
  4. Ejecuta la validación previa a la ingesta de Windows WIGS y hace que los resultados se puedan ver en Systems Manager State Manager.

Herramientas

- AWS CloudFormation: AWS CloudFormation es un servicio que le ayuda a modelar y configurar sus recursos de AWS. Puede utilizar una que describa todos los recursos de AWS que desee y sus dependencias, de modo que pueda lanzar y configurar esos recursos como una pila. Este patrón utiliza una CloudFormation plantilla para automatizar la implementación de los recursos de este patrón.
- AWS Managed Services (AMS): AWS Managed Services (AMS) es un servicio empresarial que ofrece administración continua de infraestructura de AWS. Los cambios realizados en la infraestructura de un entorno de AMS deben realizarse mediante una RFC.
- AWS Systems Manager: AWS Systems Manager (anteriormente conocido como SSM) es un servicio que puede utilizar para ver y controlar su infraestructura en AWS. Mediante la consola de Systems Manager, puede ver los datos operativos de varios servicios de AWS y automatizar las tareas operativas en sus recursos de AWS. Este patrón utiliza Systems Manager para ejecutar y ver los resultados de ejecución de las actividades previas al WIGS.

- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos que ofrece escalabilidad, disponibilidad de datos, seguridad y rendimiento líderes del sector. Este patrón utiliza Amazon S3 para almacenar la CloudFormation plantilla y un PowerShell script de Windows que se descarga.

Epics

Cree un PowerShell script de Windows personalizado para automatizar tareas adicionales

Tarea	Descripción	Habilidades requeridas
Realice los cambios necesarios en los servidores en función de las necesidades empresariales.	Si necesita que los cambios se apliquen automáticamente a sus servidores antes de incorporarlos, cree un PowerShell script de Windows denominado `ingestion-prep.ps1` . Importante: el script no debe contener instrucciones para reiniciar el servidor y no debe requerir privilegios de administrador.	PowerShell creación de scripts
Elimine el software que no sea compatible con AMS.	AMS requiere que determinados programas, como las aplicaciones antivirus y VMware Tools, se eliminen antes de que se ejecute el WIGS. Incluya la desinstalación en el script `ingestion-prep.ps1` . Para obtener más información sobre el software no compatible, consulte la documentación de AWS.	PowerShell creación de guiones

Cargue la CloudFormation plantilla y el PowerShell script de Windows opcional en Amazon S3

Tarea	Descripción	Habilidades requeridas
Cree una carpeta en S3.	En un bucket de S3 en la misma cuenta de AWS en la que implementa este patrón, cree una carpeta.	AWS general
Cargue los scripts.	Cargue la `PreWIGs_CFN.json` CloudFormation plantilla y el PowerShell script de `ingestion-prep.ps1` Windows, que creó en la epopeya anterior, a la carpeta Amazon S3.	AWS general

Implemente la CloudFormation pila

Tarea	Descripción	Habilidades requeridas
Seleccione el tipo de cambio.	Navegue hasta la consola AMS para crear un RFC. Utilice el tipo de cambio de plantilla Crear pila a partir de CloudFormation (CFN).	AMS general
Establezca los parámetros de ejecución para la ruta a la CloudFormation plantilla.	En la sección de Configuración de la ejecución, amplíe Configuración adicional. En el cuadro de punto final de S3 de la CloudFormation plantilla, pegue la URL en la CloudFormation plantilla.	AMS general
Especifique la ruta hacia la carpeta de Amazon S3.	En Parámetros, ScriptSourceutilícela como nombre. En	AMS general

Tarea	Descripción	Habilidades requeridas
	Value, introduzca la ruta a la carpeta S3 que contiene los PowerShell scripts de Windows. Asegúrese de utilizar la URL `https://xxx` en lugar de la URI `s3://xxx` e incluya `/` al final.	
Implemente la pila.	Para implementar la pila, seleccione Crear.	AMS general
Escale el RFC a AMS Ops.	El equipo de operaciones de AMS debe implementar la RFC manualmente, ya que utiliza Systems Manager para implementar los recursos y requiere una revisión de seguridad. Tan pronto como cree la RFC, el sistema la rechazará automáticamente. Elija la RFC y añada una correspondencia a la RFC que diga Ejecutar manualmente. Anote el ID de RFC y amplíelo con una solicitud de servicio.	AMS general

Aplique la automatización a las instancias

Tarea	Descripción	Habilidades requeridas
Agrega la etiqueta AutoPre WiGS a las instancias.	Anote los ID de todas las instancias a las que desee aplicar esta automatiz ación y espere al menos 30 minutos hasta que la instancia	AMS general

Tarea	Descripción	Habilidades requeridas
	finalice las automatizaciones implementadas por AMS. Envía un RFC automático para añadir la etiqueta con AutoPrelas WIG como clave y cualquier cadena, como 1, como valor. La automatización se aplicará unos minutos después de añadir la etiqueta.	
Verifique los resultados de la automatización.	Abra la consola de Systems Manager y seleccione State Manager. Elija el ID de asociación con el nombre AMS-Prewig-Prep-and-Validation-Association. En la pestaña Historial de ejecuciones, puede ver los resultados de la automatización.	AMS general
Corrija los posibles errores.	Si la automatización falla, elija su ID de ejecución. Puede ver los resultados de la ejecución de cada instancia de EC2. Para ver los detalles de cada paso de la automatización, elija Salida. Si se produce un error en un paso concreto, utilice la información de las secciones Resultado y Error para diagnosticar el problema.	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
Quita la etiqueta AutoPre WiGS.	Importante: Después de corregir los errores, si los hubiera, envía un RFC automático para eliminar la etiqueta de los AutoPreWiGS. El WIGS fallará si no elimina la etiqueta.	AMS general

Ingiera las instancias preparadas

Tarea	Descripción	Habilidades requeridas
Envíe las RFC para WIGS.	Ahora que las instancias están listas para la ingesta de la carga de trabajo, envíe las RFC para WIGS.	AMS general

Recursos relacionados

- Ingesta de carga de trabajo de AMS (WIGS)
- Migración de cargas de trabajo: validación previa a la ingestión de Windows
- Guía de inicio rápido para el Servicio de migración de aplicaciones de AWS
- Cómo empezar a usar AWS CloudFormation
- Configuración de AWS Systems Manager

Crear un proceso de aprobación para las solicitudes de firewall durante una migración para volver a alojar a AWS

Creado por Srikanth Rangavajhala (AWS)

Tipo R: volver a alojar	Entorno: producción	Tecnologías: Migración
Origen: En las instalaciones	Destino: Nube de AWS	

Resumen

Si desea utilizar AWS Application Migration Service o Cloud Migration Factory en AWS para una migración para volver a alojar a la nube de Amazon Web Services (AWS), uno de los requisitos previos es mantener abiertos los puertos TCP 443 y 1500. Por lo general, la apertura de estos puertos de firewall requiere la aprobación de su equipo de seguridad de la información (InfoSec).

Este patrón describe el proceso para obtener la aprobación de una solicitud de firewall por parte de un InfoSec equipo durante una migración de realojamiento a la nube de AWS. Puede utilizar este proceso para evitar que el InfoSec equipo rechace su solicitud de firewall, lo que puede resultar caro y llevar mucho tiempo. El proceso de solicitud del firewall consta de dos pasos de revisión y aprobación entre los asesores de migración de AWS y los líderes, quienes trabajan con sus equipos InfoSec y los de aplicaciones para abrir los puertos del firewall.

Este patrón supone que está planificando una migración para volver a alojar con consultores o especialistas en migración de AWS de su organización. Puede utilizar este patrón si su organización no cuenta con un proceso de aprobación de firewall o si no tiene un formulario de aprobación global para solicitar un firewall. Para obtener más información al respecto, consulte la sección Limitaciones de este patrón. Para obtener más información sobre los requisitos de red del Servicio de migración de aplicaciones, consulte los Requisitos de red en la documentación del Servicio de migración de aplicaciones.

Requisitos previos y limitaciones

Requisitos previos

- Una migración planificada para volver a alojar con consultores de AWS o especialistas en migración de su organización

- La información de puerto e IP necesaria para migrar la pila
- Diagramas de arquitectura de estados actuales y futuros
- Información del firewall sobre la infraestructura local y de destino, los puertos y el flujo de zone-to-zone tráfico
- Una lista de verificación para revisar las solicitudes de firewall (adjunta)
- Un documento de solicitud de firewall, configurado de acuerdo con los requisitos de su organización
- Una lista de contactos para los revisores y aprobadores de firewall, que incluya los siguientes roles:
  - Presentador de la solicitud de firewall – Especialista o consultor en migración de AWS. El remitente de la solicitud de firewall también puede ser un especialista en migración de su organización.
  - Revisor de solicitudes de firewall – Normalmente, se trata del punto de contacto único (SPOC) de AWS.
  - Aprobador de solicitudes de firewall: miembro InfoSec del equipo.

Limitaciones

- Este patrón describe un proceso genérico de aprobación de una solicitud de firewall. Los requisitos pueden variar de una organización a otra.
- Asegúrese de realizar un seguimiento de los cambios en el documento de solicitud de firewall.

En la tabla siguiente se muestran los casos de uso de este patrón.

¿Cuenta su organización con un proceso de aprobación de firewalls existente?	¿Cuenta su organización con un formulario de solicitud de firewall existente?	Acción sugerida
Sí	Sí	Colabore con los consultores de AWS o sus especialistas en migración para implementar el proceso de su organización.
No	Sí	Utilice el proceso de aprobación de firewall de este patrón.

		Utilice un consultor de AWS o un especialista en migración de su organización para enviar el formulario de aprobación general de la solicitud de firewall.
No	No	Utilice el proceso de aprobación de firewall de este patrón. Utilice un consultor de AWS o un especialista en migración de su organización para enviar el formulario de aprobación general de la solicitud de firewall.

Arquitectura

En el siguiente diagrama, se muestran los pasos del proceso de aprobación de solicitudes de firewall.

Herramientas

Puede utilizar herramientas de escaneo, como Palo Alto Networks, o SolarWindspara analizar y validar los firewalls y las direcciones IP.

Epics

Analizar la solicitud de firewall

Tarea	Descripción	Habilidades requeridas
Analice los puertos y las direcciones IP.	El remitente de la solicitud de firewall realiza un análisis inicial para comprender los puertos y las direcciones IP de firewall necesarios. Una	Ingeniero de nube de AWS, especialista en migración

Tarea	Descripción	Habilidades requeridas
	vez hecho esto, solicitan que tu InfoSec equipo abra los puertos necesarios y mapee las direcciones IP.	

Validar la solicitud de firewall

Tarea	Descripción	Habilidades requeridas
Valide la información de firewall.	El ingeniero de la nube de AWS programa una reunión con su InfoSec equipo. Durante esta reunión, el ingeniero examina y valida la información de la solicitud de firewall. Por lo general, el remitente de la solicitud de firewall es la misma persona que el solicitante de firewall. Esta fase de validación puede pasar a ser iterativa en función de los comentarios que dé el responsable de la aprobació n si se observa o recomienda algo.	Ingeniero de nube de AWS, especialista en migración
Actualice el documento de solicitud de firewall.	Una vez que el InfoSec equipo comparte sus comentarios, el documento de solicitud de firewall se edita, se guarda y se vuelve a cargar. Este documento se actualiza después de cada iteración.	Ingeniero de nube de AWS, especialista en migración

Tarea	Descripción	Habilidades requeridas
	Se recomienda almacenar este documento en una carpeta de almacenamiento con control de versiones. Esto significa que se realiza un seguimiento de todos los cambios y se aplican correctamente.	

Enviar la solicitud de firewall

Tarea	Descripción	Habilidades requeridas
Envíe la solicitud de firewall.	Una vez que el aprobador de la solicitud de firewall haya aprobado la solicitud de aprobación general de firewall, el ingeniero de la nube de AWS envía la solicitud de firewall. La solicitud especific a los puertos que deben estar abiertos y las direcciones IP que se requieren para asignar y actualizar la cuenta de AWS. Puede hacer sugerencias o enviar comentarios una vez enviada la solicitud de firewall. Le recomendamos que automatice este proceso de comentarios y envíe cualquier modificación mediante un mecanismo de flujo de trabajo definido.	Ingeniero de nube de AWS, especialista en migración

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Incorporar y migrar instancias de Windows de EC2 a una cuenta de AWS Managed Services

Documento creado por Anil Kunapareddy (AWS) y Venkatramana Chintha (AWS)

Entorno: producción	Origen: VPC en la nube de AWS	Destino: VPC administrada por AWS Managed Services
Tipo R: volver a alojar	Carga de trabajo: Microsoft	Tecnologías: migración ; operaciones; seguridad , identidad, cumplimiento; nativo en la nube
Servicios de AWS: AWS Managed Services		

Resumen

Este patrón explica el step-by-step proceso de migración e ingesta de instancias de Windows de Amazon Elastic Compute Cloud (Amazon EC2) Compute EC2) en una cuenta de Amazon Web Services (AWS) Managed Services (AMS). AMS puede ayudar a administrar la instancia de manera más eficiente y segura. AMS proporciona flexibilidad operativa, mejora la seguridad y el cumplimiento, y ayuda a optimizar la capacidad y reducir los costos.

Este patrón comienza con una instancia EC2 de Windows que se ha migrado a una subred provisional de la cuenta de AMS. Hay varios servicios y herramientas de migración disponibles para realizar esta tarea, como AWS Application Migration Service.

Para realizar un cambio en su entorno administrado por AMS, debe crear y enviar una solicitud de cambio (RFC) para una operación o acción concreta. Con una RFC de incorporación de carga de trabajo de AMS (WIGS), se incorpora la instancia en la cuenta de AMS y se crea una imagen de máquina de Amazon (AMI) personalizada. A continuación, se debe crear la instancia de EC2 administrada por AMS enviando otra RFC para crear una pila de EC2. Para obtener más información, consulte AMS Workload Ingest (Incorporación de carga de trabajo de AMS) en la documentación de AMS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa y administrada por AMS
- Una zona de aterrizaje existente
- Permisos para realizar cambios en la VPC administrada por AMS
- Una instancia de Amazon EC2 para Windows en una subred provisional de la cuenta AMS
- Cumplimiento de los requisitos previos generales para la migración de cargas de trabajo mediante AMS WIGS
- Cumplimiento de los requisitos previos de Windows para la migración de cargas de trabajo mediante AMS WIGS

Limitaciones

- Este patrón es para las instancias de EC2 que funcionan con Windows Server. Este patrón no se aplica a las instancias que ejecutan otros sistemas operativos, como Linux.

Arquitectura

Pila de tecnología de origen

Una instancia de Amazon EC2 para Windows en una subred provisional de la cuenta AMS

Pila de tecnología de destino

Una instancia de Amazon EC2 para Windows administrada por AWS Managed Services (AMS)

Arquitectura de destino

Herramientas

Servicios de AWS

- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de AWS. Puede utilizar Amazon EC2 para lanzar tantos servidores virtuales como necesite, y puede escalar horizontalmente o reducir horizontalmente.

- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Managed Services (AMS) ayuda a operar de manera más eficiente y segura al proporcionar una administración continua de la infraestructura de AWS, que incluye supervisión, administración de incidentes, orientación de seguridad, soporte de parches y respaldo para las cargas de trabajo de AWS.

Otros servicios

- PowerShelles un programa de administración de automatización y configuración de Microsoft que se ejecuta en Windows, Linux y macOS.

Epics

Configurar los ajustes de la instancia

Tarea	Descripción	Habilidades requeridas
Cambie la configuración del cliente DNS.	1. En la instancia de EC2, abra el símbolo del sistema como administrador, escriba `gpedit.msc` y, a continuación, pulse Intro. 2. En el editor de políticas de grupo local, vaya a Computer Configuration (Configuración del equipo), Administrative Templates (Plantillas administrativas), Network (Red) y DNS Client. 3. En Primary DNS suffix (Sufijo DNS principal), seleccione Not configured. 4. En Primary DNS suffix devolution (Devolución	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	del sufijo DNS principal), seleccione Not configured.	
Cambie la configuración de Windows Update (actualiz aciones de Windows).	1. En el editor de políticas de grupo local, vaya a Computer Configuration (Configuración del equipo), Administrative Templates (Plantillas administrativas), Windows Components (Componentes de Windos), Windows Update (Actualiz ación de Windows). 2. En Specify intranet Microsoft update service location (Especificar la ubicación del servicio de actualización de Microsoft en la intranet), seleccione Not configured. 3. En Configure Automatic Updates (Configurar actualizaciones automátic as), seleccione Not configured. 4. En Automatic Updates detection frequency (Frecuencia de detección de actualizaciones automática), seleccione Not configured. 5. Cierre el editor de políticas de grupo local.	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
Habilitar un firewall.	1. En la instancia de EC2, abra el símbolo del sistema como administrador, escriba `services.msc` y, a continuación, pulse Intro. 2. En los Servicios de Windows, habilite el Firewall. 3. Cierre los Servicios de Windows.	Ingeniero de migraciones

Preparar la instancia para AMS WIGS

Tarea	Descripción	Habilidades requeridas
Limpie y prepare la instancia.	1. Con un host bastión y credenciales locales, cree una conexión de Protocolo de escritorio remoto (RDP) a la instancia de EC2 de la subred de almacenamiento. 2. Elimine todo el software antiguo, el software antivirus y las soluciones de copia de seguridad que no sean necesarios en AMS.	Ingeniero de migraciones
Repare el archivo sppnp.dll.	1. Vaya a `C:\Windows\System32\sppnp.dll`. 2. Cambie el nombre de `sppnp.dll` a `sppnp_old.dll`.	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	3. Con PowerShell las credenciales de administrador, introduzca los siguientes comandos: `dism /online /cleanup-image /restorehealth` `sfc /scannnow` 4. Reinicie la instancia de Windows EC2.	

Tarea	Descripción	Habilidades requeridas
Ejecute el script de validación previa a WIG.	1. Descargue el archivo zip de validación previa a la incorporación de Windows WIGS (`windows-prewings-valication.zip`) de la sección Migrating workloads: Windows pre-ingestion validation (Migrar cargas de trabajo: validación previa a la incorporación de Windows), en la documentación de AMS. 2. Ejecute el script de validación previa a WIG de Windows y compruebe los resultados. 3. Si se produce un error en la validación, solucione el problema y vuelva a ejecutar el script de validación hasta que la validación se realice correctamente.	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
Cree la AMI a prueba de fallos.	Una vez superada la validación previa a WIG, cree una AMI previa a la incorporación de la siguiente manera: 1. Seleccione Deployment (Implementación), Advanced stack components (Componentes de pila avanzados), AMI y Create. 2. Durante la creación, añada una etiqueta `Key=Name, Value=APPLICATION-ID_IngestReady` . 3. Espere a que se cree la AMI antes de continuar. Para obtener más información, consulte AMI | Create (AMI | Crear) en la documentación de AMS.	Ingeniero de migraciones

Incorporar y validar la instancia

Tarea	Descripción	Habilidades requeridas
Envíe la RFC para crear la pila de incorporación de carga de trabajo.	Envíe una solicitud de cambio (RFC) para iniciar AMS WIGS. Para obtener instrucciones, consulte Workload Ingest Stack: Creating (Pila de incorporación de carga de trabajo: creación) en la	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	documentación de AMS. Esto inicia la incorporación de carga de trabajo e instala todo el software requerido por AMS, lo que incluye las herramientas de respaldo, el software de administración de Amazon EC2 y el software antivirus.	

Tarea	Descripción	Habilidades requeridas
Valide que la migración sea correcta.	Una vez completada la incorporación de carga de trabajo, podrá ver la instancia administrada por AMS y la AMI incorporada por AMS. 1. Inicie sesión en la instancia administrada por AMS con las credenciales de dominio. 2. Valide la unión al dominio de la siguiente manera: a. En Explorador de Windows, haga clic con el botón secundario en This PC (Este ordenador) y elija Properties (Propiedades). b. En la sección Especific ación del dispositivo, confirme que aparezca el dominio en el Full device name (Nombre completo del dispositivo). 3. Valide las unidades de disco de origen y destino.	Ingeniero de migraciones

Lanzar la instancia en la cuenta AMS de destino

Tarea	Descripción	Habilidades requeridas
Envíe la RFC para crear una pila de EC2.	1. Con la AMI incorporada por AMS de la instancia de	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	Windows, prepare una RFC para una pila de EC2 de acuerdo con las instrucciones de la sección Create EC2 stack instance (Crear una instancia de pila de EC2) en la documentación de AMS. En la RFC de la pila de EC2, proporcione todos los parámetros, incluidos el nombre del servidor, las etiquetas, la VPC de destino, la subred de destino, el tipo de instancia, los grupos de seguridad de destino, la AMI de incorporación y la función. 2. Envíe la RFC de la pila de EC2 y espere a que la instancia se cree correctamente.	

Recursos relacionados

Recomendaciones de AWS

- Automate pre-workload ingestion activities for AWS Managed Services on Windows (Automatizar las actividades previas a la incorporación de cargas de trabajo para AWS Managed Services en Windows)
- Automatically create an RFC in AMS using Python (Crear automáticamente una RFC en AMS mediante Python)

Documentación de AMS

- AMS Workload Ingest (Incorporar carga de trabajo de AMS)
- How Migration Changes Your Resource (Cómo la migración cambia el recurso)
- Migrating Workloads: Standard Process (Migración de cargas de trabajo: proceso estándar)

Recursos de marketing

- AWS Managed Services
- Preguntas frecuentes de AWS Managed Services
- Recursos de AWS Managed Services
- Características de AWS Managed Services

Migre Db2 para LUW a Amazon EC2 mediante envío de registros para reducir el tiempo de interrupción

Creado por Feng Cai (AWS), Ambarish Satarkar (AWS) y Saurabh Sharma (AWS)

Entorno: Producción	Origen: Db2 para Linux en las instalaciones	Destino: Db2 en Amazon EC2
Tipo R: volver a alojar	Carga de trabajo: IBM	Tecnologías: Migración; bases de datos
Servicios de AWS: AWS Direct Connect; Amazon EBS; Amazon EC2; Amazon S3; AWS Site-to-Site VPN		

Resumen

Cuando los clientes migran sus cargas de trabajo de IBM Db2 for LUW (Linux, UNIX y Windows) a Amazon Web Services (AWS), la forma más rápida es utilizar Amazon Elastic Compute Cloud (Amazon EC2) con el modelo Bring Your Own License (BYOL). Sin embargo, migrar grandes cantidades de datos de Db2 local a AWS puede ser un desafío, especialmente cuando el período de interrupción es corto. Muchos clientes intentan establecer el periodo de interrupción en menos de 30 minutos, lo que deja poco tiempo para la propia base de datos.

Este patrón explica cómo realizar una migración a Db2 con un breve periodo de interrupción mediante el envío del registro de transacciones. Este enfoque se aplica a Db2 en una plataforma Linux little endian.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una instancia Db2 que se ejecuta en una instancia EC2 que coincide con las disposiciones del sistema de archivos en las instalaciones

- Un bucket de Amazon Simple Storage Service (Amazon S3) accesible para la instancia EC2
- Política y función de AWS Identity and Access Management (IAM) para realizar llamadas programáticas a Amazon S3
- Relojes del sistema y zona horaria sincronizados en Amazon EC2 y el servidor en las instalaciones
- La red en las instalaciones conectada a AWS a través de AWS Site-to-Site VPN o AWS Direct Connect

Limitaciones

- La instancia en las instalaciones de Db2 y Amazon EC2 deben estar en la misma familia de plataformas.
- Se debe registrar la carga de trabajo en las instalaciones de Db2. Establezca `blocknonlogged=yes` en la configuración de la base de datos para bloquear cualquier transacción no registrada.

Versiones de producto

- Db2 para LUW, versión 11.5.9 y posteriores

Arquitectura

Pila de tecnología de origen

- Db2 en Linux x86_64

Pila de tecnología de destino

- Amazon EBS
- Amazon EC2
- AWS Identity y Access Management (IAM)
- Amazon S3
- VPN Site-to-Site de AWS o Direct Connect

Arquitectura de destino

El siguiente diagrama muestra una instancia de Db2 que se ejecuta localmente con una conexión de red privada virtual (VPN) a Db2 en Amazon EC2. Las líneas de puntos representan el túnel de VPN entre su centro de datos y la nube de AWS.

Herramientas

Servicios de AWS

- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su shell de línea de comandos.
- AWS Direct Connect vincula su red interna con una ubicación Direct Connect a través de un cable estándar Ethernet de fibra óptica. Con esta conexión, puede crear interfaces virtuales directamente en servicios públicos de AWS omitiendo a los proveedores de servicios de Internet en su ruta de acceso a la red.
- Amazon Elastic Block Store (Amazon EBS) proporciona volúmenes de almacenamiento por bloques para su uso con instancias de Amazon Elastic Compute Cloud (Amazon EC2).
- Amazon Elastic Compute Cloud (Amazon EC2) brinda capacidad de computación escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Site-to-Site VPN le ayuda a transferir el tráfico entre las instancias que lance en AWS y su propia red remota.

Otras herramientas

- db2cli es el comando CLI interactivo de Db2.

Prácticas recomendadas

- En la base de datos de destino, utilice los puntos de conexión de puerta de enlace de Amazon S3 para acceder a la imagen de copia de seguridad y a los archivos de registro de la base de datos en Amazon S3.
- En la base de datos de origen, utilice AWS PrivateLink para Amazon S3 para enviar la imagen de respaldo y los archivos de registro de la base de datos a Amazon S3.

Epics

Configuración de las variables de entorno

Tarea	Descripción	Habilidades requeridas
Configuración de las variables de entorno.	Este patrón utiliza los siguientes nombres: • Nombre de instancia: `db2inst1` • Nombre de la base de datos: `SAMPLE` Puede cambiarlos para adaptarlos a su entorno.	Administrador de base de datos

Configure el servidor Db2 en las instalaciones

Tarea	Descripción	Habilidades requeridas
Configure la CLI de AWS.	Para descargar e instalar la versión más reciente de la AWS CLI, ejecute los siguientes comandos: `$ curl "https://awscli.amazonaws.c`	Administrador de Linux

Tarea	Descripción	Habilidades requeridas
	om/awscli-exe-linu x-x86_64.zip" -o "awscliv2.zip" unzip awscliv2.zip sudo ./aws/install	

Tarea	Descripción	Habilidades requeridas
Configure un destino en las instalaciones para los registros de archivos de Db2.	Para mantener la base de datos de destino de Amazon EC2 sincronizada con la base de datos de origen en las instalaciones, es necesario recuperar los registros de transacciones más recientes del origen. En esta configuración, `/db2logs` se establece como `LOGARCHMETH2` en la fuente como área de almacenam iento provisional. Los registros archivados en este directorio se sincronizarán con Amazon S3 y Db2 accederá a ellos desde Amazon EC2. El patrón usa `LOGARCHMETH2` porque `LOGARCHMETH1` podría haberse configurado para usar una herramienta de un proveedor externo a la que el comando de la CLI de AWS no pudiera acceder. Para recuperar los registros, ejecute el siguiente comando: `db2 connect to sample` `db2 update db cfg for SAMPLE using LOGARCHMETH2 disk:/db2logs`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Realice una copia de seguridad de la base de datos en línea.	Ejecute una copia de seguridad de la base de datos en línea y guárdela en el sistema de archivos de copia de seguridad local: `db2 backup db sample online to /backup`	Administrador de base de datos

Configuración del bucket de S3 y de la política de IAM

Tarea	Descripción	Habilidades requeridas
Crear un bucket de S3.	Cree un bucket de S3 para que el servidor en las instalaciones envíe los archivos de registro y las imágenes Db2 de copia de seguridad a AWS. Amazon EC2 también accederá al bucket: `aws s3api create-bucket --bucket logshipmig-db2 --region us-east-1`	Administrador de sistemas de AWS
Cree una política de IAM.	El `db2bucket.json` archivo contiene la política de IAM para acceder al bucket de Amazon S3: `{ "Version": "2012-10-17", "Statement": [ {`	Administrador AWS, administrador de sistemas AWS

Tarea	Descripción	Habilidades requeridas
	"Effect": "Allow", "Action": ["kms:GenerateDataKey", "kms:Decrypt", "s3:PutObject", "s3:GetObject", "s3:AbortMultipartUpload", "s3:ListBucket", "s3:DeleteObject", "s3:GetObjectVersion", "s3:ListMultipartUploadParts"], "Resource": ["arn:aws:s3:::logshipmig-db2/*", "arn:aws:s3:::logshipmig-db2"] }] }	

Tarea	Descripción	Habilidades requeridas
	Para crear la política, utilice el siguiente comando de la AWS CLI: `aws iam create-policy \ --policy-name db2s3policy \ --policy-document file://db2bucket.json` El resultado de JSON muestra el nombre de recurso de Amazon (ARN) de la política, donde `aws_account_id` representa el ID de su cuenta: `"Arn": "arn:aws:iam::aws_account_id:policy/db2s3policy"`	

Tarea	Descripción	Habilidades requeridas
Adjunte la política de IAM a la función de IAM utilizada por la instancia EC2.	En la mayoría de los entornos de AWS, una instancia EC2 en ejecución tiene un rol de IAM establecido por el administrador del sistema. Si la función de IAM no está configurada, cree la función y elija Modificar la función de IAM en la consola de EC2 para asociar la función a la instancia de EC2 que aloja la base de datos de Db2. Adjunte la política de IAM a la función de IAM con el ARN de la política: `aws iam attach-role-policy \ --policy-arn "arn:aws:iam::aws_account_id:policy/db2s3policy" \ --role-name db2s3role` Una vez asociada la política, cualquier instancia de EC2 asociada a la función de IAM puede acceder al bucket de S3.	Administrador AWS, administrador de sistemas AWS

Envíe los archivos de registro y la imagen de copia de seguridad de la base de datos de origen a Amazon S3

Tarea	Descripción	Habilidades requeridas
Configure la AWS CLI en el servidor Db2 local.	Configure la AWS CLI con el `Access Key ID` y `Secret Access Key` generado en el paso anterior: `$ aws configure` `AWS Access Key ID` `[None]: **********` `AWS Secret Access Key` `[None]: **********` `Default region name` `[None]: us-east-1` `Default output format` `[None]: json`	Administrador AWS, administrador de sistemas AWS
Envíe la imagen de copia de seguridad a Amazon S3.	Anteriormente, se guardó una copia de seguridad de la base de datos en línea en el directorio `/backup` en las instalaciones. Para enviar esa imagen de respaldo al bucket de S3, ejecute el siguiente comando: `aws s3 sync /backup s3://logshipmig-db2/SAMPLE_backup`	Administrador de AWS, ingeniero de migraciones
Envíe los registros de archivo Db2 a Amazon S3.	Sincronice los registros del archivo Db2 local con el bucket de S3 al que puede	Administrador de AWS, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	acceder la instancia de Db2 de destino en Amazon EC2: `aws s3 sync /db2logs s3://logshipmig-db2/SAMPLE_LOG` Ejecute este comando periódicamente mediante cron u otras herramientas de programación. La frecuencia depende de la periodicidad con la que la base de datos de origen archiva los archivos de registro de transacciones.	

Conecte Db2 en Amazon EC2 a Amazon S3 e inicie la sincronización de la base de datos

Tarea	Descripción	Habilidades requeridas
Cree un almacén de claves PKCS12.	Db2 utiliza un almacén de claves de cifrado de estándares de criptografía de clave pública (PKCS) para mantener la seguridad de la clave de acceso de AWS. Cree un almacén de claves y configure la instancia de Db2 de origen para usarla: `gsk8capicmd_64 -keydb -create -db "/home/db2inst1/.keystore/db2s3.p12" -pw "<password>" -type pkcs12 -stash`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`db2 "update dbm cfg using keystore_location /home/db2inst1/.keystore/db2s3.p12 keystore_type pkcs12"`	
Cree el alias de acceso al almacenamiento de Db2.	Para crear el alias de acceso al almacenamiento, utilice la siguiente sintaxis de script: `db2 "catalog storage access alias <alias_name> vendor S3 server <S3 endpoint> container '<bucket_name>'"` Por ejemplo, el script podría tener el siguiente aspecto: `db2 "catalog storage access alias DB2AWSS3 vendor S3 server s3.us-east-1.amazonaws.com container 'logshipmig-db2'"`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Establece el área de almacenamiento provisional.	De forma predeterminada, Db2 usa `DB2_OBJECT_STORAGE_LOCAL_STAGING_PATH` como área de montaje para cargar y descargar archivos desde y hacia Amazon S3. La ruta predeterminada es `sqllib/tmp/RemoteStorage.xxxx`, en el directorio principal de la instancia, y `xxxx` hace referencia al número de partición de Db2. Tenga en cuenta que el área de montaje debe tener capacidad suficiente para almacenar las imágenes de copia de seguridad y los archivos de registro. Puede usar el registro para apuntar el área de montaje a un directorio diferente. También recomendamos usar `DB2_ENABLE_COS_SDK=ON DB2_OBJECT_STORAGE_SETTINGS=EnableStreamingRestore`, y el enlace a la `awssdk` biblioteca para evitar el área de almacenamiento provisional de Amazon S3 para realizar copias de seguridad y restaurar bases de datos:	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`#By root:` `cp -rp /home/db2inst1/sqllib/lib64/awssdk/RHEL/7.6/* /home/db2inst1/sqllib/lib64/` `#By db2 instance owner:` `db2set DB2_OBJECT_STORAGE_LOCAL_STAGING_PATH=/db2stage` `db2set DB2_ENABLE_COS_SDK=ON` `Db2set DB2_OBJECT_STORAGE_SETTINGS=EnableStreamingRestore` `db2stop` `db2start`	
Restaure la base de datos a partir de la imagen de copia de seguridad.	Restaure la base de datos de destino en Amazon EC2 a partir de la imagen de respaldo del bucket de S3: `db2 restore db sample from DB2REMOTE://DB2AWSS3/logshipmig-db2/SAMPLE_backup replace existing`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Restaure la base de datos.	Una vez completada la restauración, la base de datos de destino pasará al estado pendiente de recuperación. Configure `LOGARCHMETH1` y `LOGARCHMETH2` para que Db2 sepa dónde obtener los archivos de registro de transacciones: `db2 update db cfg for SAMPLE using LOGARCHMETH1 'DB2REMOTE://DB2AWSS3//SAMPLE_LOGS/'` `db2 update db cfg for SAMPLE using LOGARCHMETH2 OFF` Inicie la actualización de la base de datos: `db2 ROLLFORWARD DATABASE sample to END OF LOGS` Este comando procesa todos los archivos de registro que se han transferido al bucket de S3. Ejecútelo periódicamente en función de la frecuencia del comando `s3 sync` en los servidores Db2 locales. Por ejemplo, si `s3 sync` se ejecuta cada hora y se tarda 10 minutos en sincronizar todos los archivos de registro,	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	configure el comando para que se ejecute 10 minutos después de cada hora.	

Ponga en línea Db2 en Amazon EC2 durante el periodo de transición

Tarea	Descripción	Habilidades requeridas
Ponga en línea la base de datos de destino.	Durante el periodo de transición, realice una de las siguientes acciones: • Ponga la base de datos local en `ADMIN MODE` y ejecute el comando `s3 sync` para forzar el archivado del último registro de transacciones. • Apague la base de datos. Una vez sincronizado el último registro de transacciones en Amazon S3, ejecute el `ROLLFORWARD` comando por última vez: `db2 rollforward DB sample to END OF LOGS` `db2 rollforward DB sample complete` `Rollforward Status` `....`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`Rollforward status = not pending ....` `DB20000I The ROLLFORWARD command completed successfully.` `db2 activate db sample` `DB20000I The ACTIVATE DATABASE command completed successfully.` Ponga en línea la base de datos de destino y apunte las conexiones de la aplicación a Db2 en Amazon EC2.	

Solución de problemas

Problema	Solución
Si varias bases de datos tienen el mismo nombre de instancia y nombre de base de datos en diferentes hosts (DEV, QA, PROD), las copias de seguridad y los registros pueden ir al mismo subdirectorio.	Utilice diferentes buckets de S3 para DEV, QA y PROD, y añada el nombre de host como prefijo del subdirectorio para evitar confusiones.
Si hay varias imágenes de respaldo en la misma ubicación, aparecerá el siguiente error al realizar la restauración: `SQL2522N More than one backup file matches the time stamp value`	En el `restore` comando, añade la marca de tiempo de la copia de seguridad: `db2 restore db sample from DB2REMOTE://DB2AWSS3/logshipmig-db2/SAMPLE_backup taken at 20230628164042 replace existing`

Problema	Solución
`provided for the backed up database image.`	

Recursos relacionados

- Operaciones de copia de seguridad y restauración de Db2 entre diferentes sistemas operativos y plataformas de hardware
- Configure Db2 STORAGE ACCESS ALIAS y DB2REMOTE
- Comando Db2 ROLLFORWARD
- Método de archivo de registro secundario de Db2

Migración de Db2 para LUW a Amazon EC2 con recuperación de desastres de alta disponibilidad

Creado por Feng Cai (AWS), Aruna Gangireddy (AWS) y Venkatesan Govindan (AWS)

Entorno: producción	Origen: IBM Db2 para LUW en las instalaciones	Destino: Db2 en Amazon EC2
Tipo R: volver a alojar	Carga de trabajo: IBM	Tecnologías: migración; bases de datos; sistemas operativos
Servicios de AWS: AWS Direct Connect; Amazon EC2; Amazon S3; AWS Site-to-Site VPN		

Resumen

Cuando los clientes migran su carga de trabajo de IBM Db2 LUW (Linux, UNIX y Windows) a Amazon Web Services (AWS), lo más rápido es utilizar Amazon Elastic Compute Cloud (Amazon EC2) con el modelo Bring Your Own License (BYOL). Sin embargo, migrar grandes cantidades de datos de Db2 local a AWS puede ser un desafío, especialmente cuando el período de interrupción es corto. Muchos clientes intentan establecer el periodo de interrupción en menos de 30 minutos, lo que deja poco tiempo para la propia base de datos.

Este patrón explica cómo realizar una migración a Db2 con un breve período de interrupción mediante la recuperación de desastres de alta disponibilidad (HADR) de Db2. Este enfoque se aplica a las bases de datos Db2 que se encuentran en la plataforma Linux Little-Endian y no utilizan la característica de particionamiento de datos (DPF).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una instancia de Db2 que se ejecute en una instancia de Amazon EC2 que coincida con los diseños del sistema de archivos en las instalaciones

- Un bucket de Amazon Simple Storage Service (Amazon S3) accesible para la instancia EC2
- Política y función de AWS Identity and Access Management (IAM) para realizar llamadas programáticas a Amazon S3
- Relojes del sistema y zona horaria sincronizados en Amazon EC2 y el servidor en las instalaciones
- La red en las instalaciones conectada a AWS a través de AWS Site-to-Site VPN o AWS Direct Connect
- Comunicación entre el servidor en las instalaciones y Amazon EC2 en los puertos HADR

Limitaciones

- La instancia en las instalaciones de Db2 y Amazon EC2 deben estar en la misma familia de plataformas.
- El HADR no se admite en un entorno de base de datos particionado.
- El HADR no admite el uso de E/S sin procesar (acceso directo al disco) para los archivos de registro de la base de datos.
- HADR no admite registros infinitos.
- `LOGINDEXBUILD` debe configurarse como `YES`, lo que aumentará el uso del registro para reconstruir el índice.
- Se debe registrar la carga de trabajo en las instalaciones de Db2. Configure `blocknonlogged=yes` en la configuración de la base de datos para bloquear cualquier transacción no registrada.

Versiones de producto

- Db2 para LUW, versión 11.5.9 y posteriores

Arquitectura

Pila de tecnología de origen

- Db2 en Linux x86_64

Pila de tecnología de destino

- Amazon EC2

- AWS Identity y Access Management (IAM)
- Amazon S3
- AWS Site-to-Site VPN

Arquitectura de destino

En el siguiente diagrama, Db2 en las instalaciones se ejecuta `db2-server1` como principal. Tiene dos objetivos HADR en espera. Hay un objetivo de reserva en las instalaciones y es opcional. El otro objetivo en espera, `db2-ec2`, está en Amazon EC2. Una vez que la base de datos pasa a AWS, `db2-ec2` pasa a ser la principal.

1. Los registros se transmiten desde la base de datos en las instalaciones principal a la base de datos en las instalaciones en espera.
2. Con el HADR de Db2, los registros se transmiten desde la base de datos en las instalaciones principal a través de una Site-to-Site VPN a Db2 en Amazon EC2.
3. Los registros de copia de seguridad y archivo de Db2 se envían desde la base de datos en las instalaciones principal al bucket de S3 en AWS.

Herramientas

Servicios de AWS

- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su shell de línea de comandos.
- AWS Direct Connect vincula su red interna con una ubicación Direct Connect a través de un cable estándar Ethernet de fibra óptica. Con esta conexión, puede crear interfaces virtuales directamente en servicios públicos de AWS y derivar a los proveedores de Internet a su ruta de acceso a la red.
- Amazon Elastic Compute Cloud (Amazon EC2) brinda capacidad de computación escalable en la Nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Site-to-Site VPN le ayuda a transferir el tráfico entre las instancias que lance en AWS y su propia red remota.

Otras herramientas

- db2cli es el comando CLI interactivo de Db2.

Prácticas recomendadas

- En la base de datos de destino, utilice los puntos de conexión de puerta de enlace de Amazon S3 para acceder a la imagen de copia de seguridad y a los archivos de registro de la base de datos en Amazon S3.
- En la base de datos de origen, utilice AWS PrivateLink para Amazon S3 para enviar la imagen de respaldo y los archivos de registro de la base de datos a Amazon S3.

Epics

Configuración de las variables de entorno

Tarea	Descripción	Habilidades requeridas
Configuración de las variables de entorno.	Este patrón utiliza los siguientes nombres y puertos: 1. Nombre de host en las instalaciones de Db2: `db2-server1` 2. Nombre de host en espera de HADR: `db2-server2` (si HADR se está ejecutando actualmente en las instalaciones) 3. Nombre de host de Amazon EC2: `db2-ec2`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	4. Nombre de instancia: `db2inst1` 5. Nombre de la base de datos: `SAMPLE` 6. Puertos HDR: • `db2-server1: 50010` • `db2-server2: 50011` • `db2-ec2: 50012` Puede cambiarlos para adaptarlos a su entorno.	

Configure el servidor Db2 en las instalaciones

Tarea	Descripción	Habilidades requeridas
Configure AWS CLI.	Para descargar e instalar la versión más reciente de la AWS CLI, ejecute los siguientes comandos: `$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"` `unzip awscliv2.zip` `sudo ./aws/install`	Administrador de Linux
Configure un destino en las instalaciones para los registros de archivos de Db2.	Condiciones como los trabajos por lotes de actualización intensiva y la ralentización de la red pueden provocar un retraso en el servidor HADR	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	en espera. Para ponerse al día, el servidor en espera necesita los registros de transacciones del servidor principal. La secuencia de lugares de los registros de solicitud es la siguiente: • El directorio de registro activo del servidor principal • La ubicación `LOGARCHMETH1` o `LOGARCHMETH2` en el servidor en espera • La ubicación `LOGARCHMETH1` o `LOGARCHMETH2` en el servidor principal En esta configuración, `/db2logs` se establece como `LOGARCHMETH2` en la fuente como área de almacenamiento provisional. Los registros archivados en este directorio se sincronizarán con Amazon S3 y Db2 accederá a ellos desde Amazon EC2. El patrón se usa `LOGARCHMETH2` porque `LOGARCHMETH1` podría haberse configurado para usar una herramienta de un proveedor externo a la que el comando de AWS CLI no puede acceder:	

Tarea	Descripción	Habilidades requeridas
	`db2 connect to sample` `db2 update db cfg for SAMPLE using LOGARCHMETH2 disk:/db2logs`	
Realice una copia de seguridad de la base de datos en línea.	Ejecute una copia de seguridad de la base de datos en línea y guárdela en el sistema de archivos de copia de seguridad local: `db2 backup db sample online to /backup`	Administrador de base de datos

Configuración del bucket de S3 y de la política de IAM

Tarea	Descripción	Habilidades requeridas
Crear un bucket de S3.	Cree un bucket de S3 para que el servidor en las instalaciones envíe los archivos de registro y las imágenes Db2 de copia de seguridad a AWS. Amazon EC2 accederá al bucket: `aws s3api create-bucket --bucket hadrmig-db2 --region us-east-1`	Administrador de AWS
Cree una política de IAM.	El `db2bucket.json` archivo contiene la política de IAM para acceder al bucket de S3: `{`	Administrador AWS, administrador de sistemas AWS

Tarea	Descripción	Habilidades requeridas
	"Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["kms:GenerateDataKey", "kms:Decrypt", "s3:PutObject", "s3:GetObject", "s3:AbortMultipartUpload", "s3:ListBucket", "s3:DeleteObject", "s3:GetObjectVersion", "s3:ListMultipartUploadParts"], "Resource": ["arn:aws:s3:::hadrmig-db2/*", "arn:aws:s3:::hadrmig-db2"] }]	

Tarea	Descripción	Habilidades requeridas
	<pre>}</pre> Para crear la política, utilice el siguiente comando de la AWS CLI: <pre>aws iam create-policy \ --policy-name db2s3hapolicy \ --policy-document file://db2bucket.j son</pre> El resultado de JSON muestra el nombre de recurso de Amazon (ARN) de la política, donde `aws_account_id` representa el ID de su cuenta: <pre>"Arn": "arn:aws: iam::aws_account_i d:policy/db2s3hapo licy"</pre>	

Tarea	Descripción	Habilidades requeridas
Adjunte la política de IAM al rol de IAM.	Por lo general, la instancia EC2 con Db2 en ejecución tendría una función de IAM asignada por el administr ador del sistema. Si no se ha asignado ningún rol de IAM, puede elegir Modificar el rol de IAM en la consola Amazon EC2. Adjunte la política de IAM a la función de IAM asociada a la instancia EC2. Una vez asociada la política, la instancia EC2 puede acceder al bucket de S3: `aws iam attach-role-policy --policy-arn "arn:aws:iam::aws_account_id:policy/db2s3hapolicy" --role-name db2s3harole`	

Envíe los archivos de registro y la imagen de copia de seguridad de la base de datos de origen a Amazon S3

Tarea	Descripción	Habilidades requeridas
Configure AWS CLI en el servidor Db2 en las instalaci ones.	Configure la AWS CLI con el `Access Key ID` y `Secret Access Key` que generó anteriormente: `$ aws configure`	Administrador AWS, administr ador de sistemas AWS

Tarea	Descripción	Habilidades requeridas
	`AWS Access Key ID [None]: ********** AWS Secret Access Key [None]: ********* ********** Default region name [None]: us-east-1 Default output format [None]: json`	
Envíe la imagen de copia de seguridad a Amazon S3.	Anteriormente, se guardó una copia de seguridad de la base de datos en línea en el directorio `/backup` en las instalaciones. Para enviar esa imagen de respaldo al bucket de S3, ejecute el siguiente comando: `aws s3 sync /backup s3://hadrmig-db2/SAMPLE_backup`	Administrador AWS, administrador de sistemas AWS

Tarea	Descripción	Habilidades requeridas
Envíe los registros de archivo Db2 a Amazon S3.	Sincronice los registros del archivo Db2 local con el bucket de Amazon S3 al que puede acceder la instancia de Db2 de destino en Amazon EC2: `aws s3 sync /db2logs s3://hadrmig-db2/SAMPLE_LOGS` Ejecute este comando periódicamente mediante cron u otras herramientas de programación. La frecuencia depende de la periodicidad con la que la base de datos de origen archiva los archivos de registro de transacciones.	

Conecte Db2 de Amazon EC2 a Amazon S3 e inicie la sincronización inicial de la base de datos

Tarea	Descripción	Habilidades requeridas
Cree un almacén de claves PKCS12.	Db2 utiliza un almacén de claves de cifrado de estándares de criptografía de clave pública (PKCS) para mantener la seguridad de la clave de acceso de AWS. Cree un almacén de claves y configure el Db2 de origen para usarlo: `gsk8capicmd_64 -keydb -create -db "/home/db`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	2inst1/.keystore/db2s3.p12" -pw "<password>" -type pkcs12 -stash db2 "update dbm cfg using keystore_location /home/db2inst1/.keystore/db2s3.p12 keystore_type pkcs12"	

Tarea	Descripción	Habilidades requeridas
Cree el alias de acceso al almacenamiento de Db2.	Db2 usa un alias de acceso al almacenamiento para acceder a Amazon S3 directamente con los comandos `INGEST`, `LOAD`, `BACKUP DATABASE` o `RESTORE DATABASE`. Porque ha asignado una función de IAM a la instancia EC2 `USER` y `PASSWORD` no es obligatorio: `db2 "catalog storage access alias <alias_name> vendor S3 server <S3 endpoint> container '<bucket_name>'"` Por ejemplo, el script podría tener el siguiente aspecto: `db2 "catalog storage access alias DB2AWSS3 vendor S3 server s3.us-east-1.amazonaws.com container 'hadrmig-db2'"`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Establece el área de almacenamiento provisional.	Recomendamos usar `DB2_ENABLE_COS_SDK=ON DB2_OBJECT_STORAGE_SETTINGS=EnableStreamingRestore` , y el enlace a la `awssdk` biblioteca para evitar el área de almacenamiento provisional de Amazon S3 para realizar copias de seguridad y restaurar bases de datos: `#By root:` `cp -rp /home/db2inst1/sqllib/lib64/awssdk/RHEL/7.6/* /home/db2inst1/sqllib/lib64/` `#By db2 instance owner:` `db2set DB2_OBJECT_STORAGE_LOCAL_STAGING_PATH=/db2stage` `db2set DB2_ENABLE_COS_SDK=ON` `db2set DB2_OBJECT_STORAGE_LOCAL_STAGING_PATH=/db2stage` `db2stop` `db2start`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Restaure la base de datos a partir de la imagen de copia de seguridad.	Restaure la base de datos de destino en Amazon EC2 a partir de la imagen de respaldo del bucket de S3: `db2 create db sample on /data1` `db2 restore db sample from DB2REMOTE://DB2AWSS3/hadrmig-db2/SAMPLE_backup replace existing`	Administrador de base de datos

Configurar HADR sin HADR en las instalaciones

Tarea	Descripción	Habilidades requeridas
Configure el servidor Db2 en las instalaciones como el principal.	Actualice los ajustes de configuración de la base de datos para el HADR en `db2-server1` (la fuente en las instalaciones) como principal . `HADR_SYNCMODE` Configúrelo en el `SUPERASYNC` modo que tenga el menor tiempo de respuesta a las transacciones: `db2 update db cfg for sample using HADR_LOCAL_HOST db2-server1 HADR_LOCAL_SVC 50010 HADR_REMOTE_HOST db2-ec2 HADR_REMOTE_SVC 50012 HADR_REMOTE_INST db2inst1`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`HADR_SYNCMODE SUPERASYNC DB20000 I The UPDATE DATABASE CONFIGURATION command completed successfu lly` Se esperan algunos retrasos en la red entre el centro de datos en las instalaciones y AWS. (Puede establecer un valor `HADR_SYNCMODE` diferente en función de la fiabilidad de la red. Para obtener más informaci ón, consulte la sección de Recursos relacionados.	
Cambie el destino del archivo de registro de la base de datos de destino.	Cambie el destino del archivo de registros de la base de datos de destino para que coincida con el entorno Amazon EC2: `db2 update db cfg for SAMPLE using LOGARCHME TH1 'DB2REMOTE://DB2AW SS3//SAMPLE_LOGS/' LOGARCHMETH2 OFF DB20000I The UPDATE DATABASE CONFIGURA TION command completed successfully`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Configure HADR para Db2 en el servidor Amazon EC2.	Actualice la configuración de la base de datos para el HADR en `db2-ec2` modo de espera: `db2 update db cfg for sample using HADR_LOCAL_HOST db2-ec2 HADR_LOCAL_SVC 50012 HADR_REMOTE_HOST db2-server1 HADR_REMOTE_SVC 50010 HADR_REMOTE_INST db2inst1 HADR_SYNCMODE SUPERASYNC DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Verifique la configuración de HADR.	Compruebe los parámetros del HADR en los servidores Db2 de origen y destino. Para comprobar que la configuración está activada`db2-server1` , ejecute el siguiente comando: `db2 get db cfg for sample|grep HADR` `HADR database role = PRIMARY` `HADR local host name (HADR_LOCAL_HOST) = db2-server1` `HADR local service name (HADR_LOCAL_SVC) = 50010` `HADR remote host name (HADR_REMOTE_HOST) = db2-ec2` `HADR remote service name (HADR_REMOTE_SVC) = 50012` `HADR instance name of remote server (HADR_REMOTE_INST) = db2inst1` `HADR timeout value (HADR_TIMEOUT) = 120` `HADR target list (HADR_TARGET_LIST) =` `HADR log write synchronization mode`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	<pre>(HADR_SYNCMODE) = NEARSYNC HADR spool log data limit (4KB) (HADR_SPOOL_LIMIT) = AUTOMATIC(52000) HADR log replay delay (seconds) (HADR_REPLAY_DELAY) = 0 HADR peer window duration (seconds) (HADR_PEER_WINDOW) = 0 HADR SSL certificate label (HADR_SSL_LABEL) = HADR SSL Hostname Validation (HADR_SSL_HOST_VAL) = OFF</pre> Para comprobar que la configuración está activada`db2-ec2`, ejecute el siguiente comando: <pre>db2 get db cfg for sample|grep HADR HADR database role = STANDBY HADR local host name (HADR_LOCAL_HOST) = db2-ec2 HADR local service name (HADR_LOCAL_SVC) = 50012 HADR remote host name (HADR_REM</pre>	

Tarea	Descripción	Habilidades requeridas
	OTE_HOST) = db2-serve r1 HADR remote service name (HADR_REMOTE_SVC) = 50010 HADR instance name of remote server (HADR_REMOTE_INST) = db2inst1 HADR timeout value (HADR_TIMEOUT) = 120 HADR target list (HADR_TAR GET_LIST) = HADR log write synchronization mode (HADR_SYNCMODE) = SUPERASYNC HADR spool log data limit (4KB) (HADR_SPOOL_LIMIT) = AUTOMATIC(52000) HADR log replay delay (seconds) (HADR_REP LAY_DELAY) = 0 HADR peer window duration (seconds) (HADR_PEER_WINDOW) = 0 HADR SSL certifica te label (HADR_SSL_LABEL) = HADR SSL Hostname Validation (HADR_SSL_HOST_VAL) = OFF Los parámetros HADR_LOCA L_HOST , HADR_LOCA L_SVC , HADR_REMO	

Tarea	Descripción	Habilidades requeridas
	`TE_HOST` y `HADR_REMO` `TE_SVC` indican una configuración de HADR principal y otra de reserva.	
Inicie la instancia HADR de Db2.	Inicie primero la instancia HADR de Db2 en el servidor `db2-ec2` en espera: `db2 start hadr on db sample as standby` `DB20000I The START HADR ON DATABASE command completed successfully.` Inicie el HADR de Db2 en el servidor principal (de origen): `db2-server1` `db2 start hadr on db sample as primary` `DB20000I The START HADR ON DATABASE command completed successfully.` La conexión HADR entre Db2 en las instalaciones y Amazon EC2 ya se ha establecido correctamente. El servidor principal de Db2 `db2-server1` comienza a transmitir los registros de transacciones a `db2-ec2` en tiempo real.	Administrador de base de datos

Configure HADR cuando HADR exista en las instalaciones

Tarea	Descripción	Habilidades requeridas
Añada Db2 en Amazon EC2 como reserva auxiliar.	Si HADR se ejecuta en la instancia de Db2 local, puede añadir Db2 en Amazon EC2 como modo de espera auxiliar `HADR_TARGET_LIST` mediante la ejecución de los siguientes comandos en: `db2-ec2` `db2 update db cfg for sample using HADR_LOCAL_HOST db2-ec2 HADR_LOCAL_SVC 50012 HADR_REMOTE_HOST db2-server1 HADR_REMOTE_SVC 50010 HADR_REMOTE_INST db2inst1 HADR_SYNCMODE SUPERASYNC DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully. db2 update db cfg for sample using HADR_TARGET_LIST "db2-server1:50010 |db2-server2:50011 " DB20000I The UPDATE DATABASE CONFIGURATION command`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`completed successfully.`	

Tarea	Descripción	Habilidades requeridas
Agregue la información auxiliar en espera a los servidores en las instalaciones.	Actualice `HADR_TARGET_LIST` en los dos servidores en las instalaciones (principal y en espera). Activado, ejecute el siguiente `db2-server1` código: `db2 update db cfg for sample using HADR_TARGET_LIST "db2-server2:50011|db2-ec2:50012" DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully. SQL1363W One or more of the parameters submitted for immediate modification were not changed dynamically. For these configuration parameters, the database must be shutdown and reactivated before the configuration parameter changes become effective.`  `db2-server2` Activado, ejecuta el siguiente código:  `db2 update db cfg for sample using HADR_TARG`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`ET_LIST "db2-serv er1:50010|db2-ec2: 50012" DB20000I The UPDATE DATABASE CONFIGURATION command completed successfu lly. SQL1363W One or more of the parameter s submitted for immediate modificat ion were not changed dynamically. For these configura tion parameters, the database must be shutdown and reactivated before the configuration parameter changes become effective.`	

Tarea	Descripción	Habilidades requeridas
Verifique la configuración de HADR.	Compruebe los parámetros del HADR en los servidores Db2 de origen y destino. `db2-server1` Activado, ejecuta el siguiente código: `db2 get db cfg for sample|grep HADR` `HADR database role = PRIMARY` `HADR local host name (HADR_LOCAL_HOST) = db2-server1` `HADR local service name (HADR_LOCAL_SVC) = 50010` `HADR remote host name (HADR_REMOTE_HOST) = db2-server2` `HADR remote service name (HADR_REMOTE_SVC) = 50011` `HADR instance name of remote server (HADR_REMOTE_INST) = db2inst1` `HADR timeout value (HADR_TIMEOUT) = 120` `HADR target list (HADR_TARGET_LIST) = db2-server2:50011|db2-ec2:50012`	

Tarea	Descripción	Habilidades requeridas
	HADR log write synchronization mode (HADR_SYNCMODE) = NEARSYNC HADR spool log data limit (4KB) (HADR_SPOOL_LIMIT) = AUTOMATIC(52000) HADR log replay delay (seconds) (HADR_REPLAY_DELAY) = 0 HADR peer window duration (seconds) (HADR_PEER_WINDOW) = 0 HADR SSL certificate label (HADR_SSL_LABEL) = HADR SSL Hostname Validation (HADR_SSL_HOST_VAL) = OFF `db2-server2` Activado, ejecuta el siguiente código: `db2 get db cfg for sample|grep HADR` HADR database role = STANDBY HADR local host name (HADR_LOCAL_HOST) = db2-server2 HADR local service name (HADR_LOCAL_SVC) = 50011 HADR remote host name (HADR_REMOTE_HOST) = db2-server1	

Tarea	Descripción	Habilidades requeridas
	HADR remote service name (HADR_REMOTE_SVC) = 50010 HADR instance name of remote server (HADR_REMOTE_INST) = db2inst1 HADR timeout value (HADR_TIMEOUT) = 120 HADR target list (HADR_TARGET_LIST) = db2-server1:50010|db2-ec2:50012 HADR log write synchronization mode (HADR_SYNCMODE) = NEARSYNC HADR spool log data limit (4KB) (HADR_SPOOL_LIMIT) = AUTOMATIC(52000) HADR log replay delay (seconds) (HADR_REPLAY_DELAY) = 0 HADR peer window duration (seconds) (HADR_PEER_WINDOW) = 0 HADR SSL certificate label (HADR_SSL_LABEL) = HADR SSL Hostname Validation (HADR_SSL_HOST_VAL) = OFF db2-ec2Activado, ejecuta el siguiente código:	

Tarea	Descripción	Habilidades requeridas
	`db2 get db cfg for sample|grep HADR` `HADR database role = STANDBY` `HADR local host name (HADR_LOCAL_HOST) = db2-ec2` `HADR local service name (HADR_LOCAL_SVC) = 50012` `HADR remote host name (HADR_REMOTE_HOST) = db2-server1` `HADR remote service name (HADR_REMOTE_SVC) = 50010` `HADR instance name of remote server (HADR_REMOTE_INST) = db2inst1` `HADR timeout value (HADR_TIMEOUT) = 120` `HADR target list (HADR_TARGET_LIST) = db2-server1:50010|db2-server2:50011` `HADR log write synchronization mode (HADR_SYNCMODE) = SUPERASYNC` `HADR spool log data limit (4KB) (HADR_SPOOL_LIMIT) = AUTOMATIC(52000)`	

Tarea	Descripción	Habilidades requeridas
	HADR log replay delay (seconds) (HADR_REPLAY_DELAY) = 0 HADR peer window duration (seconds) (HADR_PEER_WINDOW) = 0 HADR SSL certificate label (HADR_SSL_LABEL) = HADR SSL Hostname Validation (HADR_SSL_HOST_VAL) = OFF Los parámetros HADR_LOCAL_HOST , HADR_LOCAL_SVC , HADR_REMOTE_HOST , HADR_REMOTE_SVC y HADR_TARGET_LIST indican una configuración de HADR principal y otra en espera.	

Tarea	Descripción	Habilidades requeridas
Detenga e inicie el Db2 HADR.	`HADR_TARGET_LIST` ya está configurado en los tres servidores. Cada servidor Db2 conoce los otros dos. Detenga y reinicie el HADR (interrup ción breve) para aprovechar la nueva configuración. `db2-server1` Activado, ejecute los siguientes comandos: `db2 stop hadr on db sample` `db2 deactivate db sample` `db2 activate db sample` `db2-server2` Activado, ejecute los siguientes comandos: `db2 deactivate db sample` `db2 start hadr on db sample as standby` `SQL1766W The command completed successfully` `db2-ec2`Activado, ejecute los siguientes comandos: `db2 start hadr on db sample as standby` `SQL1766W The command completed successfully`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`db2-server1` Activado, ejecute los siguientes comandos: `db2 start hadr on db sample as primary` `SQL1766W The command completed successfully` La conexión HADR entre Db2 en las instalaciones y Amazon EC2 ya se ha establecido correctamente. El servidor principal de Db2 `db2-server1` comienza a transmitir los registros de transacciones a `db2-server2` y `db2-ec2` en tiempo real.	

Haga que Db2 en Amazon EC2 sea principal durante la ventana de transición

Tarea	Descripción	Habilidades requeridas
Asegúrese de que no haya ningún retraso HADR en el servidor en espera.	Compruebe el estado del HADR desde el servidor principal. `db2-server1` No se alarme cuando `HADR_STATE` esté en estado `REMOTE_CATCHUP`, lo cual es normal cuando `HADR_SYNCMODE` está configurado en `SUPERASYNC`. Los `PRIMARY_LOG_TIME` y `STANDBY_REPLAY_LOG`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	_TIME muestran que están sincronizados: `db2pd -hadr -db sample` `HADR_ROLE = PRIMARY` `REPLAY_TYPE = PHYSICAL` `HADR_SYNCMODE = SUPERASYNC` `STANDBY_ID = 2` `LOG_STREAM_ID = 0` `HADR_STATE = REMOTE_CATCHUP` `.....` `PRIMARY_LOG_TIME = 10/26/2022 02:11:32.000000 (1666750292)` `STANDBY_LOG_TIME = 10/26/2022 02:11:32.000000 (1666750292)` `STANDBY_REPLAY_LOG_TIME = 10/26/2022 02:11:32.000000 (1666750292)`	

Tarea	Descripción	Habilidades requeridas
Ejecute la adquisición HADR.	Para completar la migración , especifique `db2-ec2` como la base de datos principal ejecutando el comando de adquisición de HADR. Usa el comando db2pd para verificar el `HADR_ROLE` valor: `db2 TAKEOVER HADR ON DATABASE sample` `DB20000I The TAKEOVER HADR ON DATABASE command completed successfully.` `db2pd -hadr -db sample` `Database Member 0 -- Database SAMPLE -- Active -- Up 0 days 00:03:25 -- Date 2022-10-26-02.46.45.048988` `HADR_ROLE = PRIMARY` `REPLAY_TYPE = PHYSICAL` Para completar la migración a AWS, dirija las conexiones de la aplicación a Db2 en Amazon EC2.	

Solución de problemas

Problema	Solución
Si utiliza la NAT por motivos de seguridad y firewall, el host puede tener dos direccion es IP (una interna y otra externa), lo que puede provocar un error de comprobación de dirección IP del HADR. El `START HADR ON DATABASE` comando devolverá el siguiente mensaje: `HADR_LOCAL_HOST:HADR_LOCAL_SVC (-xx-xx-xx-xx.:50011 (xx.xx.xx .xx:50011)) on remote database is different from HADR_REMOTE_HOST:H ADR_REMOTE_SVC (xx-xx-xx- xx.:50011 (x.x.x.x:50011)) on local database.`	Para admitir el HADR en un entorno NAT, puede configurar el `HADR_LOCAL_HOST` con la dirección interna y externa. Por ejemplo, si el servidor Db2 tiene el nombre interno `host1` y el nombre externo `host1E`, `HADR_LOCA L_HOST` puede ser. `HADR_LOCAL_HOST: "host1 | host1E"`

Recursos relacionados

- Operaciones de copia de seguridad y restauración de Db2 entre diferentes sistemas operativos y plataformas de hardware
- Configure Db2 STORAGE ACCESS ALIAS y DB2REMOTE
- Recuperación de desastres de alta disponibilidad de Db2
- hadr_syncmode: modo de sincronización HADR para escrituras de registros en un parámetro de configuración de estado del mismo nivel

Migración de las máquinas virtuales de VMware con HCX Automation mediante PowerCLI

Creado por Giri Nadiminty (AWS), Hassan Adekoya (AWS) y Naveen Deshwal

Entorno: producción	Origen: VMware vCenter o SDDC local o basado en la nube	Destino: VMware Cloud en AWS
Tipo R: volver a alojar	Carga de trabajo: todas las demás cargas de trabajo	Tecnologías: migración; nube híbrida
Servicios de AWS: VMware Cloud en AWS		

Resumen

Aviso: A partir del 30 de abril de 2024, VMware Cloud on AWS ya no será revendido por AWS sus socios de canal. El servicio seguirá estando disponible a través de Broadcom. Le recomendamos que se ponga en contacto con su AWS representante para obtener más información.

Este patrón describe cómo migrar las máquinas virtuales (VM) en las instalaciones de VMware a VMware Cloud en AWS mediante la automatización de la extensión de la nube híbrida de VMware (HCX) basada en scripts VMware PowerCLI. PowerCLI es una herramienta de línea de comandos que se basa en Windows. PowerShell Le ayuda a administrar el software de VMware y automatiza las tareas de infraestructura y migración.

Puede adaptar este patrón para la migración entre cualquier combinación de vCenters, centros de datos definidos por software (SDDC) y entornos de nube. Los scripts de PowerCLI incluidos en este patrón utilizan la automatización en lugar de hacer clic con el ratón para todas las tareas de configuración y programación de las máquinas virtuales, por lo que ahorran tiempo en las actividades de migración y ayudan a reducir el riesgo de errores humanos.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de VMware Cloud en AWS con SDDC
- Un vCenter o SDDC existente en las instalaciones o en la nube
- Una cuenta de usuario con los permisos necesarios para los vCenters o SDDC de origen y destino
- Emparejamiento de sitios HCX con la Extensión de red HCX (HCX-NE) configurada entre los vCenters o SDDC de origen y destino
- VMware PowerCLI está instalado en el servidor de su elección

Limitaciones

- Si la vCenter de origen usa Cross-vCenter NSX, el módulo PowerCLI no funcionará. Utilice un método de secuencias de comandos (como Python) con la API HCX en lugar de PowerCLI.
- Si las máquinas virtuales migradas necesitan nombres o direcciones IP nuevos, utilice un método de secuencias de comandos (como Python) con la API HCX.
- Este patrón no rellena el archivo.csv, que es obligatorio. Puede rellenar el archivo mediante VMware vRealize Network Insight (vRNI) o algún otro método.

Versiones de producto

- VMware vSphere versión 5 o posterior
- VMware HCX versión 4.4 o posterior
- VMware PowerCLI versión 12.7 o posterior

Arquitectura

Pila de tecnología de origen

- VMware en las instalaciones o basado en la nube

Pila de tecnología de destino

- VMware Cloud en AWS

Arquitectura de destino

Herramientas

Servicios de AWS

- VMware Cloud en AWS es un servicio diseñado conjuntamente por AWS y VMware para ayudarle a migrar y a ampliar sus entornos en las instalaciones basados en VMware vSphere a la nube de AWS.

Otras herramientas

- VMware Hybrid Cloud Extension (HCX) es una utilidad para migrar cargas de trabajo desde su entorno VMware local a VMware Cloud en AWS sin cambiar la plataforma subyacente. Nota: Este producto se conocía anteriormente como Hybrid Cloud Extension y NSX Hybrid Connect. Este patrón usa HCX para la migración de máquinas virtuales.
- VMware PowerCLI es una herramienta de línea de comandos para automatizar la administración de VMware vSphere y vCloud. Los comandos de PowerCLI en Windows PowerShell se ejecutan mediante cmdlets. PowerShell Este patrón usa PowerCLI para ejecutar los comandos de migración.

Código

Script sencillo e independiente

Le recomendamos que utilice este script de un solo equipo para las pruebas iniciales, a fin de comprobar que las opciones de configuración se aceptan y se comportan según lo esperado. Para obtener instrucciones, consulte la sección Epics.

```
<# Manual Variables #>
$HcxServer = "[enterValue]"
$SrcNetworkName = "[enterValue]"
$DstNetworkName = "[enterValue]"
$DstComputeName = "[enterValue]"
$DstDSName = "[enterValue]"
$DstFolderName = "[enterValue]"
$vmName = "[enterValue]"

<# Environment Setup #>
Connect-HCXServer -Server $HcxServer
$HcxDstSite = Get-HCXSite -Destination
$HcxSrcSite = Get-HCXSite -Source
```

```
$SrcNetwork = Get-HCXNetwork -Name $SrcNetworkName -Type VirtualWire -Site $HcxSrcSite
$DstNetwork = Get-HCXNetwork -Name $DstNetworkName -Type NsxtSegment -Site $HcxDstSite
$DstCompute = Get-HCXContainer -Name $DstComputeName -Site $HcxDstSite
$DstDS = Get-HCXDatastore -Name $DstDSName -Site $HcxDstSite
$DstFolder = Get-HCXContainer -name $DstFolderName -Site $HcxDstSite
$vm = Get-HCXVM -Name $vmName

<# Migration #>
$NetworkMapping = New-HCXNetworkMapping -SourceNetwork $SrcNetwork -DestinationNetwork
 $DstNetwork
$NewMigration = New-HCXMigration -VM $vm -MigrationType vMotion -SourceSite $HcxSrcSite
 -DestinationSite $HcxDstSite -Folder $DstFolder -TargetComputeContainer $DstCompute
 -TargetDatastore $DstDS -NetworkMapping $NetworkMapping -DiskProvisionType Thin
 -UpgradeVMTools $True -RemoveISOs $True -ForcePowerOffVm $True -RetainMac $True -
UpgradeHardware $True -RemoveSnapshots $True
```

Script basado en .csv con todas las funciones

Una vez finalizadas las pruebas, puede utilizar el siguiente script en sus entornos de producción. Para obtener instrucciones, consulte la sección Epics.

```
<# Schedule #>
write-host("Getting Time for Scheduling")
$startTime = [DateTime]::Now.AddDays(12)
$endTime = [DateTime]::Now.AddDays(15)

<# Migration #>
Connect-HCXServer -Server [enterValue]
write-host("Getting Source Site")
$HcxSrcSite = Get-HCXSite
write-host("Getting Target Site")
$HcxDstSite = Get-HCXSite -Destination
$HCXVMS = Import-CSV .\Import_VM_list.csv
ForEach ($HCXVM in $HCXVMS) {
    $DstFolder = Get-HCXContainer $HCXVM.DESTINATION_VM_FOLDER -Site $HcxDstSite
    $DstCompute = Get-HCXContainer $HCXVM.DESTINATION_COMPUTE  -Site $HcxDstSite
    $DstDatastore = Get-HCXDatastore $HCXVM.DESTINATION_DATASTORE -Site $HcxDstSite
    $SrcNetwork = Get-HCXNetwork $HCXVM.SOURCE_NETWORK -Type VirtualWire -Site
 $HcxSrcSite
    $DstNetwork = Get-HCXNetwork $HCXVM.DESTINATION_NETWORK -Type NsxtSegment -Site
 $HcxDstSite
    $NetworkMapping = New-HCXNetworkMapping -SourceNetwork $SrcNetwork -
DestinationNetwork $DstNetwork
```

```
    $NewMigration = New-HCXMigration -VM (Get-HCXVM $HCXVM.VM_NAME) -MigrationType
 Bulk -SourceSite $HcxSrcSite -DestinationSite $HcxDstSite -Folder $DstFolder -
TargetComputeContainer $DstCompute -TargetDatastore $DstDatastore -NetworkMapping
 $NetworkMapping -DiskProvisionType Thin -UpgradeVMTools $True -RemoveISOs $True -
ForcePowerOffVm $True -RetainMac $True -UpgradeHardware $True -RemoveSnapshots $True -
ScheduleStartTime $startTime -ScheduleEndTime $endTime
    Start-HCXMigration -Migration $NewMigration -Confirm:$false
}
```

Epics

Recopile información para las variables manuales

Tarea	Descripción	Habilidades requeridas
Busque los nombres de los servidores vCenter y SDDC de origen y destino.	Los scripts de PowerCLI requieren las variables descritas en esta epopeya. Puede recopilar esta informaci ón con antelación para facilitar el uso de los scripts. En la sección HCX de la consola vSphere, elija Infraestructura, Emparejam iento de sitios. Anote los nombres de los servidore s de origen y destino que aparecen.	Arquitecto de la nube
Busque los nombres de los HCX de origen y destino.	En la sección HCX de la consola vSphere, elija Sistema, Administración. Anote los nombres de los HCX de origen y destino que aparecen.	Arquitecto de la nube
Busque los nombres de las redes de origen y destino.	En la sección HCX de la consola vSphere, elija	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	Sistema, Extensión de red. Anote los nombres de las redes de origen y destino. Nota: Como alternativa, puede obtener los nombres de las redes de origen y destino mediante los comandos Get-HCXNetwork y Get-HCXNetwork-Destination de PowerCLI después de conectarse al servidor HCX.	
Recopile información adicional de la consola vSphere.	En la consola vSphere, recopile la siguiente informaci ón: • Nombres de las máquinas virtuales que desea migrar • Entorno informático de destino (clúster/host) • Almacén de datos de destino • Nombre de la carpeta de la VM de destino	Arquitecto de la nube

Tome decisiones de migración

Tarea	Descripción	Habilidades requeridas
Determine las opciones de migración.	Determine lo siguiente: • `MigrationType` : Los tipos de migración asistida por HCX son VMotion, bulk,	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	cold y RAV. La elección depende de los requisitos de tiempo de inactividad, el ancho de banda de la red, el período de migración y el tipo de carga de trabajo. Para obtener más información, consulte la entrada del blog de AWS Migración de cargas de trabajo a VMware Cloud en AWS con Hybrid Cloud Extension (HCX). • `DiskProvisionType (Thin, Thick)` • `UpgradeVMTools ($True, $False)` • `RemoveISOs ($True, $False)` • `ForcePowerOffVm ($True, $False)` • `RetainMac ($True, $False)` • `UpgradeHardware ($True, $False)` • `RemoveSnapshots ($True, $False)` Para obtener más información acerca de cada opción, consulte la documentación para desarrolladores de VMware.	

Ejecute el script sencillo para las pruebas iniciales

Tarea	Descripción	Habilidades requeridas
Copie el script.	La versión simple del script está contenida en un solo archivo. Puede utilizarla para probar la migración de una sola máquina. Copie el primer script de la sección Código de este patrón y guárdelo en el equipo que tiene instalado el módulo VMware PowerCLI. (Para instalar PowerCLI, siga las instrucciones de la documentación de VMware).	Arquitecto de la nube
Configure las variables del script.	Defina todas las variables en la sección del script `Manual Variables` .	Arquitecto de la nube
Establezca las variables de migración.	Establezca todos los ajustes `New-HCXMigration` en la sección del script `Migration` .	Arquitecto de la nube
Especifique los sitios.	(Opcional) Si el origen o el destino tienen varios sitios, especifique los sitios manualmente en la sección del script `Environment Setup`. Si el origen y el destino tienen sitios únicos, el script buscará	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	automáticamente la informaci ón.	
Ejecute el script.	En el servidor en el que está instalado PowerCLI, ejecute el script desde una PowerShell ventana elevada e introduzca sus credenciales cuando se le pida.	Arquitecto de la nube
Valide el script.	Confirme que se haya iniciado la migración de la máquina virtual.	Arquitecto de la nube

Ejecute el script con todas las funciones para migrar varias máquinas virtuales

Tarea	Descripción	Habilidades requeridas
Cree y complete el archivo .csv.	Cree un archivo.csv llamado `Import_VM_list.csv` en su computadora y llénelo con el siguiente contenido de muestra: `VM_NAME,DESTINATIO N_VM_FOLDER,DESTIN ATION_COMPUTE,DEST INATION_DATASTORE, SOURCE_NETWORK,DES TINATION_NETWORK [enterValue],[enter Value],[enterValue ],[enterValue],[en terValue],[enterVa lue]`	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	Sustituya cada `[enterValue]` del archivo.csv por la información que recopiló anteriormente. Nota: Puede rellenar el archivo.csv mediante VMware vRealize Network Insight (vRNI) o algún otro método.	
Copie el script.	La versión completa del script utiliza la información de un archivo.csv externo para migrar automáticamente varias máquinas virtuales. Copie el segundo script de la sección Código de este patrón y guárdelo en el equipo que tiene instalado el módulo VMware PowerCLI, en la misma carpeta que el archivo.csv.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Modifique el script.	Edite el script para realizar los siguientes cambios: • Línea 7: defina la variable de servidor HCX (`Connect-HCXServer`). • Línea 12: (opcional) Si establece el nombre de archivo.csv de forma diferente, actualícelo. • Líneas 3-4: (Opcional) Establezca el horario. • Línea 20: (opcional) Especifique la configuración `New-HCXMigration` en la sección `Migration` . • Líneas 9 y 11: (opcional) Si el origen o el destino incluyen varios sitios, especifique los sitios deseados manualmente.	Arquitecto de la nube
Ejecute el script.	En el servidor en el que está instalado PowerCLI, ejecute el script desde una PowerShell ventana elevada e introduzca sus credenciales cuando se le pida.	Arquitecto de la nube
Valide el script.	Confirme que se haya iniciado la migración de la máquina virtual.	Arquitecto de la nube

Resolución de problemas

Problema	Solución
El script falla y muestra el siguiente mensaje de error: “¡No todas las redes de origen están mapeadas al destino!”	Si la vCenter de origen usa Cross-vCenter NSX, el módulo PowerCLI no funcionará. Utilice un método de secuencias de comandos (como Python) con la API HCX en lugar de PowerCLI. Esta es una limitación conocida del script PowerCLI.
El script falla y muestra el siguiente mensaje de error: “Error de servidor Connect-HCX: no autorizado”	Las credenciales que ha introducido no proporcionan los permisos necesarios.

Recursos relacionados

- Migración de cargas de trabajo a VMware Cloud en AWS con Hybrid Cloud Extension (HCX) (entrada del blog de AWS)
- Elegir un enfoque de migración para reubicar aplicaciones y cargas de trabajo en la nube de AWS (Recomendaciones de AWS)
- Migración de VMware SDDC a VMware Cloud en AWS mediante VMware HCX (Recomendaciones de AWS)
- Introducción al módulo HCX (entrada del blog de VMware)

Migración de una carga de trabajo de F5 BIG-IP a F5 BIG-IP VE en la nube de AWS

Creado por Will Bauer (AWS)

Origen: F5 BIG-IP TMOS 13.1 y posteriores	Destino: F5 BIG-IP VE en AWS	Tipo R: volver a alojar
Entorno: producción	Tecnologías: migración ; seguridad, identidad, cumplimiento; redes	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon EC2; Amazon VPC; AWS Transit Gateway; Amazon; CloudFront Amazon; AWS Global CloudWatch Accelerator; AWS CloudFormation		

Resumen

Las organizaciones optan por migrar a la nube de Amazon Web Services (AWS) para aumentar su agilidad y resiliencia. Si migra sus soluciones de seguridad y gestión de tráfico de su F5 BIG-IP a la nube de AWS, podrá centrarse en la agilidad y adopción de modelos operativos de alto valor en toda la arquitectura de su empresa.

Este patrón describe cómo migrar una carga de trabajo de F5 BIG-IP a una carga de trabajo de F5 BIG-IP Virtual Edition (VE) en la nube de AWS. La carga de trabajo se migrará volviendo a alojar un entorno existente y utilizando aspectos de redefinición de la plataforma, como la detección de servicios y las integraciones de la API. CloudFormation Las plantillas de AWS aceleran la migración de la carga de trabajo a la nube de AWS.

Este patrón está destinado a equipos de ingeniería técnica y arquitectura que migran soluciones de gestión de tráfico y seguridad de F5, y complementa la guía Migrar de F5 BIG-IP a F5 BIG-IP VE en la nube de AWS que encontrará en Recomendaciones de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una carga de trabajo de F5 BIG-IP existente en las instalaciones.
- Licencias de F5 existentes para las versiones de BIG-IP VE.
- Una cuenta de AWS activa.
- Una nube privada virtual (VPC) existente configurada con una salida a través de una puerta de enlace NAT o una dirección IP elástica, y configurada con acceso a los siguientes puntos de enlace: Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2), AWS Security Token Service (AWS STS) y Amazon. CloudWatch También puede modificar el inicio rápido de Arquitectura de VPC modular y escalable como base de sus implementaciones.
- Una o dos zonas de disponibilidad existentes, según sus necesidades.
- Tres subredes privadas existentes en cada zona de disponibilidad.
- CloudFormation Plantillas de AWS, disponibles en el GitHub repositorio de F5.

Durante la migración, si lo necesita, puede que también deba usar:

- Una extensión de conmutación por error de F5 Cloud para gestionar el mapeo elástico de direcciones IP, el mapeo de IP secundaria y los cambios en la tabla de enrutamiento.
- Si cuenta con varias zonas de disponibilidad, necesitará usar las extensiones de conmutación por error de F5 Cloud para gestionar la asignación de IP elástica a los servidores virtuales.
- Considere la posibilidad de usar F5 Application Services 3 (AS3), F5 Application Services Templates (FAST) u otro modelo de infraestructura como código (IaC) para gestionar las configuraciones. La preparación de las configuraciones en un modelo IaC y el uso de repositorios de código le ayudarán en la migración y en las labores de gestión continuada.

Experiencia

- Este patrón requiere cierta familiaridad con la conexión de una o más VPC a centros de datos existentes. Para obtener más información sobre esto, consulte Opciones de conectividad de red a Amazon VPC en la documentación de Amazon VPC.
- También es necesaria cierta familiaridad con los productos y módulos de F5, como Traffic Management Operating System (TMOS), Local Traffic Manager (LTM), Global Traffic Manager

(GTM), Access Policy Manager (APM), Application Security Manager (ASM), Advanced Firewall Manager (AFM) y BIG-IQ.

Versiones de producto

- Le recomendamos que use F5 BIG-IP versión 13.1 o posterior, aunque el patrón es compatible con F5 BIG-IP versión 12.1 o posterior.

Arquitectura

Pila de tecnología de origen

- Carga de trabajo de F5 BIG-IP

Pila de tecnología de destino

- Amazon CloudFront
- Amazon CloudWatch
- Amazon EC2
- Amazon S3
- Amazon VPC
- AWS Global Accelerator
- AWS STS
- AWS Transit Gateway
- F5 BIG-IP VE

Arquitectura de destino

Herramientas

- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- Amazon CloudFront acelera la distribución de tu contenido web al distribuirlo a través de una red mundial de centros de datos, lo que reduce la latencia y mejora el rendimiento.

- Amazon le CloudWatch ayuda a supervisar las métricas de sus recursos de AWS y las aplicaciones que ejecuta en AWS en tiempo real.
- Amazon Elastic Compute Cloud (Amazon EC2) brinda capacidad de computación escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Security Token Service (AWS STS) le ayuda a solicitar credenciales temporales con privilegios limitados para los usuarios.
- AWS Transit Gateway es un núcleo central que conecta las nubes privadas virtuales (VPC) y las redes en las instalaciones.
- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esa red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Epics

Descubrimiento y evaluación

Tarea	Descripción	Habilidades requeridas
Evalúe el rendimiento de F5 BIG-IP.	Recopile y registre las métricas de rendimiento de las aplicaciones del servidor virtual, así como las métricas de los sistemas que se migrarán. Esto ayudará a dimensionar correctamente la infraestructura de destino de AWS para una mejor optimización de los costos.	Arquitecto de F5, ingeniero y arquitecto de redes, ingeniero
Evalúe el sistema operativo y la configuración de F5 BIG-IP.	Evalúe qué objetos se migrarán y si es necesario	Arquitecto de F5, ingeniero

Tarea	Descripción	Habilidades requeridas
	mantener una estructura de red, como VLAN.	
Evalúe las opciones de licencia de F5.	Evalúe qué licencia y modelo de consumo necesitará. Esta valoración debe basarse en su evaluación del sistema operativo y la configuración de F5 BIG-IP.	Arquitecto de F5, ingeniero
Evalúe las aplicaciones públicas.	Determine qué aplicaciones requerirán direcciones IP públicas. Alinee dichas aplicaciones con las instancias y los clústeres necesarios para cumplir con sus necesidades de rendimiento y acuerdo de nivel de servicio (SLA).	Arquitecto de F5, arquitecto de la nube, arquitecto de redes, ingeniero, equipos de aplicación
Evalúe las aplicaciones internas.	Evalúe qué aplicaciones necesitarán los usuarios internos. Asegúrese de saber dónde se encuentran esos usuarios internos en la organización, y cómo se conectan esos entornos a la nube de AWS. También debe garantizar que esas aplicaciones puedan usar el sistema de nombres de dominio (DNS) como parte del dominio predeterminado.	Arquitecto de F5, arquitecto de la nube, arquitecto de redes, ingeniero, equipos de aplicación

Tarea	Descripción	Habilidades requeridas
Finalice la AMI.	No todas las versiones de F5 BIG-IP se crean como imágenes de máquina de Amazon (AMI). Puede usar la herramienta generadora de imágenes de F5 BIG-IP si necesita versiones específicas de ingeniería de reparación rápida (QFE). Para obtener más información sobre esta herramienta, consulte la sección «Recursos relacionados».	Arquitecto de F5, arquitecto de la nube, ingeniero
Finalice los tipos de instancia y la arquitectura.	Decida los tipos de instancias, la arquitectura de VPC y la arquitectura interconectada.	Arquitecto de F5, arquitecto de la nube, arquitecto de redes, ingeniero

Complete las actividades de seguridad y cumplimiento

Tarea	Descripción	Habilidades requeridas
Documente las políticas de seguridad de F5 existentes.	Recopile y documente las políticas de seguridad existentes de F5. Asegúrese de crear una copia de las mismas en un repositorio de código seguro.	Arquitecto de F5, ingeniero
Cifre la AMI.	(Opcional) Es posible que su organización requiera el cifrado de los datos en reposo. Para obtener más información acerca de cómo crear una imagen personalizada de	Arquitecto de F5, ingeniero y arquitecto de redes, ingeniero

Tarea	Descripción	Habilidades requeridas
	tipo traiga su propia licencia (BYOL), consulte la sección “Recursos relacionados”.	
Refuerce los dispositivos.	Esto ayudará a protegerlos contra posibles vulnerabi lidades.	Arquitecto de F5, ingeniero

Configure su nuevo entorno de AWS

Tarea	Descripción	Habilidades requeridas
Cree cuentas periféricas y de seguridad.	Inicie sesión en la Consola de administración de AWS y cree las cuentas de AWS que proporcionarán y operarán los servicios de periferia y seguridad. Estas cuentas pueden ser diferentes de las que emplean las VPC para aplicaciones y servicios compartidos. Este paso se puede completar como parte de una zona de aterrizaje.	Arquitecto de la nube, ingeniero
Implemente VPC de periferia y seguridad.	Instale y configure las VPC necesarias para ofrecer servicios de periferia y seguridad.	Arquitecto de la nube, ingeniero
Conectar al centro de datos de origen.	Conéctese al centro de datos de origen que aloja su carga de trabajo de F5 BIG-IP.	Arquitecto de la nube, arquitecto de redes, ingeniero

Tarea	Descripción	Habilidades requeridas
Implemente las conexiones de VPC.	Conecte las VPC de servicios de periferia y seguridad a las VPC de aplicaciones.	Arquitecto de redes, ingeniero
Implemente las instancias.	Implemente las instancia s mediante las CloudForm ation plantillas de AWS de la sección «Recursos relaciona dos».	Arquitecto de F5, ingeniero
Pruebe y configure la conmutación por error de la instancia.	Asegúrese de que la plantilla AWS Advanced HA iAPP o la extensión de conmutación por error de F5 Cloud estén configuradas y funcionen correctamente.	Arquitecto de F5, ingeniero

Configurar redes

Tarea	Descripción	Habilidades requeridas
Prepare la topología de la VPC.	Abra la consola de Amazon VPC y asegúrese de que su VPC cuenta con todas las subredes y protecciones necesarias para la implement ación de F5 BIG-IP VE.	Arquitecto de redes, arquitect o de F5, arquitecto de la nube, ingeniero
Prepare sus puntos de conexión de VPC.	Prepare los puntos de conexión de VPC para Amazon EC2, Amazon S3 y AWS STS en caso de que una carga de trabajo de F5 BIG-IP no tenga acceso a una puerta de enlace NAT o a una	Arquitecto de la nube, ingeniero

Tarea	Descripción	Habilidades requeridas
	dirección IP elástica en una interfaz TMM.	

Migrar datos

Tarea	Descripción	Habilidades requeridas
Migre la configuración.	Migre la configuración de F5 BIG-IP a F5 BIG-IP VE en la nube de AWS.	Arquitecto de F5, ingeniero
Asocie las IP secundarias.	Las direcciones IP de los servidores virtuales tienen relación con las direcciones IP secundarias asignadas a las instancias. Asigne direcciones IP secundarias y asegúrese de seleccionar la opción “Permitir remapeo/reasignación”.	Arquitecto de F5, ingeniero

Probar la configuración

Tarea	Descripción	Habilidades requeridas
Valide las configuraciones del servidor virtual.	Pruebe los servidores virtuales .	Arquitecto de F5, equipos de aplicación

Finalice las operaciones

Tarea	Descripción	Habilidades requeridas
Cree la estrategia de respaldo.	Los sistemas deben estar apagados para crear una instantánea completa. Para obtener más información, consulte “Actualizar una máquina virtual F5 BIG-IP” en la sección “Recursos relaciona dos”.	Arquitecto de F5, arquitecto de la nube, ingeniero
Cree el manual de procedimi entos de conmutación por error del clúster.	Asegúrese de que el proceso del manual de procedimientos de conmutación por error esté completo.	Arquitecto de F5, ingeniero
Configure y valide el registro.	Configure la transmisión por telemetría de F5 para enviar los registros a los destinos requeridos.	Arquitecto de F5, ingeniero

Complete la transición

Tarea	Descripción	Habilidades requeridas
Transicione a la nueva implementación.		Arquitecto de F5, arquitecto de nube, arquitecto de redes, ingeniero, AppTeams

Recursos relacionados

Guía de migración

- Migración de F5 BIG-IP a F5 BIG-IP VE en la nube de AWS

Recursos de F5

- CloudFormation Plantillas de AWS en el repositorio de F5 GitHub
- F5 en AWS Marketplace
- Descripción general de F5 BIG-IP VE
- Ejemplo de inicio rápido: BIG-IP Virtual Edition con WAF (LTM + ASM)
- Servicios de aplicaciones de F5 en AWS: información general (video)
- Guía del usuario para la extensión Application Services 3 de F5
- Documentación de F5 Cloud
- iControl REST de F5 wiki
- Descripción general de los archivos de configuración individuales (11.x - 15.x) de F5
- Laboratorio de topología de F5
- Documentos técnicos de F5
- Herramienta generadora de imágenes de F5 BIG-IP
- Actualizar una máquina virtual F5 BIG-IP VE
- Descripción general de la opción de «migración de plataforma» de UCS archive

Migración de una aplicación web Go en las instalaciones a AWS Elastic Beanstalk mediante el método binario

Creado por Suhas Basavaraj (AWS) y Shumaz Mukhtar Kazi (AWS)

Entorno: PoC o piloto	Origen: aplicaciones	Destino: elastic Beanstalk
Tipo R: volver a alojar	Tecnologías: migración; aplicaciones web y móviles	Servicios de AWS: AWS Elastic Beanstalk

Resumen

En este patrón se describe cómo migrar una aplicación web Go en las instalaciones a AWS Elastic Beanstalk. Después de migrar la aplicación, Elastic Beanstalk crea el binario para la agrupación de código fuente y lo implementa en una instancia de Amazon Elastic Compute Cloud (Amazon EC2).

Como estrategia de migración para volver a alojar, el enfoque de este patrón es rápido y no requiere cambios de código, lo que se traduce en menos tiempo de pruebas y migración.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una aplicación web Go en las instalaciones.
- Un GitHub repositorio que contiene el código fuente de la aplicación Go. Si no lo usa GitHub, hay otras formas de crear un paquete de código fuente de aplicación para Elastic Beanstalk.

Versiones de producto

- La versión de Go más reciente compatible con Elastic Beanstalk. Para obtener más información, consulte la documentación de Elastic Beanstalk.

Arquitectura

Pila de tecnología de origen

- Una aplicación web Go en las instalaciones

Pila de tecnología de destino

- AWS Elastic Beanstalk
- Amazon CloudWatch

Arquitectura de destino

Herramientas

- AWS Elastic Beanstalk permite implementar y administrar aplicaciones rápidamente en la nube de AWS sin tener que los usuarios tengan que preocuparse por la infraestructura que las ejecuta. Elastic Beanstalk reduce la complejidad de la administración sin restringir la libertad de elección ni el control.
- GitHubes un sistema de control de versiones distribuido de código abierto.

Epics

Crear el archivo .zip de la agrupación de código fuente de la aplicación web Go

Tarea	Descripción	Habilidades requeridas
Cree la agrupación de código fuente de la aplicación web Go.	Abre el GitHub repositorio que contiene el código fuente de tu aplicación Go y prepara el paquete fuente. La agrupació n de código fuente contiene un archivo `application.go` de origen en el directorio raíz, que aloja el paquete principal de la aplicación Go. Si no lo utilizas GitHub, consulta la sección de requisitos previos que aparece anteriormente	Administrador del sistema, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	en este patrón para ver otras formas de crear el paquete fuente de la aplicación.	
Cree un archivo de configuración.	Cree una carpeta `.ebextensions` en la agrupación de código fuente y, a continuación, cree un archivo `options.config` dentro de esta carpeta. Para obtener más información, consulte la documentación de Elastic Beanstalk.	Administrador del sistema, desarrollador de aplicaciones
Cree el archivo .zip de la agrupación de código fuente.	Ejecute el siguiente comando de la . `git archive -o ../godemoapp.zip HEAD` Esto crea el archivo .zip de la agrupación de código fuente. Descargue y guarde el archivo .zip como un archivo local. Importante: El archivo .zip no puede superar los 512 MB y no puede incluir una carpeta principal ni un directorio de nivel superior.	Administrador del sistema, desarrollador de aplicaciones

Migración de la aplicación web Go a Elastic Beanstalk

Tarea	Descripción	Habilidades requeridas
Seleccione la aplicación de Elastic Beanstalk.	1. Inicie sesión en la consola de administración de AWS y abra la consola de Elastic Beanstalk. 2. En la lista Regions, seleccione su región de AWS. 3. En el panel de navegación, seleccione Applications y, a continuación, seleccione una aplicación de Elastic Beanstalk existente o cree una. Para obtener instrucciones sobre cómo crear una aplicación de Elastic Beanstalk, consulte la documentación de Elastic Beanstalk.	Administrador del sistema, desarrollador de aplicaciones
Inicie el entorno del servidor web de Elastic Beanstalk.	1. En la página de descripción general de la aplicación, seleccione Create a new environment (Crear un nuevo entorno) y, a continuación, Web server environment (Entorno de servidor web). 2. Complete los campos Environment name (Nombre del entorno) y	Administrador del sistema, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	Domain name (Nombre de dominio). 3. Seleccione Platform version (Versión de la plataform a) y seleccione Go como plataforma.	
Cargue el archivo .zip de la agrupación de código fuente en Elastic Beanstalk.	1. En Application code (Código de la aplicación), seleccione Upload your code (Cargar el código) y, a continuación, Upload. 2. Seleccione el archivo .zip que contiene la agrupación de código fuente. 3. En Version label, asigne un nombre exclusivo al archivo y, a continuación, seleccion e Create environment (Crear entorno).	Administrador del sistema, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Pruebe la aplicación web Go implementada.	Se le redirigirá a la página de información general de la aplicación Elastic Beanstalk . En la parte superior de la descripción general, junto a Environment ID, seleccione la URL que termina en `elasticbeanstalk.com` para navegar hasta la aplicación. La aplicación debe usar este nombre en su archivo de configuración como variable de entorno y mostrarlo en la página web.	Administrador del sistema, desarrollador de aplicaciones

Solución de problemas

Problema	Solución
No se puede acceder a la aplicación a través de un equilibrador de carga de aplicación.	Compruebe el grupo de destino que contiene su aplicación de Elastic Beanstalk. Si no está en buen estado, inicie sesión en la instancia de Elastic Beanstalk y compruebe la configuración del archivo `nginx.conf` para asegurar que se dirija a la URL de estado correcta. Es posible que tenga que cambiar la URL de la comprobación de estado del grupo objetivo.

Recursos relacionados

- Go platform versions supported by Elastic Beanstalk (Versiones de la plataforma Go compatibles con Elastic Beanstalk)

- Using configuration files with Elastic Beanstalk (Usar archivos de configuración con Elastic Beanstalk)
- Creating an example application in Elastic Beanstalk (Crear una aplicación de ejemplo en Elastic Beanstalk)

Migración de un servidor SFTP en las instalaciones a AWS mediante AWS Transfer para SFTP

Creado por Akash Kumar (AWS)

Entorno: producción	Origen: almacenamiento	Destino: Amazon S3
Tipo R: volver a alojar	Tecnologías: migración; almacenamiento y respaldo; aplicaciones web y móviles	Servicios de AWS: Amazon S3; AWS Transfer Family; Amazon CloudWatch Logs

Resumen

Este patrón describe cómo migrar una solución de transferencia de archivos en las instalaciones que utiliza el protocolo de transferencia de archivos (SFTP) Secure Shell (SSH) a la nube de Amazon Web Services (AWS) mediante el servicio AWS Transfer para SFTP. Por lo general, los usuarios se conectan a un servidor SFTP a través de su nombre de dominio o mediante una IP fija. Este patrón cubre ambos casos.

AWS Transfer para SFTP forma parte de AWS Transfer Family. Es un servicio de transferencia segura que le permite transferir archivos dentro y fuera de los servicios de almacenamiento mediante SFTP. Puede utilizar AWS Transfer para SFTP con Amazon Simple Storage Service (Amazon S3) o Amazon Elastic File System (Amazon EFS). Este patrón utiliza Amazon S3 para el almacenamiento.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Un nombre de dominio SFTP existente o una IP SFTP fija.

Limitaciones

- El objeto más grande que se puede transferir en una solicitud es de 5 GiB actualmente. Para archivos de más de 100 MiB, considere la posibilidad de utilizar la carga multiparte de Amazon S3.

Arquitectura

Pila de tecnología de origen

- Archivos planos en las instalaciones o archivos de volcado de bases de datos.

Pila de tecnología de destino

- AWS Transfer for SFTP
- Amazon S3
- Amazon Virtual Private Cloud (Amazon VPC)
- Roles y políticas de AWS Identity and Access Management (IAM)
- Direcciones IP elásticas
- Grupos de seguridad
- Amazon CloudWatch Logs (opcional)

Arquitectura de destino

Automatizar y escalar

Para automatizar la arquitectura de destino de este patrón, utilice las CloudFormation plantillas de AWS adjuntas:

- `amazon-vpc-subnets.yml` aprovisiona una nube privada virtual (VPC) con dos subredes públicas y dos privadas.
- `amazon-sftp-server.yml` aprovisiona el servidor SFTP.
- `amazon-sftp-customer.yml` añade usuarios.

Herramientas

Servicios de AWS

- Amazon CloudWatch Logs le ayuda a centralizar los registros de todos sus sistemas, aplicaciones y servicios de AWS para que pueda supervisarlos y archivarlos de forma segura.

- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos. Este patrón utiliza Amazon S3 como sistema de almacenamiento para las transferencias de archivos.
- AWS Transfer para SFTP le ayuda a transferir archivos dentro y fuera de los servicios de almacenamiento de AWS a través del protocolo SFTP.
- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esta red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Epics

Creación de una VPC

Tarea	Descripción	Habilidades requeridas
Cree una VPC con dos subredes.	Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/. Cree una nube privada virtual (VPC) con dos subredes públicas. (La segunda subred proporciona alta disponibilidad). —o— Puede implementar la CloudFormation plantilla adjunta en la CloudFormation consola para automatizar las tareas de esta epopeya. `amazon-vpc-subnets.yml`	Desarrollador, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Añada una puerta de enlace de Internet.	Cree una puerta de enlace de Internet y vincúlela a la VPC.	Desarrollador, administrador de sistemas
Migre una IP existente.	Adjunte una IP existente a la dirección IP elástica. Puede crear una dirección IP elástica a partir de su grupo de direcciones y utilizarla.	Desarrollador, administrador de sistemas

Aprovisionar un servidor SFTP

Tarea	Descripción	Habilidades requeridas
Cree un servidor SFTP.	Abra la consola de AWS Transfer Family en https://console.aws.amazon.com/transfer/. Siga las instrucciones en Cree un punto de conexión con acceso a Internet para su servidor en la documentación de AWS Transfer Family para crear un servidor SFTP con un punto de conexión accesible desde Internet. En Tipo de punto de enlace, seleccione Alojado en la VPC. En Acceso, seleccione Acceso a Internet. En VPC, seleccione la VPC que acaba de crear en los pasos anteriores. —o— Puedes implementar la CloudFormation plantilla	Desarrollador, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	adjunta en la CloudFormation consola para automatizar las tareas de esta epopeya. `amazon-sftp-server.yml`	
Migre el nombre del dominio.	Adjunte el nombre de dominio existente al nombre de host personalizado. Si utiliza un nombre de dominio nuevo, utilice el alias DNS de Amazon Route 53. Para un nombre de dominio existente, seleccione Otros DNS. Para obtener más información, consulte Working with custom hostnames en la documentación de AWS Transfer Family.	Desarrollador, administrador de sistemas
Agrega una función de CloudWatch registro.	(Opcional) Si quieres habilitar el CloudWatch registro, crea un `Transfer` rol con las operaciones de la API de CloudWatch registros `logs:CreateLogGroup logs:CreateLogStream` , `logs:DescribeLogStreams` , `ylogs:PutLogEvents` . Para obtener más información, consulte Registrar la actividad CloudWatch en la documentación de AWS Transfer Family.	Desarrollador, administrador del sistema

Tarea	Descripción	Habilidades requeridas
Guarde y envíe.	Seleccione Guardar. En Acciones, seleccione Iniciar y espere a que se cree el servidor SFTP con el estado En línea.	Desarrollador, administrador de sistemas

Asignar direcciones IP elásticas al servidor SFTP

Tarea	Descripción	Habilidades requeridas
Detenga el servidor para poder modificar la configuración.	En la Consola de AWS Transfer Family, seleccione Servidores y, a continuación, seleccione el servidor SFTP que creó. En Acciones, seleccione Detener. Cuando el servidor esté desconectado, seleccione Editar para modificar su configuración.	Desarrollador, administrador del sistema
Seleccione zonas de disponibilidad y subredes.	En la sección Zonas de disponibilidad, seleccione las zonas de disponibilidad y subredes para su VPC.	Desarrollador, administrador de sistemas
Agregue direcciones IP elásticas.	En Direcciones IPv4, seleccione una dirección IP elástica para cada subred y, a continuación, seleccione Guardar.	Desarrollador, administrador de sistemas

Agregar usuarios

Tarea	Descripción	Habilidades requeridas
Cree un rol de IAM para que los usuarios accedan al bucket de S3.	Cree un rol de IAM para `Transfer` y añada `s3:ListBucket`, `s3:GetBucketLocation` y `s3:PutObject` con el nombre del bucket de S3 como recurso. Para obtener más información, consulte Crear un rol y política de IAM en la documentación de AWS Transfer Family. —o— Puede implementar la CloudFormation plantilla adjunta en la CloudFormation consola para automatizar las tareas de esta epopeya. `amazon-sftp-customer.yml`	Desarrollador, administrador de sistemas
Cree un bucket de S3.	Cree un bucket de S3 para la aplicación.	Desarrollador, administrador de sistemas
Cree una carpeta opcional.	(Opcional) Si desea almacenar los archivos de los usuarios por separado, en carpetas específicas de Amazon S3, añada carpetas según corresponda.	Desarrollador, administrador de sistemas
Cree una clave pública SSH.	Para crear un par de claves SSH, consulte Generar claves	Desarrollador, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	SSH en la documentación de AWS Transfer Family.	
Agregue usuarios.	En la Consola de AWS Transfer Family, seleccione Servidores, seleccione el servidor SFTP que creó y, a continuación, seleccione Añadir un usuario. En el Directorio principal, seleccione el bucket de S3 que creó. En Clave pública SSH, escriba el componente de clave pública del par de claves de SSH. Añada usuarios al servidor SFTP y, a continuación, seleccione Añadir.	Desarrollador, administrador de sistemas

Probar el servidor SFTP

Tarea	Descripción	Habilidades requeridas
Actualice el grupo de seguridad.	En la sección Grupos de seguridad de su servidor SFTP, añada la IP de su máquina de prueba para obtener acceso a SFTP.	Desarrollador
Utilice una utilidad de cliente SFTP para probar el servidor.	Pruebe las transferencias de archivos mediante cualquier utilidad de cliente SFTP. Para obtener una lista de clientes e instrucciones, consulte Transferir archivos mediante	Desarrollador

Tarea	Descripción	Habilidades requeridas
	un cliente en la documentación de AWS Transfer Family.	

Recursos relacionados

- AWS Transfer Family User Guide
- Guía del usuario de Amazon S3
- Direcciones IP elásticas en la documentación de Amazon EC2

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Migre una máquina virtual en las instalaciones a Amazon EC2 mediante el Servicio de migración de aplicaciones de AWS

Creado por Thanh Nguyen (AWS)

Entorno: producción	Origen: máquina virtual en las instalaciones	Destino: Amazon EC2
Tipo R: volver a alojar	Tecnologías: migración	Servicios de AWS: servicio de migración de aplicaciones de AWS; Amazon EC2; Amazon EBS

Resumen

En lo que respecta a la migración de aplicaciones, las organizaciones pueden adoptar diferentes enfoques para volver a alojar (migrar mediante lift-and-shift) los servidores de las aplicaciones del entorno local a la nube de Amazon Web Services (AWS). Una forma de hacerlo es aprovisionar nuevas instancias de Amazon Elastic Compute Cloud (Amazon EC2) y, a continuación, instalar y configurar la aplicación desde cero. Otro enfoque consiste en utilizar servicios de migración nativos de AWS o de terceros para migrar varios servidores al mismo tiempo.

Este patrón describe los pasos para migrar una máquina virtual (VM) compatible a una instancia de Amazon EC2 en la nube de AWS mediante el Servicio de migración de aplicaciones de AWS. Puede utilizar el enfoque de este patrón para migrar una o varias máquinas virtuales de forma manual, una por una o automáticamente mediante la creación de los scripts de automatización adecuados en función de los pasos descritos.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa en una de las regiones de AWS que admiten el Servicio de migración de aplicaciones
- Conectividad de red entre el servidor de origen y el servidor EC2 de destino a través de una red privada mediante AWS Direct Connect o una red privada virtual (VPN), o a través de Internet

Limitaciones

- Para obtener la lista más reciente de regiones admitidas, consulte las regiones de AWS admitidas.
- Para obtener una lista de los sistemas operativos compatibles, consulte la sección Sistemas operativos compatibles y la sección General de las preguntas frecuentes de Amazon EC2.

Arquitectura

Pila de tecnología de origen

- Un servidor físico, virtual o alojado en la nube que ejecute un sistema operativo compatible con Amazon EC2

Pila de tecnología de destino

- Una instancia de Amazon EC2 que ejecute el mismo sistema operativo que la máquina virtual de origen
- Amazon Elastic Block Store (Amazon EBS)

Arquitectura de origen y destino

El siguiente diagrama muestra la arquitectura de alto nivel y los componentes principales de la solución. En el centro de datos en las instalaciones, hay máquinas virtuales con discos locales. En AWS, hay un área de ensayo con servidores de replicación y un área de recursos migrados con instancias EC2 para realizar pruebas y transiciones. Ambas subredes contienen volúmenes de EBS.

1. Inicie el Servicio de migración de aplicaciones de AWS.
2. Configure la configuración y los informes del servidor del área de ensayo, incluidos los recursos del área de ensayo.
3. Instale los agentes en los servidores de origen y utilice la replicación continua de datos a nivel de bloques (comprimidos y cifrados).
4. Automatice la orquestación y la conversión del sistema para acortar el período de transición.

Arquitectura de redes

El siguiente diagrama muestra la arquitectura de alto nivel y los componentes principales de la solución desde la perspectiva de las redes, incluidos los protocolos y puertos necesarios para la comunicación entre los componentes principales del centro de datos en las instalaciones y de AWS.

Herramientas

- El Servicio de migración de aplicaciones de AWS le ayuda a volver a alojar (migrar mediante lift-and-shift) aplicaciones a la nube de AWS sin cambios y con un tiempo de inactividad mínimo.

Prácticas recomendadas

- No desconecte el servidor de origen ni lo reinicie hasta que se complete la transición a la instancia EC2 de destino.
- Ofrezca a los usuarios amplias oportunidades de realizar pruebas de aceptación del usuario (UAT) en el servidor de destino para identificar y resolver cualquier problema. Lo ideal es que estas pruebas comiencen al menos dos semanas antes de la transición.
- Supervise con frecuencia el estado de replicación del servidor en la consola del Servicio de migración de aplicaciones para identificar los problemas desde el principio.
- Utilice las credenciales de AWS Identity and Access Management (IAM) temporales para instalar el agente en lugar de las credenciales de usuario de IAM permanentes.

Epics

Generar credenciales de AWS

Tarea	Descripción	Habilidades requeridas
Cree el rol de IAM de AWS Replication Agent.	Inicie sesión en la cuenta de AWS con permisos administrativos. Cree un rol de IAM en la consola de AWS Identity and Access Management (IAM):	Administrador de AWS, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	1. En la consola de IAM, seleccione Roles. 2. Elija Create role (Crear rol). 3. En la página Seleccionar una entidad de confianza, en la sección Tipo de entidad de confianza, seleccione Cuenta de AWS. 4. En la sección Una cuenta de AWS, seleccione Esta cuenta (< account-id>). 5. Elija Siguiente. 6. En la página Add permissions (Añadir permisos), busque la política `AWSApplicationMigrationAgentInstallationPolicy`, seleccione la casilla de verificación situada junto al nombre de la política. 7. Elija Siguiente. 8. En la página de Role details (Detalles del rol), introduzca MGN_Agent_Installation_Role como nombre del rol. 9. Compruebe que los campos son correctos y, a continuación, seleccione Create rol (Crear rol).	

Tarea	Descripción	Habilidades requeridas
Genere credenciales de seguridad temporales.	En una máquina con la Interfaz de la línea de comandos de AWS (AWS CLI) instalada, inicie sesión con permisos de administrador. O bien (dentro de una región de AWS compatible), en la consola de administración de AWS, inicie sesión con permisos administrativos en la cuenta de AWS y abra AWS CloudShell. Genere credenciales temporales con el siguiente comando y sustitúyalas por `<account-id>` con el ID de la cuenta de AWS. `aws sts assume-role --role-arn arn:aws:iam::<account-id>:role/MGN_Agent_Installation_Role --role-session-name mgn_installation_session_role` En el resultado del comando, copie los valores de `AccessKeyId`, `SecretAccessKey`, y `SessionToken`. Guárdelos en un lugar seguro para usarlos más adelante.	Administrador de AWS, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	Importante: estas credencia les temporales caducarán después de una hora. Si necesita las credenciales después de una hora, repita los pasos anteriores.	

Inicie el Servicio de migración de aplicaciones y cree la plantilla de configuración de replicación

Tarea	Descripción	Habilidades requeridas
Inicie el servicio.	Inicie sesión en la consola con permisos administrativos para la cuenta de AWS. Elija Application Migration Service (Servicio de migración de aplicaciones) y, a continuac ión, elija Get started (Introduc ción).	Administrador de AWS, ingeniero de migraciones
Cree y configure la plantilla de ajustes de replicación.	1. Proporcione los siguientes detalles de configuración: a. Seleccione la subred del área de ensayo. b. Seleccione el tipo de instancia del servidor de replicación (`t3.small` por defecto). c. Seleccione el tipo de volumen de EBS (gp3 por defecto). d. Seleccione la opción de cifrado de EBS.	Administrador de AWS, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	e. Asegúrese de que la casilla Usar siempre el grupo de seguridad del Servicio de migración de aplicaciones esté seleccionada. f. Seleccione la casilla Usar IP privada para la replicación de datos (VPN DirectConnect, interconexión de VPC) si utiliza una conectividad de red privada entre el entorno local y AWS. g. Seleccione la casilla Reducir el ancho de banda de la red (por servidor, en Mbps) si desea limitar el ancho de banda de la red para el Servicio de migración de aplicaciones. 2. Seleccione Crear plantilla. El Servicio de aplicación de migraciones creará automátic amente todos los roles de IAM necesarios para facilitar la replicación de datos y el lanzamiento de los servidores migrados.	

Instale los agentes de replicación de AWS en las máquinas de origen

Tarea	Descripción	Habilidades requeridas
Tenga preparadas las credenciales de AWS necesarias.	Cuando ejecute el archivo de instalación en un servidor de origen, tendrá que introducir las credenciales temporales que generó anteriormente, incluidas `AccessKeyId` , `SecretAccessKey` , y `SessionToken` .	Ingeniero de migraciones; administrador de AWS
Para los servidores de Linux, instale el agente.	Copie el comando del instalador, inicie sesión en los servidores de origen y ejecute el instalador. Para obtener instrucciones detalladas, consulte la documentación de AWS.	Administrador de AWS, ingeniero de migraciones
Para los servidores de Windows, instale el agente.	Descargue el archivo del instalador en cada servidor y, a continuación, ejecute el comando del instalador. Para obtener instrucciones detalladas, consulte la documentación de AWS.	Administrador de AWS, ingeniero de migraciones
Espere a que se complete la replicación inicial de los datos.	Cuando se haya instalado el agente, el servidor de origen aparecerá en la consola del Servidor de migración de aplciaciones, en la sección Servidores de origen. Espere a que el servidor realice la replicación inicial de los datos.	Administrador de AWS, ingeniero de migraciones

Configure los ajustes de lanzamiento

Tarea	Descripción	Habilidades requeridas
Especifique los detalles del servidor.	En la consola del Servicio de migración de aplicaciones, elija la sección Servidores de origen y, a continuación, elija un nombre de servidor de la lista para acceder a los detalles del servidor.	Administrador de AWS, ingeniero de migraciones
Configure los ajustes de lanzamiento.	Seleccione la pestaña ajustes de lanzamiento. Puede configurar una variedad de ajustes, incluidos los ajustes generales de lanzamiento y los ajustes de la plantilla de lanzamiento de EC2. Para obtener instrucciones detalladas, consulte la documentación de AWS.	Administrador de AWS, ingeniero de migraciones

Realice una prueba

Tarea	Descripción	Habilidades requeridas
Pruebe los servidores de origen.	1. En la consola del Servicio de migración de aplicaciones, en la sección Servidores de origen, asegúrese de que el ciclo de vida de migración de los servidores de origen esté preparado para las pruebas y de que el estado de la	Administrador de AWS, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	replicación de los datos sea correcto. 2. Marque la casilla situada a la izquierda de cada servidor de origen. 3. Elija Test and Cutover (Prueba y transición) y, a continuación, elija Launch Test Instance (Lanzar instancia de prueba). 4. Cuando se le pregunte, elija Launch (Lanzar). Se lanzarán los servidores.	
Compruebe que la prueba se haya completado correctam ente.	Una vez que el servidor de prueba se haya iniciado por completo, el estado de las alertas de la página mostrará Lanzado para cada servidor.	Administrador de AWS, ingeniero de migraciones
Pruebe el servidor.	Realice pruebas con el servidor de prueba para asegurarse de que funciona según lo esperado.	Administrador de AWS, ingeniero de migraciones

Programe y realice una transición

Tarea	Descripción	Habilidades requeridas
Programe una transición temporal.	Programe un período de transición adecuado con los equipos pertinentes.	Administrador de AWS, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
Lleve a cabo la transición.	1. En la consola de migración de aplicaciones, en la página Servidores de origen, active la casilla de verificación situada a la izquierda de cada servidor de origen. 2. Elija Test and Cutover (Prueba y transición) y seleccione Mark as “Ready for cutover” (Marcar como “Listo para la transición”). 3. Compruebe que el ciclo de vida de migración de cada servidor de origen esté preparado para la transició n. 4. Elija Test and Cutover (Prueba y transición) y, a continuación, elija Launch cutover instances (Lanzar instancias de transición). 5. Cuando se le pregunte, elija Launch (Lanzar). Se lanzarán los servidores. El ciclo de vida de la migración del servidor de origen pasará a transición en curso.	Administrador de AWS, ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
Compruebe que la transición se haya completado correctamente.	Una vez que los servidores de transición se hayan iniciado por completo, el estado de las Alertas en los Servidores de origen de la página mostrarán Lanzado para cada servidor.	Administrador de AWS, ingeniero de migraciones
Pruebe el servidor.	Realice pruebas con el servidor de transición para asegurarse de que funciona según lo esperado.	Administrador de AWS, ingeniero de migraciones
Finalice la transición.	Elija Test and Cutover (Prueba y transición) y, a continuación, seleccione Finalize cutover (Finalizar la transición) para finalizar el proceso de migración.	Administrador de AWS, ingeniero de migraciones

Recursos relacionados

- AWS Application Migration Service
- Guía de usuario del Servicio de migración de aplicaciones de AWS

Migración de pequeños conjuntos de datos de las instalaciones a Amazon S3 mediante AWS SFTP

Tipo R: volver a alojar	Origen: almacenamiento	Destino: Amazon S3
Creado por: AWS	Entorno: producción	Tecnologías: almacenamiento y copia de seguridad; migración
Servicios de AWS: Amazon S3		

Resumen

Este patrón describe cómo migrar pequeños conjuntos de datos (5 TB o menos) de centros de datos locales a Amazon Simple Storage Service (Amazon S3) mediante AWS Transfer for SFTP (AWS SFTP). Los datos pueden ser volcados de bases de datos o archivos planos.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un enlace de AWS Direct Connect establecido entre su centro de datos y AWS

Limitaciones

- Los archivos de datos deben tener menos de 5 TB. Para archivos de más de 5 TB, puede realizar una carga multiparte a Amazon S3 o elegir otro método de transferencia de datos.

Arquitectura

Pila de tecnología de origen

- Archivos planos en las instalaciones o volcados de bases de datos locales

Pila de tecnología de destino

- Amazon S3

Arquitectura de origen y destino

Herramientas

- AWS SFTP: permite la transferencia de archivos directamente hacia y desde Amazon S3 mediante el Protocolo seguro de transferencia de archivos (SFTP).
- AWS Direct Connect: establece una conexión de red dedicada desde sus centros de datos locales a AWS.
- Puntos de enlace de VPC: le permiten conectar de forma privada una VPC a los servicios de AWS compatibles y a los servicios de puntos finales de VPC con tecnología de PrivateLink AWS sin una puerta de enlace a Internet, un dispositivo de traducción de direcciones de red (NAT), una conexión VPN o una conexión AWS Direct Connect. Las instancias en una VPC no necesitan direcciones IP públicas para comunicarse con los recursos del servicio.

Epics

Preparación para la migración

Tarea	Descripción	Habilidades requeridas
Documente los requisitos actuales de SFTP.		Propietario de la aplicación, SA
Identifique los requisitos de autenticación.	Los requisitos pueden incluir la autenticación basada en claves, el nombre de usuario o la contraseña o el proveedor de identidades (IdP).	Propietario de la aplicación, SA
Identifique los requisitos de integración de la aplicación.		Propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Identifique a los usuarios que requieren el servicio.		Propietario de la aplicación
Determine el nombre DNS del punto de conexión del servidor SFTP.		Red
Determinar la estrategia de copia de seguridad.		SA, Administrador de base de datos (si se transfieren datos)
Identifique la estrategia de migración o transición de la aplicación.		Propietario de la aplicación, SA, Administrador de base de datos

Configuración de la infraestructura

Tarea	Descripción	Habilidades requeridas
Crear una o más nubes privadas virtuales (VPC) y subredes en la cuenta de AWS.		Propietario de la aplicación, AMS
Crear grupos de seguridad y listas de control de acceso a la red (ACL).		Seguridad, redes, AMS
Cree el bucket de S3.		Propietario de la aplicación, AMS
Cree el rol de Identity and Access Management (IAM).	Una política de IAM que incluya los permisos para que tenga acceso al bucket de S3. Esta política de IAM determina el nivel de acceso que otorga a los usuarios de SFTP. Cree	Seguridad, AMS

Tarea	Descripción	Habilidades requeridas
	otra política de IAM para establecer una relación de confianza con AWS SFTP.	
Asocia un dominio registrado (opcional).	Si tiene su propio dominio registrado, puede asociarlo al servidor SFTP. Puede enrutar el tráfico SFTP al punto de conexión de su servidor SFTP desde un dominio o desde un subdominio.	Redes, AMS
Cree un servidor SFTP.	Especifique el tipo del proveedor de identidad que el servicio debe usar para autenticar a los usuarios.	Propietario de la aplicación, AMS
Abrir un cliente SFTP.	Abra un cliente SFTP y configure la conexión para que use el nombre de host del punto de conexión de SFTP correspondiente al host. AWS SFTP es compatible con cualquier cliente SFTP estándar. Los clientes SFTP más utilizados incluyen OpenSSH, WinSCP, Cyberduck y. FileZilla Puede obtener el nombre de host del servidor SFTP en la consola SFTP de AWS.	Propietario de la aplicación, AMS

Planificar y probar

Tarea	Descripción	Habilidades requeridas
Planifique la migración de la aplicación.	Planifique los cambios necesarios en la configuración de la aplicación, establezc a la fecha de migración y determine el programa de pruebas.	Propietario de la aplicación, AMS
Pruebe la infraestructura.	Realice pruebas en un entorno que no sea de producción.	Propietario de la aplicación, AMS

Recursos relacionados

Referencias

- Guía del usuario de AWS Transfer para SFTP
- Recursos de AWS Direct Connect
- Puntos de enlace de la VPC

Tutoriales y videos

- AWS Transfer para SFTP (video)
- Guía del usuario de AWS Transfer para SFTP
- Pizarra blanca sobre AWS SA: Direct Connect (video)

Migre de Oracle GlassFish a AWS Elastic Beanstalk

Tipo R: volver a alojar	Origen: desarrollo de aplicaciones	Destino: AWS Elastic Beanstalk
Creado por: AWS	Entorno: PoC o piloto	Tecnologías: contenedores y microservicios; aplicaciones web y móviles; migración
Carga de trabajo: código abierto; Oracle	Servicios de AWS: AWS Elastic Beanstalk	

Resumen

Este patrón describe cómo migrar una aplicación Java que se ejecuta en un GlassFish servidor Oracle local a AWS Elastic Beanstalk en la nube de AWS.

En AWS, la aplicación Java se implementa en un GlassFish servidor Docker con AWS Elastic Beanstalk, que se ejecuta en un grupo de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) Auto Scaling.

Características adicionales:

- Amazon Elastic Beanstalk actúa como contenedor de varios recursos subyacentes. Configura el equilibrador de carga elástico (que gestiona el tráfico entrante de Amazon Route 53), dispersa el tráfico en una o más instancias de EC2 y también sirve como herramienta de implementación.
- Para migrar una base de datos en las instalaciones a Amazon Relational Database Service (Amazon RDS), actualice los detalles de conexión a la base de datos. En la base de datos de backend, puede configurar las implementaciones Multi-AZ de Amazon RDS y elegir el tipo de motor de base de datos.
- Puede usar la Implementación multi-AZ para una alta disponibilidad junto con el grupo de escalado automático y la política de escalado para mejorar la resiliencia.
- Puedes configurar una política de escalado basada en CloudWatch las métricas de Amazon.
- En AWS Elastic Beanstalk, puede configurar los ajustes subyacentes de Elastic Load Balancing y Amazon EC2 Auto Scaling.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una aplicación Java local que se ejecuta en GlassFish
- Un archivo de recursos de aplicaciones web (WAR) de Java

Versiones de producto

- Oracle Glassfish 4.1.2 y 5.0
- Java 7 4.0 GlassFish
- Java 8 GlassFish 4.1 o posterior

Arquitectura

Pila de tecnología de origen

- Aplicaciones desarrolladas en GlassFish

Pila de tecnología de destino

- Elastic Beanstalk

Arquitectura de destino

Flujo de trabajo de una implementación

Herramientas

- Amazon Elastic Beanstalk es un servicio para implementar y escalar servicios y aplicaciones web desarrollados con Java, .NET, PHP, Node.js, Python, Ruby, Go y Docker en servidores conocidos, como, por ejemplo, Apache, NGINX, Passenger e IIS.

- Amazon CloudWatch: proporciona datos e información procesable para monitorear las aplicaciones, responde a los cambios de rendimiento en todo el sistema, optimiza la utilización de los recursos y proporciona una visión unificada del estado operativo.
- Docker: una plataforma que empaqueta el software en unidades estandarizadas para crear, probar e implementar aplicaciones rápidamente.
- Java: un lenguaje de programación de uso general. Java está basado en clases, orientado a objetos y diseñado para tener menos dependencias de implementación.

Epics

Configurar una VPC

Tarea	Descripción	Habilidades requeridas
Cree una instancia de nube privada virtual (VPC) con la información necesaria.		SysAdmin
Cree al menos dos subredes en la VPC.		SysAdmin
Cree una tabla de enrutamie nto según los requisitos.		SysAdmin

Configuración de Amazon S3

Tarea	Descripción	Habilidades requeridas
Cree un bucket de Amazon Simple Storage Service (Amazon S3).		SysAdmin
Copie el archivo WAR en el bucket de S3 y suba el código de la aplicación.		SysAdmin

Creación de un rol de IAM

Tarea	Descripción	Habilidades requeridas
Cree un rol de IAM de AWS Identity and Access Management.	Puede usar el perfil predeterminado «aws-elasticbeanstalk-ec2-role» o dejar que Elastic Beanstalk lo cree automáticamente.	SysAdmin

Configurar Elastic Beanstalk

Tarea	Descripción	Habilidades requeridas
Abra el panel de Elastic Beanstalk.		SysAdmin
Cree una nueva aplicación y seleccione el nuevo entorno de servidor web.		SysAdmin
Elija GlassFish Docker como plataforma preconfigurada.		SysAdmin
Suba el código.	Proporcione la URL del archivo de bucket de S3 o el archivo ZIP de los archivos del sistema local.	SysAdmin
Elija el tipo de entorno.	En los ajustes de capacidad de configuración, elija Instancia única o Equilibrador de carga.	SysAdmin
Configuración del equilibrador de carga.	Si eligió equilibrador de carga en el paso anterior, configure la implementación Multi-AZ.	SysAdmin

Tarea	Descripción	Habilidades requeridas
En Configuration Security settings (Ajustes de seguridad de la configuración), seleccione el rol de IAM creado anteriormente.		SysAdmin
En los ajustes de Seguridad de configuración, si ya tiene un par de claves, utilícelo o cree un nuevo par de claves de Amazon EC2.		SysAdmin
En los ajustes de Monitorización de la configuración, configura Amazon CloudWatch.		SysAdmin
En Configuration Security settings (Ajustes de seguridad de la configuración), elija la VPC creada anteriormente.		SysAdmin
Seleccione Create environment (Crear entorno).		SysAdmin

Pruebe la aplicación

Tarea	Descripción	Habilidades requeridas
Pruebe la aplicación mediante la URL proporcionada en el entorno creado.		
Aplique los cambios del Servicio de nombres de		

Tarea	Descripción	Habilidades requeridas
dominio (DNS) en Amazon Route 53.		

Recursos relacionados

- GlassFish Documentación de Oracle
- GlassFish Implementación de referencia de código abierto de Java EE
- Documentación de AWS Elastic Beanstalk
- Uso de Elastic Beanstalk con Amazon CloudWatch
- Precio de AWS Elastic Beanstalk
- Grupo de escalado automático EC2
- Escalado del tamaño del grupo de escalado automático
- Implementaciones Multi-AZ de Amazon RDS

Migre una base de datos de Oracle en las instalaciones a Amazon EC2

Creado por Baji Shaik (AWS) y Pankaj Choudhary (AWS)

Entorno: PoC o piloto	Origen: bases de datos: relacionales	Destino: Oracle en Amazon EC2
Tipo R: volver a alojar	Carga de trabajo: Oracle	Tecnologías: migración; bases de datos
Servicios de AWS: Amazon EC2		

Resumen

Este patrón muestra los pasos para migrar la base de datos de Oracle en las instalaciones a una instancia de Amazon Elastic Compute Cloud (Amazon EC2). Describe dos opciones de migración: usar AWS Data Migration Service (AWS DMS) o usar herramientas nativas de Oracle, como RMAN, importación/exportación de Data Pump, espacios de tabla transportables y Oracle. GoldenGate

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos de Oracle de origen en un centro de datos en las instalaciones

Limitaciones

- El sistema operativo de destino debe ser compatible con Amazon EC2. Para ver una lista completa de los sistemas compatibles, consulte las Preguntas frecuentes de Amazon EC2.

Versiones del producto

- Versiones de Oracle 10.2 y posteriores (para las versiones 10.x), 11g y hasta 12.2 y 18c para las ediciones Enterprise, Standard, Standard One y Standard Two. Para ver la lista actualizada de

versiones compatibles con AWS DMS, consulte «Bases de datos de instancias en las instalaciones y de Amazon EC2» en Fuentes para la migración de datos en la documentación de AWS DMS.

Arquitectura

Pila de tecnología de origen

- Una base de datos Oracle en las instalaciones

Pila de tecnología de destino

- Instancia de base de datos de Oracle en Amazon EC2

Arquitectura de destino

Arquitectura de migración de datos

Uso de AWS DMS:

Uso de herramientas nativas de Oracle:

Herramientas

- AWS DMS: AWS Database Migration Service (AWS DMS) admite varios tipos de bases de datos de origen y destino. Para obtener información sobre las versiones y ediciones de bases de datos compatibles, consulte Uso de una base de datos Oracle como origen para AWS DMS. Le recomendamos utilizar la versión más reciente de AWS DMS para obtener el soporte de versiones y características más completo.
- Herramientas nativas de Oracle: RMAN, importación/exportación de Data Pump, tablespaces transportables y Oracle GoldenGate

Epics

Planificar la migración

Tarea	Descripción	Habilidades requeridas
Valide las versiones de las bases de datos de origen y de destino.		Administrador de base de datos
Identifique la versión del sistema operativo de destino.		DBA, SysAdmin
Identifique los requisitos de hardware para la instancia del servidor de destino en función de la lista de compatibilidad de Oracle y los requisitos de capacidad.		DBA, SysAdmin
Identifique los requisitos de almacenamiento (como el tipo y la capacidad de almacenamiento).		DBA, SysAdmin
Identifique los requisitos de la red, como la latencia y el ancho de banda.		DBA, SysAdmin
Elegir el tipo de instancia correcto en función de la capacidad, las características de almacenamiento y las características de la red.		DBA, SysAdmin
Identifique los requisitos de seguridad de red/host para		DBA, SysAdmin

Tarea	Descripción	Habilidades requeridas
acceder a la red de las bases de datos de origen y destino.		
Identifique una lista de los usuarios del sistema operativo necesarios para la instalación del software Oracle.		DBA, SysAdmin
Descargue e instale la herramienta de conversión de esquemas de AWS (AWS SCT)		Administrador de base de datos
Cree un proyecto de AWS SCT para la carga de trabajo y conéctese a la base de datos de origen.		Administrador de base de datos
Genere archivos SQL para la creación de objetos (tablas, índices, secuencias, etc.).		Administrador de base de datos
Determine una estrategia de copia de seguridad.		DBA, SysAdmin
Determine los requisitos de disponibilidad.		Administrador de base de datos
Identifique la estrategia de migración/cambio de aplicaciones.		DBA, propietario de la SysAdmin aplicación

Configure la infraestructura

Tarea	Descripción	Habilidades requeridas
Crear una nube privada virtual (VPC) y subredes en la cuenta de AWS.		SysAdmin
Cree grupos de seguridad y listas de control de acceso (ACL) a la red.		SysAdmin
Configure e inicie la instancia EC2.		SysAdmin

Instalación del software Oracle

Tarea	Descripción	Habilidades requeridas
Cree los usuarios y grupos del sistema operativo necesarios para que funcione el software Oracle.		DBA, SysAdmin
Descargue la versión requerida del software Oracle.		
Instale el software Oracle en la instancia EC2.		DBA, SysAdmin
Cree objetos como tablas, claves principales, vistas y secuencias mediante los scripts generados por AWS SCT.		Administrador de base de datos

Migrar datos: opción 1

Tarea	Descripción	Habilidades requeridas
Utilice las herramientas nativas de Oracle o herramientas de terceros para migrar los objetos y datos de la base de datos.	Las herramientas de Oracle incluyen la importación/exportación de Data Pump, RMAN, espacios de tablas transportables y. GoldenGate	Administrador de base de datos

Migrar datos: opción 2

Tarea	Descripción	Habilidades requeridas
Determine el método de migración.		Administrador de base de datos
Crear una instancia de replicación con la consola de AWS DMS		Administrador de base de datos
Crear los puntos de conexión de origen y destino.		Administrador de base de datos
Crear una tarea de replicación.		Administrador de base de datos
Habilite la captura de datos de cambios (CDC) para capturar los cambios para una replicación continua.		Administrador de base de datos
Ejecute la tarea de replicación y supervise los registros.		Administrador de base de datos
Cree objetos secundarios como índices y claves		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
externas cuando se complete la carga.		

Migrar la aplicación

Tarea	Descripción	Habilidades requeridas
Seguir la estrategia de migración de aplicaciones.		SysAdminDBA, propietario de la aplicación

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Siga la estrategia de transición o cambio de la aplicación.		DBA, propietario de la SysAdmin aplicación

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cierre los recursos temporales de AWS Secrets Manager.		DBA, SysAdmin
Revise y valide los documento s del proyecto.		DBA, propietario de la SysAdmin aplicación
Recopilar métricas sobre el tiempo necesario para migrar, el porcentaje de migracion es manuales frente a las realizadas con herramientas, el ahorro de costos, etc.		DBA, propietario de la SysAdmin aplicación

Tarea	Descripción	Habilidades requeridas
Cerrar el proyecto y enviar comentarios.		

Recursos relacionados

Referencias

- Estrategias para migrar la base de datos de Oracle a AWS
- Migración de bases de datos de Oracle a la nube de AWS
- Sitio web de Amazon EC2
- Sitio web de AWS DMS
- Publicaciones del blog de AWS DMS
- Precios de Amazon EC2
- Licencia del software de Oracle en el entorno de computación en la nube

Tutoriales y videos

- Introducción a Amazon EC2
- Introducción a AWS DMS
- Introducción a Amazon EC2: Elastic Cloud Server y alojamiento con AWS (video)

Migre una base de datos de Oracle en las instalaciones a Amazon EC2 mediante Oracle Data Pump

Creado por Navakanth Talluri (AWS)

Entorno: PoC o piloto	Origen: Base de datos Oracle en las instalaciones	Destino: base de datos de Oracle en Amazon EC2
Tipo R: volver a alojar	Carga de trabajo: Oracle	Tecnologías: Migración; bases de datos
Servicios de AWS: Amazon EC2; AWS Direct Connect		

Resumen

Al migrar las bases de datos, debe tener en cuenta factores como los motores y las versiones de las bases de datos de origen y destino, las herramientas y servicios de migración y los períodos de inactividad aceptables. Si va a migrar una base de datos Oracle en las instalaciones a Amazon Elastic Compute Cloud (Amazon EC2), puede utilizar herramientas de Oracle, como Oracle Data Pump y Oracle Recovery Manager (RMAN). Para obtener más información sobre estrategias, consulte la guía Migración de bases de datos de Oracle a la nube de AWS.

Oracle Data Pump le permite extraer la copia de seguridad lógica y coherente de la base de datos y a restaurarla en la instancia EC2 de destino. Este patrón describe cómo migrar una base de datos Oracle en las instalaciones a una instancia EC2 mediante Oracle Data Pump y el parámetro `NETWORK_LINK`, con un tiempo de inactividad mínimo. El parámetro `NETWORK_LINK` inicia una importación a través de un enlace de base de datos. El cliente Oracle Data Pump Import (impdp) de la instancia EC2 de destino se conecta a la base de datos de origen, recupera los datos de la misma y los escribe directamente en la base de datos de la instancia de destino. En esta solución no se utilizan archivos de copia de seguridad ni de volcado.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.

- Una base de datos de Oracle en las instalaciones:
  - No es una base de datos Oracle Real Application Clusters (RAC)
  - No es una base de datos de Oracle Automatic Storage Management (Oracle ASM)
  - Está en modo de lectura-escritura.
- Ha creado un enlace de AWS Direct Connect entre su centro de datos en las instalaciones y AWS. Para obtener más información, consulte Crear una conexión (documentación de Direct Connect).

Versiones de producto

- Oracle Database 10g versión 1 (10.1) y posteriores

Arquitectura

Pila de tecnología de origen

- Un servidor de base de datos Oracle independiente (sin RAC ni ASM) en un centro de datos en las instalaciones

Pila de tecnología de destino

- Una base de datos de Oracle en Amazon EC2

Arquitectura de destino

El pilar de fiabilidad del Marco de AWS Well-Architected recomienda crear copias de seguridad de datos para ayudar a proporcionar alta disponibilidad y resiliencia. Para obtener más información, consulte Diseño de arquitectura para alta disponibilidad en Prácticas recomendadas para ejecutar bases de datos Oracle en AWS. Este patrón configura las bases de datos principales y en espera en las instancias EC2 mediante Oracle Active Data Guard. Para un alto nivel de disponibilidad, debe crear varias instancias EC2 en diferentes zonas de disponibilidad. Sin embargo, las zonas de disponibilidad pueden estar en la misma región de AWS o en regiones de AWS diferentes.

Active Data Guard proporciona acceso de solo lectura a una base de datos física en espera al tiempo que rehace los cambios de forma continua desde la base de datos principal. En función de su objetivo de punto de recuperación (RPO) y el objetivo de tiempo de recuperación (RTO), puede elegir entre las opciones de transporte de rehacer síncrono y asíncrono.

La siguiente imagen muestra la arquitectura de destino si las instancias EC2 principal y en espera se encuentran en distintas regiones de AWS.

Arquitectura de migración de datos

Cuando haya terminado de configurar la arquitectura de destino, utilice Oracle Data Pump para migrar los datos y esquemas en las instalaciones a la instancia EC2 principal. Durante la transición, las aplicaciones no pueden acceder a la base de datos en las instalaciones ni a la base de datos de destino. Debe cerrar estas aplicaciones hasta que se puedan conectar a la nueva base de datos de destino de la instancia EC2 principal.

En la imagen siguiente, se muestra la arquitectura durante la migración de datos. En este ejemplo de arquitectura, las instancias EC2 principales y en espera se encuentran en distintas regiones de AWS.

Herramientas

Servicios de AWS

- AWS Direct Connect vincula su red interna con una ubicación de Direct Connect a través de un cable estándar Ethernet de fibra óptica. Con esta conexión, puede crear interfaces virtuales directamente en servicios públicos de AWS y derivar a los proveedores de Internet a su ruta de acceso a la red.
- Amazon Elastic Compute Cloud (Amazon EC2) brinda capacidad de computación escalable en la Nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.

Otras herramientas y servicios

- Oracle Active Data Guard le ayuda a crear, mantener, gestionar y supervisar bases de datos en espera.
- Oracle Data Pump le ayuda a trasladar datos y metadatos entre una base de datos y otra a altas velocidades.

Prácticas recomendadas

- Best Practices for Running Oracle Database on AWS
- Importación de datos mediante NETWORK_LINK

Epics

Configurar las instancias EC2 en AWS

Tarea	Descripción	Habilidades requeridas
Identifique la configuración de hardware de origen para el host en las instalaciones y los parámetros del núcleo.	Valide la configuración en las instalaciones, incluidos el tamaño de almacenamiento, las operaciones de entrada/salida por segundo (IOPS) y la CPU. Esto es importante para las licencias de Oracle, que se basan en los núcleos de la CPU.	DBA, SysAdmin
Preparar la infraestructura en AWS.	Creación de la nube privada virtual (VPC), subredes privadas, grupos de seguridad, listas de control de acceso (ACL) a la red, tablas de enrutamiento y puerta de enlace de Internet. Para obtener más información, consulte los siguientes temas: • VPC y subredes • Tutorial: Creación de una VPC para utilizarla con una instancia de base de datos	Administrador de base de datos, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Configure las instancias de EC2 mediante Active Data Guard.	Configure las instancias EC2 de AWS mediante una configuración de Active Data Guard, tal y como se describe en el Marco de AWS Well-Architected. La versión de la base de datos Oracle de la instancia EC2 puede ser diferente de la versión en las instalaciones porque este patrón utiliza copias de seguridad lógicas. Tenga en cuenta lo siguiente: • Coloque la base de datos de destino en modo de lectura-escritura. • En la base de datos de destino, proporcione los detalles del sustrato de red transparente (TNS) de la base de datos de origen. Para obtener más información, consulte: • Puesta en marcha de una base de datos (document ación de Oracle) • Creación y configuración de una base de datos Oracle (documentación de Oracle)	Administrador de base de datos, administrador de sistemas

Migrar la base de datos a Amazon EC2

Tarea	Descripción	Habilidades requeridas
Cree un dblink a la base de datos en las instalaciones desde la instancia EC2.	Cree un enlace de base de datos (dblink) entre la base de datos Oracle de la instancia EC2 y la base de datos Oracle en las instalaciones. Para obtener más información, consulte Uso de la importación de enlaces de red para mover datos (documentación de Oracle).	Administrador de base de datos
Compruebe la conexión entre la instancia EC2 y el host en las instalaciones.	Utilice el dblink para confirmar que la conexión entre la instancia EC2 y la base de datos en las instalaciones funciona. Para obtener instrucciones, consulte CREATE DATABASE LINK (documentación de Oracle).	Administrador de base de datos
Detenga todas las aplicaciones conectadas a la base de datos en las instalaciones.	Una vez aprobado el tiempo de inactividad de la base de datos, cierre todas las aplicaciones y trabajos dependientes que se conecten a la base de datos en las instalaciones. Puede hacerlo directamente desde la aplicación o desde la base de datos mediante cron. Para obtener más información, consulte Uso de la utilidad	Administrador de base de datos, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	Crontab para programar tareas en Oracle Linux.	
Programe el trabajo de migración de datos.	En el host de destino, utilice el comando `impdb` para programar la importación de Data Pump. Esto conecta la base de datos de destino con el host en las instalaciones e inicia la migración de datos. Para obtener más información, consulte Importación de Data Pump y NETWORK_LINK (documentación de Oracle).	Administrador de base de datos
Validar la migración de datos.	La validación de los datos es un paso crucial. Para la validación de datos, puede utilizar herramientas personalizadas o herramientas de Oracle, como una combinación de consultas dblink y SQL.	Administrador de base de datos

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Coloque la base de datos de origen en un modo de solo lectura.	Confirme que la aplicación esté cerrada y que no se estén realizando cambios en la base de datos de origen. Abra la base de datos de origen en modo de solo lectura. Esto le permite evitar cualquier transacción	DBA, DevOps ingeniero, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	abierta. Para obtener más información, consulte `ALTER DATABASE` en SQL Statements (documentación de Oracle).	
Valide el recuento de objetos y los datos.	Para validar los datos y objetos, puede utilizar herramientas personalizadas o herramientas de Oracle, como una combinación de consultas dblink y SQL.	Administrador de base de datos, desarrollador de aplicaciones
Conecta las aplicaciones la nueva base de datos de la instancia EC2 principal	Cambie el atributo de conexión de la aplicación para que apunte a la nueva base de datos que creó en la instancia EC2 principal.	Administrador de base de datos, desarrollador de aplicaciones
Valide el rendimiento de la aplicación.	Inicie la aplicación. Valide la funcionalidad y el rendimiento de la aplicación mediante el Repositorio automatizado de cargas de trabajo (documentación de Oracle).	Desarrollador de aplicaciones, DevOps ingeniero, DBA

Recursos relacionados

Referencias de AWS

- Migración de bases de datos de Oracle a la Nube de AWS
- Amazon EC2 para Oracle
- Migración de bases de datos voluminosas de Oracle a AWS para entornos multiplataforma
- VPC y subredes
- Tutorial: Creación de una VPC para utilizarla con una instancia de base de datos

Referencias de Oracle

- Configuraciones de Oracle Data Guard
- Importación de Data Pump

Migración de una base de datos de SAP ASE en las instalaciones a Amazon EC2

Tipo R: volver a alojar	Origen: bases de datos: relacionales	Destino: SAP Adaptive Server Enterprise en Amazon EC2
Creado por: AWS	Entorno: PoC o piloto	Tecnologías: bases de datos; migración
Carga de trabajo: SAP	Servicios de AWS: Amazon EC2	

Resumen

Este patrón describe la migración de una base de datos de SAP Adaptive Server Enterprise (ASE) de un host en las instalaciones a una instancia de Amazon Elastic Compute Cloud (Amazon EC2). El patrón abarca el uso de AWS Database Migration Service (AWS DMS) o herramientas nativas de SAP ASE, como ASE Cockpit, Sybase Central para ASE y Administrador de base de datos Cockpit para la migración.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos de origen SAP ASE en un centro de datos en las instalaciones

Limitaciones

- La base de datos de origen debe tener menos de 64 TB

Versiones de producto

- SAP ASE versiones 15.x y 16.x o posteriores

Arquitectura

Pila de tecnología de origen

- Base de datos de SAP ASE en las instalaciones

Pila de tecnología de destino

- Una base de datos SAP ASE en una instancia EC2

Arquitectura de migración de base de datos

Uso de AWS DMS:

Uso de herramientas SAP ASE nativas:

Herramientas

- AWS DMS es un servicio de migración de datos AWS (AWS DMS) que admite varios tipos de bases de datos de origen y destino. Para obtener más información, consulte Orígenes de la migración de datos y Objetivos de la migración de datos. Le recomendamos utilizar la versión más reciente de AWS DMS para obtener el soporte más completo de versiones y características.
- SAP ASE: las herramientas nativas incluyen ASE Cockpit, Sybase Central para ASE y DBA Cockpit.

Epics

Analice la migración

Tarea	Descripción	Habilidades requeridas
Valide las versiones de las bases de datos de origen y de destino.		Administrador de base de datos
Identifique la versión del sistema operativo de destino.		DBA, SysAdmin
Identifique los requisitos de hardware para la instancia del servidor de destino en función de la lista de compatibilidad de SAP ASE y los requisitos de capacidad.		DBA, SysAdmin
Identifique los requisitos para el tipo y la capacidad de almacenamiento.		DBA, SysAdmin
Identifique los requisitos de la red, como la latencia y el ancho de banda.		DBA, SysAdmin
Elija el tipo de instancia, la capacidad, las caracterí sticas de almacenamiento y las características de red adecuadas.		DBA, SysAdmin
Identificar los requisitos de seguridad para acceder a la red y al host de las bases de datos de origen y destino.		DBA, SysAdmin

Tarea	Descripción	Habilidades requeridas
Identifique una lista de los usuarios del sistema operativo necesarios para la instalación del software SAP ASE.		DBA, SysAdmin
Determinar la estrategia de copia de seguridad.		Administrador de base de datos
Determinar los requisitos de disponibilidad.		Administrador de base de datos
Identifique la estrategia de migración y transición de aplicaciones.		DBA, propietario de la SysAdmin aplicación

Configuración de la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC) y subredes.		SysAdmin
Cree grupos de seguridad y listas de control de acceso a la red (ACL).		SysAdmin
Configure e inicie la instancia EC2.		SysAdmin

Instalar el software

Tarea	Descripción	Habilidades requeridas
Cree los usuarios y grupos del sistema operativo necesarios		DBA, SysAdmin

Tarea	Descripción	Habilidades requeridas
para que funcione el software SAP ASE.		
Descargue la versión requerida del software SAP ASE.		DBA, SysAdmin
Instale la base de datos SAP ASE, el software del servidor de copia de seguridad y el software del servidor de replicación en la instancia EC2 y, a continuación, configure el servidor.		DBA, SysAdmin

Migración de datos: opción 1

Tarea	Descripción	Habilidades requeridas
Utilice las herramientas nativas de SAP ASE o herramientas de terceros para migrar los objetos y datos de la base de datos.	Consulte la documentación de SAP ASE o de herramientas de terceros. Las herramientas nativas incluyen ASE Cockpit, Sybase Central para ASE y DBA Cockpit.	Administrador de base de datos

Migración de datos: opción 2

Tarea	Descripción	Habilidades requeridas
Migre los datos mediante AWS DMS.		Administrador de base de datos

Migración de la aplicación

Tarea	Descripción	Habilidades requeridas
Seguir la estrategia de migración de aplicaciones.		DBA, propietario de la SysAdmin aplicación

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Siga la estrategia de transición o cambio de la aplicación.		DBA, propietario de la SysAdmin aplicación

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cerrar los recursos temporales de AWS.		DBA, SysAdmin
Revise y valide los documentos del proyecto.		DBA, propietario de la SysAdmin aplicación
Recopile métricas sobre el tiempo de migración, el porcentaje de ahorro de costos manuales en comparación con los de herramientas, etc.		DBA, propietario de la SysAdmin aplicación
Cierre el proyecto y envíe sus comentarios.		DBA, propietario de la SysAdmin aplicación

Recursos relacionados

Referencias

- Amazon EC2
- AWS DMS
- Precios de Amazon EC2

Tutoriales y videos

- Introducción a Amazon EC2
- Introducción a AWS Database Migration Service (AWS DMS)
- AWS Data Migration Service (video)
- Introducción a Amazon EC2: Elastic Cloud Server y alojamiento con AWS (video)

Migración de una base de datos de Microsoft SQL Server en las instalaciones a Amazon EC2

Tipo R: volver a alojar	Origen: bases de datos: relacionales	Destino: Microsoft SQL Server en Amazon EC2
Creado por: AWS	Entorno: PoC o piloto	Tecnologías: bases de datos; migración
Carga de trabajo: Microsoft	Servicios de AWS: Amazon EC2	

Resumen

Este patrón describe cómo migrar una base de datos de Microsoft SQL Server en las instalaciones a Microsoft SQL Server en una instancia de Amazon Elastic Compute Cloud (Amazon EC2). Incluye dos opciones de migración: utilizar el AWS Data Migration Service (AWS DMS) o utilizar herramientas nativas de Microsoft SQL Server, como la copia de seguridad y la restauración, el asistente para copiar bases de datos o la función de copiar y adjuntar bases de datos.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un sistema operativo compatible con Amazon EC2 (para obtener la lista completa de las versiones de sistemas operativos compatibles, consulte Preguntas frecuentes sobre Amazon EC2)
- Una base de datos de origen de Microsoft SQL Server en un centro de datos en las instalaciones

Versiones de producto

- Versiones de Microsoft SQL Server 2005, 2008, 2008R2, 2012, 2014, 2016 y 2017, para las ediciones Enterprise, Standard, Workgroup y Developer, si utiliza AWS DMS. Para migrar la edición Web o Express de Microsoft SQL Server, utilice herramientas nativas o de terceros. Para ver la lista actualizada de versiones compatibles, consulte Uso de una base de datos de Microsoft SQL Server como destino para AWS DMS.

Arquitectura

Pila de tecnología de origen

- Base de datos de Microsoft SQL Server en las instalaciones

Pila de tecnología de destino

- Base de datos de Microsoft SQL Server en una instancia de EC2

Arquitectura de destino

Arquitectura de migración de datos

- Uso de AWS DMS

- Uso de herramientas nativas de SQL Server

Herramientas

- AWS DMS: AWS Data Migration Service (AWS DMS) le permite migrar datos hacia y desde bases de datos comerciales y de código abierto muy utilizadas, incluidas Oracle, SQL Server, MySQL y PostgreSQL. Puede utilizar AWS DMS para migrar datos a la nube de AWS, entre instancias en las instalaciones (a través de una configuración de nube de AWS) o entre combinaciones de configuraciones en las instalaciones y en la nube.
- Herramientas nativas de Microsoft SQL Server: incluyen copia de seguridad y restauración, asistente para copiar bases de datos y la función de copiar y adjuntar bases de datos.

Epics

Planificación de la migración

Tarea	Descripción	Habilidades requeridas
Valide las versiones de las bases de datos de origen y de destino.		Administrador de base de datos
Identificar la versión del sistema operativo de destino.		DBA, SysAdmin
Identifique los requisitos de hardware para la instancia del servidor de destino en función de la lista de compatibilidad de Microsoft SQL Server y los requisitos de capacidad.		DBA, SysAdmin
Identificar los requisitos de almacenamiento relativos al tipo y la capacidad.		DBA, SysAdmin
Identificar los requisitos de la red, como la latencia y el ancho de banda.		DBA, SysAdmin
Elegir el tipo de instancia de EC2 en función de la capacidad, las características de almacenamiento y las características de red.		DBA, SysAdmin
Identificar los requisitos de seguridad para acceder a la red y al host de las bases de datos de origen y destino.		DBA, SysAdmin

Tarea	Descripción	Habilidades requeridas
Identificar la lista de usuarios necesarios para la instalaci ón del software Microsoft SQL Server.		DBA, SysAdmin
Determinar la estrategia de copia de seguridad.		Administrador de base de datos
Determinar los requisitos de disponibilidad.		Administrador de base de datos
Identificar la estrategia de migración y transición de aplicaciones.		DBA, SysAdmin

Configuración de la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC) y subredes.		SysAdmin
Cree grupos de seguridad y listas de control de acceso a la red (ACL).		SysAdmin
Configure e inicie una instancia EC2.		SysAdmin

Instalar el software

Tarea	Descripción	Habilidades requeridas
Crear los usuarios y grupos necesarios para el software Microsoft SQL Server.		DBA, SysAdmin
Descargar el software Microsoft SQL Server.		DBA, SysAdmin
Instalar el software Microsoft SQL Server en la instancia EC2 y configurar el servidor.		DBA, SysAdmin

Migración de datos: opción 1

Tarea	Descripción	Habilidades requeridas
Utilizar herramientas nativas de MySQL Server o herramientas de terceros para migrar los objetos y datos de la base de datos.	Las herramientas incluyen la copia de seguridad y la restauración, el asistente para copiar bases de datos y la función de copiar y adjuntar bases de datos.	Administrador de base de datos

Migración de datos: opción 2

Tarea	Descripción	Habilidades requeridas
Migre los datos mediante AWS DMS.	Para obtener información detallada sobre el uso de AWS DMS, consulte los enlaces de la sección Referencias y ayuda.	Administrador de base de datos

Migración de la aplicación

Tarea	Descripción	Habilidades requeridas
Seguir la estrategia de migración de aplicaciones.	Utilizar la herramienta de conversión de esquemas de AWS (AWS SCT) para analizar y modificar el código SQL incrustado en el código fuente de la aplicación.	Administrador de base de datos, propietario de la aplicación

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Seguir la estrategia de cambio de aplicaciones.		DBA, propietario de la SysAdmin aplicación

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cerrar todos los recursos temporales de AWS.	Los recursos temporale s incluyen la instancia de replicación de AWS DMS y la instancia de EC2 utilizadas para AWS SCT.	DBA, SysAdmin
Revise y valide los documento s del proyecto.		DBA, propietario de la SysAdmin aplicación
Recopile métricas sobre el tiempo de migración , el porcentaje de ahorro de costos manuales en		DBA, propietario de la SysAdmin aplicación

Tarea	Descripción	Habilidades requeridas
comparación con los de herramientas, etc.		
Cerrar el proyecto y enviar comentarios.		DBA, propietario de la SysAdmin aplicación

Recursos relacionados

Referencias

- Implementación de Microsoft SQL Server en Amazon Web Services
- Amazon EC2
- Preguntas frecuentes sobre Amazon EC2
- AWS Database Migration Service (AWS DMS)
- Precios de Amazon EC2
- Productos de Microsoft en AWS
- Licencias de Microsoft en AWS
- Microsoft SQL Server en AWS

Tutoriales y videos

- Introducción a Amazon EC2
- Introducción a AWS Database Migration Service (AWS DMS)
- Agregar una instancia de Amazon EC2 a su directorio (Simple AD y Microsoft AD)
- AWS Database Migration Service (AWS DMS) (video)
- Introducción a Amazon EC2: Elastic Cloud Server y alojamiento con AWS (video)

Migración de una base de datos MySQL en las instalaciones a Amazon EC2

Tipo R: volver a alojar	Origen: bases de datos: relacionales	Destino: MySQL en Amazon EC2
Creado por: AWS	Entorno: PoC o piloto	Tecnologías: bases de datos; migración
Carga de trabajo: código abierto		

Resumen

Este patrón proporciona orientación para migrar una base de datos MySQL en las instalaciones a una base de datos MySQL en una instancia de Amazon Elastic Compute Cloud (Amazon EC2). El patrón analiza el uso del AWS Database Migration Service (AWS DMS) o de herramientas nativas de MySQL, como mysqldbcopy y mysqldump para la migración.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos de MySQL de origen en un centro de datos en las instalaciones

Versiones de producto

- Versiones de MySQL 5.5, 5.6 y 5.7
- Para obtener una lista de sistemas operativos de destino compatibles con Amazon EC2, consulte las Preguntas frecuentes de Amazon EC2

Arquitectura

Pila de tecnología de origen

- Una base de datos MySQL en las instalaciones

Pila de tecnología de destino

- Una instancia de base de datos de MySQL en Amazon EC2

Métodos de migración de datos de AWS

- AWS DMS
- Herramientas nativas de MySQL (mysqldbcopy, mysqldump)

Arquitectura de destino

Arquitectura de migración de datos de AWS

Uso de AWS DMS:

Uso de herramientas MySQL nativas:

Herramientas

- AWS DMS: AWS Database Migration Service (AWS DMS) admite varias bases de datos de origen y destino. Para obtener información sobre las bases de datos de origen y destino de MySQL compatibles con AWS DMS, consulte Migrating MySQL-Compatible Databases to AWS (Migrar bases de datos compatibles con MySQL a AWS). Si su base de datos de origen no es compatible con AWS DMS, debe elegir otro método para migrar los datos.
- Herramientas nativas de MySQL: mysqldbcopy y mysqldump

Epics

Planificación de la migración

Tarea	Descripción	Habilidades requeridas
Valide las versiones de las bases de datos de origen y de destino.		Administrador de base de datos
Identificar la versión del sistema operativo de destino.		DBA, SysAdmin
Identifique los requisitos de hardware para la instancia del servidor de destino en función de la lista de compatibilidad de MySQL y los requisitos de capacidad.		DBA, SysAdmin
Identifique los requisitos de almacenamiento (como el tipo y la capacidad de almacenamiento).		DBA, SysAdmin
Identifique los requisitos de la red, como la latencia y el ancho de banda.		DBA, SysAdmin
Elija el tipo de instancia adecuado en función de la capacidad, las características de almacenamiento y las características de red.		DBA, SysAdmin
Identifique requisitos de seguridad para acceder a la		DBA, SysAdmin

Tarea	Descripción	Habilidades requeridas
red o al host de las bases de datos de origen y destino.		
Identifique una lista de los usuarios del sistema operativo necesarios para la instalación del software MySQL.		DBA, SysAdmin
Determine una estrategia de copia de seguridad.		Administrador de base de datos
Determine los requisitos de disponibilidad.		Administrador de base de datos
Identifique la estrategia de migración o transición de aplicaciones.		DBA, SysAdmin

Configuración de la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC) y subredes.		SysAdmin
Cree grupos de seguridad y listas de control de acceso (ACL) a la red.		SysAdmin
Configure e inicie una instancia EC2.		SysAdmin

Instalar el software MySQL

Tarea	Descripción	Habilidades requeridas
Cree los usuarios y grupos del sistema operativo necesarios para que funcione el software MySQL.		DBA, SysAdmin
Descargue la versión requerida del software MySQL.		DBA, SysAdmin
Instale el software MySQL en la instancia de EC2 y configure el servidor.		DBA, SysAdmin

Migración de datos: opción 1

Tarea	Descripción	Habilidades requeridas
Utilice las herramien tas nativas de MySQL o herramientas de terceros para migrar los objetos y datos de la base de datos.	Estas herramientas incluyen mysqldbcopy y mysqldump.	Administrador de base de datos

Migración de datos: opción 2

Tarea	Descripción	Habilidades requeridas
Migre datos con AWS DMS.		Administrador de base de datos

Migración de la aplicación

Tarea	Descripción	Habilidades requeridas
Seguir la estrategia de migración de aplicaciones.		DBA, propietario de la SysAdmin aplicación

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Siga la estrategia de transición o cambio de la aplicación.		DBA, propietario de la SysAdmin aplicación

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cerrar los recursos temporales de AWS.	Elimine la instancia de replicación de AWS DMS.	DBA, SysAdmin
Revise y valide los documentos del proyecto.		DBA, propietario de la SysAdmin aplicación
Recopile métricas sobre el tiempo de migración, el porcentaje de migraciones manuales en comparación con las realizadas con herramientas, el ahorro de costos, etc.		DBA, propietario de la SysAdmin aplicación
Cerrar el proyecto y enviar comentarios.		DBA, propietario de la SysAdmin aplicación

Recursos relacionados

Referencias

- Sitio web de Amazon EC2
- Sitio web de AWS DMS
- Precios de Amazon EC2
- AWS DMS Step-by-Step Walkthroughs (Guías paso a paso de AWS DMS)

Tutoriales y videos

- Introducción a AWS DMS
- Introducción a Amazon EC2: Elastic Cloud Server y alojamiento con AWS (video)

Reduzca el tiempo de transición de la migración homogénea de SAP mediante el servicio de migración de aplicaciones

Creado por Pavel Rubin (AWS), Diego Valverde (AWS) y Sunil Yadav (AWS)

Entorno: producción	Origen: base de datos de SAP ASE en las instalaciones	Destino: base de datos SAP en Amazon EC2
Tipo R: volver a alojar	Carga de trabajo: SAP	Tecnologías: migración; bases de datos
Servicios de AWS: servicio de migración de aplicaciones de AWS; Amazon EBS		

Resumen

Este patrón describe los pasos para migrar las cargas de trabajo de SAP mediante el Servicio de migración de aplicaciones de AWS. El Servicio de migración de aplicaciones facilita las transiciones mediante el uso de la replicación a nivel de bloques para mantener los volúmenes de replicación que se sincronizan continuamente desde sus orígenes.

Las cargas de trabajo de SAP incluyen las aplicaciones SAP Customer Relationship Management (SAP CRM), SAP Enterprise Resource Planning (ERP) y SAP Business Warehouse (SAP BW).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa con conectividad de red estable entre los servidores SAP de origen y la nube privada virtual (VPC) de destino en AWS
- Una base de datos fuente de SAP Adaptive Server Enterprise (ASE) para Linux o Windows en un centro de datos en las instalaciones

Limitaciones

- El sistema operativo de destino debe ser compatible con Amazon Elastic Compute Cloud (Amazon EC2). Para obtener más información, consulte Preguntas frecuentes de Amazon EC2.

Arquitectura

Pila de tecnología de origen

- Una base de datos SAP ASE

Pila de tecnología de destino

- Amazon EC2
- Amazon Elastic Block Store (Amazon EBS)

Arquitectura de origen y destino

El siguiente diagrama muestra la migración desde los servidores en las instalaciones a través del agente de replicación al punto de conexión del Servicio de migración de aplicaciones. Se utiliza un punto de conexión Amazon Simple Storage Service (Amazon S3) para acceder a los archivos de instalación y configuración. Las subredes del área de ensayo y los recursos migrados contienen instancias de EC2, con almacenamiento de datos en volúmenes de EBS. El puerto TCP 443 se utiliza para conectar la red del equipo de origen al Servicio de migración de aplicaciones y para conectar las subredes del área de ensayo a los puntos de conexión regionales del Servicio de migración de aplicaciones, Amazon EC2 y Amazon S3. El puerto TCP 1500 se utiliza para la replicación de datos entre la red local y el área de ensayo.

Herramientas

- AWS Application Migration Service le ayuda a realojar (lift-and-shift) aplicaciones en la nube de AWS sin cambios y con un tiempo de inactividad mínimo.
- Amazon Elastic Block Store (Amazon EBS) proporciona volúmenes de almacenamiento por bloques para su uso con instancias de Amazon Elastic Compute Cloud (Amazon EC2).
- Amazon Elastic Compute Cloud (Amazon EC2) brinda capacidad de computación escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Security Token Service (AWS STS) le ayuda a solicitar credenciales temporales con privilegios limitados para los usuarios.

Epics

Inicie el Servicio de migración de aplicaciones de AWS

Tarea	Descripción	Habilidades requeridas
Inicie el Servicio de migración de aplicaciones de AWS.	Inicie el Servicio de migración de aplicaciones en la región de AWS a donde desee implementar la base de datos SAP ASE. AWS proporciona una configuración automatiz ada la primera vez que navega a la página del Servicio de migración de aplicaciones en cada región.	Administrador de AWS
Cree roles de servicio manualmente.	(Opcional) Si desea utilizar la automatización (por ejemplo, AWS Control Tower) para configurar la cuenta, puede crear manualmente los seis roles de AWS Identity and Access Management (IAM) necesarios para la instalación, la replicación y el lanzamien to. Para obtener instrucciones, consulte la documentación de AWS.	Administrador de AWS
Cree una plantilla de configura ción de replicación.	La plantilla de configura ción de replicación define la	AWS general

Tarea	Descripción	Habilidades requeridas
	subred, el tipo de instancia, el cifrado de Amazon EBS y la forma en que se enrutan los datos. Para obtener información detallada sobre la configuración, consulte la documentación de AWS.	

Genere credenciales para la instalación del agente

Tarea	Descripción	Habilidades requeridas
Cree un nuevo rol de IAM.	En la consola de IAM, vaya a Roles (Roles) y, a continuación, seleccione Create Role (Crear rol). Para el Trusted entity type (Tipo de entidad de confianza), elija AWS account (Cuenta de AWS) y, a continuación, elija Next (Siguiente).	Administrador de sistemas de AWS
Adjúntelo AWSApplicationMigrationAgentPolicy a la función de IAM.	La política administrada de AWS `AWSApplicationMigrationAgentPolicy` contiene los permisos necesarios para realizar la instalación del agente del servicio de migración de aplicaciones. Después de adjuntar la política, seleccione Next (Siguiente).	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
Complete la creación del rol.	Asigne un nombre descriptivo y elija Create role (Crear rol).	Administrador de sistemas de AWS
Genere credenciales temporales.	Para generar el ID de clave de acceso, la clave de acceso secreta y el token de sesión, siga las instrucciones de la documentación de AWS STS. Estas credenciales se utilizan durante la instalación del agente.	Administrador de sistemas de AWS

Instale el agente del Servicio de migración de aplicaciones en el equipo origen de SAP

Tarea	Descripción	Habilidades requeridas
Descargue el instalador del agente en el equipo origen de SAP.	Descargue el instalador del agente adecuado para su sistema operativo de origen: Windows o Linux.	Propietario de la aplicación
Instale el agente de replicación de AWS.	Al ejecutar el archivo de instalación del agente en un equipo de origen, primero se le pide que introduzca la clave de acceso, la clave de acceso secreta, el token de sesión y la región en la que desea realizar la replicación. Utilice las credenciales temporales del rol de IAM que creó anteriormente y la misma región que configuró durante la inicialización.	Propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Espere la replicación inicial de los datos.	Una vez instalado el agente, el equipo de origen aparece en la pestaña Equipos de la consola del Servicio de migración de aplicaciones.	Propietario de la aplicación

Configure la plantilla de lanzamiento del equipo de destino

Tarea	Descripción	Habilidades requeridas
Actualice la plantilla de lanzamiento para el servidor de origen.	Cada servidor de origen utiliza una plantilla de lanzamiento de EC2 única que informa de la configuración del servidor EC2 de destino. Puede editar esta plantilla si desea personalizar la configuración de Amazon EC2 del servidor migrado.	AWS general
Establezca la versión de la plantilla de lanzamiento predeterminada.	Tras realizar los cambios necesarios en la plantilla de lanzamiento, especifiq ue utilizar esta versión actualizada como plantilla de lanzamiento predeterminada. Para obtener más información, consulte la documentación de AWS.	AWS general
Desactive el tamaño correcto del tipo de instancia.	(Opcional) El tamaño correcto del tipo de instancia proporciona recomenda ciones automáticas de tipos de instancia en función de la	AWS general

Tarea	Descripción	Habilidades requeridas
	configuración del servidor SAP de origen. Le recomendamos desactivar esta configuración para poder especificar tipos de instancias personalizados en la plantilla de lanzamiento.	

Realice una prueba

Tarea	Descripción	Habilidades requeridas
Inicie un lanzamiento de prueba.	En la consola del Servicio de migración de aplicaciones, seleccione uno o más servidores y, a continuación, seleccione Lanzar instancias de prueba en Prueba y transición.	AWS general, ingeniero de migraciones, jefe de migraciones
Espere a que se complete el proceso de conversión y lanzamiento.	Puede revisar el proceso de lanzamiento en la pestaña Historial de lanzamientos. Una vez que el equipo se haya lanzado correctamente como instancia de EC2, la pestaña Alertas se actualizará a Lanzada.	
Compruebe que la prueba se haya completado correctamente.	Conéctese a la instancia lanzada mediante el Protocolo de escritorio remoto (RDP) o SSH (Secure Shell) y realice las comprobaciones de aplicación adecuadas. Por ejemplo, inicie sesión en la	Ingeniero de migraciones, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	interfaz de SAP y valide la funcionalidad.	
Actualice el ciclo de vida de origen.	Si las pruebas se realizaron correctamente, actualice el ciclo de vida del equipo de origen para marcarlo como “Preparado para la transició n” en la pestaña Prueba y transición.	Ingeniero de migraciones, jefe de migraciones

Programe y realice una transición al destino de Amazon EC2

Tarea	Descripción	Habilidades requeridas
Programe una transición temporal.		Jefe de transición, jefe de migración, propietario de la aplicación
Inicie una transición temporal.	Seleccione uno o varios servidores. En la pestaña Prueba y transición, seleccion e Iniciar instancias transitor ias en Prueba y transición en la consola del Servicio de migración de aplicaciones.	Ingeniero de migraciones
Espere a que se completen los procesos de conversión y lanzamiento.	Puede revisar el proceso de lanzamiento en la pestaña Historial de lanzamientos. Una vez que el equipo se haya lanzado correctamente como instancia de EC2, la pestaña Alertas se actualizará a Lanzada.	

Tarea	Descripción	Habilidades requeridas
Compruebe que la transición se haya completado correctamente.	Conéctese a la instancia lanzada mediante el RDP o SSH y realice las comprobaciones de aplicación adecuadas.	Ingeniero de migraciones, propietario de la aplicación
Actualice el ciclo de vida de origen.	Si la transición se realizó correctamente, actualice el ciclo de vida del equipo de origen seleccionando Finalizar la transición en la pestaña Prueba y transición.	Ingeniero de migraciones

Recursos relacionados

Referencias

- AWS Application Migration Service
- Preguntas frecuentes sobre migración de aplicaciones de AWS

Video

- Arquitectura del Servicio de migración de aplicaciones de AWS

Vuelva a alojar las cargas de trabajo en las instalaciones en la nube de AWS: lista de verificación de migración

Creado por Srikanth Rangavajhala (AWS)

Entorno: PoC o piloto	Origen: cargas de trabajo en las instalaciones	Destino: nube de AWS
Tipo R: volver a alojar	Carga de trabajo: Microsoft	Tecnologías: migración; nube híbrida; sistemas operativos
Servicios de AWS: Servicio de migración de aplicaciones de AWS; Amazon EC2; Amazon Connect		

Resumen

Volver a alojar las cargas de trabajo en las instalaciones en la nube de Amazon Web Services (AWS) implica las siguientes fases de migración: planificación, predetección, detección, creación, prueba y transición. Este patrón describe las fases y sus tareas relacionadas. Las tareas se describen de forma detallada y soportan aproximadamente el 75 % de todas las cargas de trabajo de las aplicaciones. Puede implementar estas tareas en un plazo de dos o tres semanas en un ciclo de iteraciones ágil.

Debería revisar y examinar estas tareas con su equipo de migración y sus consultores. Tras la revisión, puede recopilar los datos, eliminar o volver a evaluar las tareas según sea necesario para cumplir con sus requisitos y modificar otras tareas para que admitan al menos el 75 % de las cargas de trabajo de las aplicaciones de su cartera. A continuación, puede utilizar una herramienta de gestión de proyectos ágil, como Atlassian Jira o Rally Software, para importar las tareas, asignarlas a los recursos y realizar un seguimiento de las actividades de migración.

El patrón supone que utiliza AWS Cloud Migration Factory para volver a alojar sus cargas de trabajo, pero puede utilizar la herramienta de migración que prefiera.

Macie puede ayudarlo a identificar los datos confidenciales de sus bases de conocimiento almacenados como fuentes de datos, modelar los registros de invocación y almacenarlos

rápidamente en depósitos de S3. Para conocer las mejores prácticas de seguridad de Macie, consulte la sección anterior de Macie en esta guía.

Requisitos previos y limitaciones

Requisitos previos

- Herramienta de gestión de proyectos para realizar un seguimiento de las tareas de migración (por ejemplo, Atlassian Jira o Rally Software)
- Herramienta de migración para volver a alojar sus cargas de trabajo en AWS (por ejemplo, Cloud Migration Factory)

Arquitectura

Plataforma de origen

- Pila de origen en las instalaciones (incluidas tecnologías, aplicaciones, bases de datos e infraestructura)

Plataforma de destino

- Pila de destino en la nube de AWS (incluidas tecnologías, aplicaciones, bases de datos e infraestructura)

Arquitectura

En el siguiente diagrama, se muestra el realojamiento (detección y migración de servidores desde un entorno de origen en las instalaciones a AWS) mediante Cloud Migration Factory y AWS Application Migration Service.

Herramientas

- Puede utilizar la herramienta de migración y gestión de proyectos que elija.

Epics

Fase de planificación

Tarea	Descripción	Habilidades requeridas
Prepare el volumen de trabajo pendiente previo a la detección.	Lleve a cabo la sesión de trabajo previa a la detección de los volúmenes de trabajo pendientes con los jefes de departamento y los propietarios de las aplicaciones.	Director de proyectos, líder de Agile Scrum
Dirija la sesión de trabajo de planificación de la iteración.	Como ejercicio de análisis, distribuya las aplicaciones que desee migrar entre iteraciones y oleadas.	Director de proyectos, líder de Agile Scrum

Fase previa a la detección

Tarea	Descripción	Habilidades requeridas
Confirmar los conocimientos de la aplicación.	Confirme y documente al propietario de la aplicación y su conocimiento de la aplicación. Determinar si hay otra persona de contacto para las cuestiones técnicas.	Especialista en migración (entrevistador)
Determine los requisitos de conformidad de las aplicaciones.	Confirme con el propietario de la aplicación que la aplicación no tiene por qué cumplir los requisitos del estándar de seguridad de datos del sector de las tarjetas de pago (PCI DSS), la Ley Sarbanes-Oxley (SOX), la información	Especialista en migración (entrevistador)

Tarea	Descripción	Habilidades requeridas
	de identificación personal (PII) u otras normas. Si existen requisitos de conformidad, los equipos deben finalizar las comprobaciones de conformidad en los servidores que se van a migrar.	
Confirme los requisitos de lanzamiento de producción.	Confirme los requisitos para lanzar la aplicación migrada a producción (como la fecha de lanzamiento y la duración del tiempo de inactividad) con el propietario de la aplicación o el contacto técnico.	Especialista en migración (entrevistador)
Obtener la lista de servidores.	Obtenga la lista de servidores asociados a la aplicación de destino.	Especialista en migración (entrevistador)
Obtener el diagrama lógico que muestra el estado actual.	Obtenga el diagrama de estado actual de la aplicación del arquitecto empresarial o del propietario de la aplicación.	Especialista en migración (entrevistador)
Crear un diagrama lógico que muestre el estado objetivo.	Cree un diagrama lógico de la aplicación que muestre la arquitectura de destino en AWS. Este diagrama debe ilustrar los servidores, la conectividad y los factores de asignación.	Arquitecto empresarial, propietario de una empresa

Tarea	Descripción	Habilidades requeridas
Obtener información sobre el servidor.	Recopile información sobre los servidores asociados a la aplicación, incluidos sus detalles de configuración.	Especialista en migración (entrevistador)
Añada la información del servidor a la plantilla de detección.	Añada información detallada del servidor a la plantilla de detección de aplicacio nes (consulte `mobilize-application-questionnaire.xlsx` en el anexo de este patrón). Esta plantilla incluye todos los detalles de seguridad, infraestructura, sistema operativo y redes relacionados con las aplicaciones.	Especialista en migración (entrevistador)
Publicar la plantilla de detección de aplicaciones.	Comparta la plantilla de detección de aplicaciones con el propietario de la aplicación y el equipo de migración para un acceso y un uso comunes.	Especialista en migración (entrevistador)

Fase de detección

Tarea	Descripción	Habilidades requeridas
Confirmar la lista de servidores.	Confirme la lista de servidores y el propósito de cada servidor con el propietario de la aplicación o el responsable técnico.	Especialista de migración

Tarea	Descripción	Habilidades requeridas
Identificar y añadir grupos de servidores.	Identifique grupos de servidores, como servidores web o servidores de aplicaciones, y añada esta información a la plantilla de detección de aplicaciones. Seleccione el nivel de la aplicación (web, aplicación, base de datos) al que debe pertenecer cada servidor.	Especialista de migración
Publicar la plantilla de detección de aplicaciones.	Complete los detalles de la plantilla de detección de aplicaciones con la ayuda del equipo de migración, el equipo de aplicaciones y AWS.	Especialista de migración
Añada los detalles del servidor que faltan (equipos de middleware y sistema operativo).	Pida a los equipos de middleware y sistema operativo (SO) que revisen la plantilla de detección de aplicaciones y añadan los detalles del servidor que falten, incluida la información de la base de datos.	Especialista de migración

Tarea	Descripción	Habilidades requeridas
Obtener las normas de tráfico entrante/saliente (equipo de red).	Pídale al equipo de red que obtenga las reglas de tráfico entrante/saliente para los servidores de origen y destino. El equipo de red también debe añadir las reglas de firewall existentes, exportarlas a un formato de grupo de seguridad y añadir los equilibradores de carga existentes a la plantilla de detección de aplicaciones.	Especialista de migración
Identificar el etiquetado necesario.	Determine los requisitos de etiquetado de la aplicación.	Especialista de migración
Crear detalles de solicitud de firewall.	Capture y filtre las reglas de firewall necesarias para comunicarse con la aplicació n.	Especialista en migración, arquitecto de soluciones y líder de redes
Actualice el tipo de instancia EC2.	Actualice el tipo de instancia de Amazon Elastic Compute Cloud (Amazon EC2) para que se utilice en el entorno de destino, en función de los requisitos de infraestructura y servidor.	Especialista en migración, arquitecto de soluciones y líder de redes
Identifique el diagrama de estado actual.	Identifique o cree el diagrama que muestra el estado actual de la aplicación. Este diagrama se utilizará en la solicitud de seguridad de la información (InfoSec).	Especialista en migración, arquitecto de soluciones

Tarea	Descripción	Habilidades requeridas
Finalice el diagrama de estado futuro.	Finalice el diagrama que muestra el estado futuro (destino) de la aplicación. Este diagrama también se utilizará en la InfoSec solicitud.	Especialista en migración, arquitecto de soluciones
Cree solicitudes de servicio de firewall o grupo de seguridad.	Cree solicitudes de servicios de firewall o grupos de seguridad (para desarrollo, control de calidad, preproducción y producción). Si utiliza Cloud Migration Factory, incluya puertos específicos para la replicación si aún no están abiertos.	Especialista en migración, arquitecto de soluciones y líder de redes
Revise las solicitudes de firewall o grupos de seguridad (InfoSec equipo).	En este paso, el InfoSec equipo revisa y aprueba las solicitudes de firewall o grupo de seguridad que se crearon en el paso anterior.	InfoSec ingeniero, especialista en migración
Implemente las solicitudes de grupos de seguridad de firewall (equipo de red).	Una vez que el InfoSec equipo aprueba las solicitudes de firewall, el equipo de red implementa las reglas de firewall de entrada y salida requeridas.	Especialista en migración, arquitecto de soluciones y líder de redes

Fase de construcción (repita para los entornos de desarrollo/control de calidad, preproducción y producción)

Tarea	Descripción	Habilidades requeridas
Importe los datos de la aplicación y del servidor.	1. Compruebe que ha iniciado sesión en el servidor de ejecución de la migración como usuario del dominio con permisos de administrador local en los servidores de origen incluidos en el ámbito de aplicación. 2. Utilice el formulario de admisión de la migración para importar los atributos de los servidores de origen incluidos en el ámbito de aplicación. Para obtener información adicional, consulte la Guía de implementación de Cloud Migration Factory. Si no utiliza Cloud Migration Factory, siga las instrucciones para configurar su herramienta de migración.	Especialista en migración, administrador de la nube
Compruebe los requisitos previos de los servidores de origen.	Conéctese con los servidores de origen incluidos en el ámbito para comprobar los requisitos previos, como el puerto TCP 1500, el puerto TCP 443, el espacio libre del volumen raíz, la versión	Especialista en migración, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	de .NET Framework y otros parámetros. Estos son necesarios para la replicación. Para obtener información adicional, consulte la Guía de implementación de Cloud Migration Factory.	
Cree una solicitud de servicio para instalar agentes de replicación.	Cree una solicitud de servicio para instalar los agentes de replicación en los servidores incluidos para fines de desarrollo, control de calidad, preproducción o producción.	Especialista en migración, administrador de la nube
Instale los agentes de replicación.	Instale los agentes de replicación en los servidores de origen incluidos en los equipos de desarrollo, control de calidad, preproducción o producción. Para obtener información adicional, consulte la Guía de implementación de Cloud Migration Factory.	Especialista en migración, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Inserte los scripts posteriores al lanzamiento.	Application Migration Service admite scripts posteriores al lanzamiento para ayudarlo a automatizar las actividades a nivel del sistema operativo, como la instalación o desinstalación del software después de lanzar las instancias de destino. Este paso envía los scripts posteriores al lanzamiento a equipos Windows o Linux, en función de los servidores identificados para la migración. Para obtener instrucciones, consulte la Guía de implementación de Cloud Migration Factory.	Especialista en migración, administrador de la nube
Verificar el estado de la replicación.	Confirme automáticamente el estado de la replicación de los servidores de origen incluidos en el ámbito de aplicación mediante el script proporcionado. El script se repite cada cinco minutos hasta que el estado de todos los servidores de origen de la oleada en cuestión cambie a Correcto. Para obtener instrucciones, consulte la Guía de implementación de Cloud Migration Factory.	Especialista en migración, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Cree el usuario administrador.	Es posible que se necesite un administrador local o un usuario de sudo en los equipos de origen para solucionar cualquier problema tras la transición de la migración de los servidore s de origen incluidos en el ámbito a AWS. El equipo de migración utiliza este usuario para iniciar sesión en el servidor de destino cuando no se puede acceder al servidor de autenticación (por ejemplo, el servidor DC o LDAP). Para obtener instrucciones para este paso, consulte la Guía de implementación de Cloud Migration Factory.	Especialista en migración, administrador de la nube
Valide la plantilla de lanzamiento.	Valide los metadatos del servidor para asegurarse de que funcionan correctamente y que no contienen datos no válidos. Este paso valida los metadatos de prueba y de transición. Para obtener instrucciones, consulte la Guía de implementación de Cloud Migration Factory.	Especialista en migración, administrador de la nube

Fase de prueba (repita para los entornos de desarrollo/control de calidad, preproducción y producción)

Tarea	Descripción	Habilidades requeridas
Cree una solicitud de servicio.	Cree una solicitud de servicio para que el equipo de infraestructura y otros equipos realicen la transición de las aplicaciones a las instancias de desarrollo, control de calidad, preproducción o producción.	Especialista en migración, administrador de la nube
Configure un equilibrador de carga (opcional).	Configure los equilibradores de carga necesarios, como un Equilibrador de carga de aplicación o un equilibrador de cargas F5 con iRules.	Especialista en migración, administrador de la nube
Inicie instancias para realizar pruebas.	Inicie todos los equipos de destino de una oleada determinada en Application Migration Service en modo de prueba. Para obtener información adicional, consulte la Guía de implementación de Cloud Migration Factory.	Especialista en migración, administrador de la nube
Verifique el estado de la instancia de destino.	Verifique el estado de la instancia de destino comprobando el proceso de arranque de todos los servidores de origen incluidos en la misma oleada. Las instancias de destino pueden tardar hasta 30 minutos en iniciarse. Para comprobar el estado manualmente, inicie	Especialista en migración, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	sesión en la consola Amazon EC2, busque el nombre del servidor de origen y revise la columna Comprobación de estado. Las dos comprobaciones de estado aprobadas indican que la instancia está en buen estado desde el punto de vista de la infraestructura.	
Modifique las entradas de DNS.	Modifique las entradas del sistema de nombres de dominio (DNS). (Utilice `resolv.conf` o `host.conf` para un entorno Microsoft Windows). Configure cada instancia EC2 para que apunte a la nueva dirección IP de este host. Nota: Asegúrese de que no haya conflictos de DNS entre los servidores en las instalaciones y los de la nube de AWS. Este paso y los siguientes son opcionales, según el entorno en el que esté alojado el servidor.	Especialista en migración, administrador de la nube
Pruebe la conectividad con los hosts de backend desde instancias EC2.	Compruebe los inicios de sesión con las credenciales de dominio de los servidores migrados.	Especialista en migración, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Actualice el registro A de DNS.	Actualice el registro A de DNS de cada host para que apunte a la nueva dirección IP privada de Amazon EC2.	Especialista en migración, administrador de la nube
Actualice el registro CNAME de DNS.	Actualice el registro CNAME de DNS para que las IP virtuales (nombres de los equilibradores de carga) apunten al clúster de los servidores web y de aplicaciones.	Especialista en migración, administrador de la nube
Pruebe la aplicación en los entornos aplicables.	Inicie sesión en la nueva instancia de EC2 y pruebe la aplicación en los entornos de desarrollo, control de calidad, preproducción y producción.	Especialista en migración, administrador de la nube
Marque como listo para la transición.	Cuando se hayan completado las pruebas, cambie el estado del servidor de origen para indicar que está listo para la transición, de modo que los usuarios puedan iniciar una instancia de transición. Para obtener instrucciones, consulte la Guía de implementación de Cloud Migration Factory.	Especialista en migración, administrador de la nube

Fase de transición

Tarea	Descripción	Habilidades requeridas
Cree un plan de implement ación de producción.	Cree un plan de implement ación de producción (que incluya un plan de respaldo).	Especialista en migración, administrador de la nube
Notifique al equipo de operaciones sobre el tiempo de inactividad.	Notifique al equipo de operaciones el programa de inactividad de los servidore s. Es posible que algunos equipos necesiten un ticket de solicitud de cambio o de solicitud de servicio (CR/SR) para esta notificación.	Especialista en migración, administrador de la nube
Replique los equipos de producción.	Replique los equipos de producción mediante Applicati on Migration Service u otra herramienta de migración.	Especialista en migración, administrador de la nube
Cierre los servidores de origen incluidos en el ámbito de aplicación.	Tras comprobar el estado de replicación de los servidore s de origen, puede cerrar los servidores de origen para detener las transacciones de las aplicaciones cliente a los servidores. Puede cerrar los servidores de origen en la ventana de transición. Para obtener más información, consulte la Guía de implement ación de Cloud Migration Factory.	Administrador de la nube
Inicie instancias para la transición.	Inicie todos los equipos de destino de una oleada	Especialista en migración, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	determinada en Application Migration Service en modo de transición. Para obtener más información, consulte la Guía de implementación de Cloud Migration Factory.	
Recupere las direcciones IP de las instancias de destino.	Recupere las direcciones IP de las instancias de destino. Si la actualización del DNS es un proceso manual en su entorno, necesitará obtener las nuevas direcciones IP de todas las instancias de destino. Para obtener más información, consulte la Guía de implementación de Cloud Migration Factory.	Especialista en migración, administrador de la nube
Verifique las conexiones del servidor de destino.	Tras actualizar los registros DNS, puede conectarse a las instancias de destino con el nombre de host para comprobar las conexiones. Para obtener más información, consulte la Guía de implementación de Cloud Migration Factory.	Especialista en migración, administrador de la nube

Recursos relacionados

- ¿Cómo migrar?
- Guía de implementación de AWS Cloud Migration Factory
- Automatizar las migraciones de servidores a gran escala con Cloud Migration Factory

- Guía de usuario del servicio de migración de aplicaciones de AWS
- Programa de aceleración de la migración AWS

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Configure una infraestructura Multi-AZ para una FCI Always On de SQL Server mediante Amazon FSx

Creado por Manish Garg (AWS), T.V.R.L.Phani Kumar Dadi (AWS), Nishad Mankar (AWS) y RAJNEESH TYAGI (AWS)

Repositorio de código: - automation aws-windows-failover-cluster	Entorno: PoC o piloto	Origen: Base de datos de Microsoft SQL Server en las instalaciones
Destino: Microsoft SQL Server en EC2	Tipo R: volver a alojar	Carga de trabajo: Microsoft
Tecnologías: migración; infraestructura; DevOps	Servicios de AWS: AWS Managed Microsoft AD; Amazon EC2; Amazon FSx; AWS Systems Manager	

Resumen

Si necesita migrar rápidamente una gran cantidad de instancias de clúster de conmutación por error (FCI) Always On de Microsoft SQL Server, este patrón puede ayudarle a minimizar el tiempo de aprovisionamiento. Al utilizar la automatización y Amazon FSx para Windows File Server, reduce los esfuerzos manuales, los errores cometidos por el hombre y el tiempo necesario para implementar una gran cantidad de clústeres.

Este patrón configura la infraestructura para las FCI de SQL Server en una implementación de zona de disponibilidad múltiple (Multi-AZ) en Amazon Web Services (AWS). El aprovisionamiento de los servicios de AWS necesarios para esta infraestructura se automatiza mediante CloudFormation plantillas de AWS. La instalación de SQL Server y la creación de nodos de clúster en una instancia de Amazon Elastic Compute Cloud (Amazon EC2) se realizan mediante comandos. PowerShell

Esta solución utiliza un sistema de archivos Amazon FSx para Windows Multi-AZ de alta disponibilidad como testigo compartido para almacenar los archivos de la base de datos de SQL Server. El sistema de archivos Amazon FSx y las instancias EC2 de Windows que alojan SQL Server se unen al mismo dominio de AWS Directory Service para Microsoft Active Directory (AWS Managed Microsoft AD).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un usuario de AWS con permisos suficientes para aprovisionar recursos mediante CloudFormation plantillas de AWS
- AWS Directory Service para Microsoft Active Directory
- Credenciales en AWS Secrets Manager para autenticarse en AWS Managed Microsoft AD en un par clave-valor:
  - `ADDomainName`: <Nombre del dominio>
  - `ADDomainJoinUserName`: <Nombre-de-usuario>
  - `ADDomainJoinPassword`: <Domain User Password>
  - `TargetOU`: <Target OU Value>

  Nota: Utilizará el mismo nombre clave en la automatización de AWS Systems Manager para la actividad de unión a AWS Managed Microsoft AD.
- Archivos multimedia de SQL Server para la instalación de SQL Server y la creación de cuentas de servicio o dominio de Windows, que se utilizarán durante la creación del clúster
- Una nube privada virtual (VPC), con dos subredes públicas en zonas de disponibilidad independientes, dos subredes privadas en las zonas de disponibilidad, una puerta de enlace de Internet, puertas de enlace NAT, asociaciones de tablas de enrutamiento y un servidor Jump

Versiones de producto

- Microsoft Windows Server 2012 R2 y Microsoft SQL Server 2016

Arquitectura

Pila de tecnología de origen

- Servidor en las instalaciones de SQL Server con FCI que utilizan una unidad compartida

Pila de tecnología de destino

- Instancias de AWS EC2

- Amazon FSx para Windows File Server
- Manual de procedimiento de Automatización de AWS Systems Manager
- Configuraciones de red (VPC, subredes, puerta de enlace de Internet, puertas de enlace NAT, servidor de salto, grupos de seguridad)
- AWS Secrets Manager
- AWS Managed Microsoft AD
- Amazon EventBridge
- AWS Identity y Access Management (IAM)

Arquitectura de destino

El siguiente diagrama muestra una cuenta de AWS en una sola región de AWS, con una VPC que incluye dos zonas de disponibilidad, dos subredes públicas con puertas de enlace NAT, un servidor de salto en la primera subred pública, dos subredes privadas, cada una con una instancia EC2 para un nodo de SQL Server en un grupo de seguridad de nodos, y un sistema de archivos Amazon FSx que se conecta a cada uno de los nodos de SQL Server. También se incluyen AWS Directory Service EventBridge, Amazon, AWS Secrets Manager y AWS Systems Manager.

Automatizar y escalar

- Puede usar AWS Systems Manager para unirse a AWS Managed Microsoft AD y realizar la instalación de SQL Server.

Herramientas

Servicios de AWS

- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- AWS Directory Service ofrece varias formas de utilizar Microsoft Active Directory (AD) con otros servicios de AWS, como Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Service (Amazon RDS) para SQL Server y Amazon FSx para Windows File Server.
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.

- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, las funciones de Lambda de AWS, los puntos de conexión de invocación HTTP que utilizan destinos de API o los buses de eventos de otras cuentas de AWS.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Secrets Manager le permite reemplazar las credenciales codificadas en el código, incluidas las contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación.
- AWS Systems Manager le permite administrar las aplicaciones y la infraestructura que se ejecutan en la nube de AWS. Simplifica la administración de aplicaciones y recursos, reduce el tiempo requerido para detectar y resolver problemas operativos y ayuda a utilizar y administrar los recursos de AWS a escala de manera segura.

Otras herramientas

- PowerShelles un programa de administración de automatización y configuración de Microsoft que se ejecuta en Windows, Linux y macOS. Este patrón utiliza PowerShell scripts.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub aws-windows-failover-cluster-automation.

Prácticas recomendadas

- Las funciones de IAM que se utilizan para implementar esta solución deben cumplir con el principio de privilegios mínimos. Para obtener más información, consulte la documentación de IAM.
- Siga las prácticas CloudFormation recomendadas de AWS.

Epics

Implementación de la infraestructura

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation pila Systems Manager.	1. Inicie sesión en su cuenta de AWS y abra la consola de administración de AWS. 2. Navegue hasta la CloudFormation consola y cargue la `ssm.yaml` plantilla para crear la CloudFormation pila de Systems Manager. Proporcione valores para los siguientes parámetros: • StateUnJoinAssociationLoggingBucketName— Proporcione un nombre para el depósito de S3 que la plantilla creará con fines de registro. • ssmAssociationAdUnjoinName: proporciona un nombre para el recurso. `AWS::SSM::Association` • SSM AutomationDocumentName: proporcione un nombre para el manual de automatización de Systems Manager.	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	• EventBridgeName— Proporcione un nombre para el bus de EventBrid ge eventos. 3. Implemente la CloudForm ation pila de Systems Manager lanzando la `ssm.yaml` CloudFormation plantilla. La plantilla creará el manual de ejecución de Systems Manager Automation que se iniciará cuando se lance una nueva instancia de EC2 con la etiqueta `ADJoined: FSXADD`. El manual de procedimiento de Automatio n añadirá la instancia al directorio de AWS Managed Microsoft AD.	

Tarea	Descripción	Habilidades requeridas
Implemente la pila de infraestructuras.	Tras la correcta implementación de la pila de Systems Manager, cree la pila `infra`, que incluye los nodos de instancia EC2, los grupos de seguridad, el sistema de archivos Amazon FSx para Windows File Server y el rol de IAM. 1. Navegue hasta la CloudFormation consola e inicie la `infra-cf.yaml` plantilla. Para implementar esta pila, se requieren los siguientes parámetros: • `ActiveDirectoryId` : Identificador de AWS Managed Microsoft AD • `ADDnsIpAddresses1` : Dirección IP DNS principal de AWS Managed Microsoft AD • `ADDnsIpAddresses2` : Dirección IP DNS secundaria de Microsoft AD gestionado por AWS • `FSxSecurityGroupName` : Nombre del grupo de seguridad de Amazon FSx • `FSxWindowsFileSystemName` : Nombre de la unidad Amazon FSx	AWS DevOps, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	• `ImageID`: Identificador de la imagen base de Windows 2012 R2 o Imagen de máquina de Amazon (AMI) utilizada para crear el nodo de instancia de SQL Server • `KeyPairName` : Par clave-valor para adjuntar a los nodos de la instancia EC2 para su acceso • `Node1SecurityGroupName` : Nombre del grupo de seguridad del primer nodo • `Node2SecurityGroupName` : Nombre del grupo de seguridad del segundo nodo • `OUSecretName` : Nombre del secreto que contiene la informaci ón de AWS Managed Microsoft AD • `PrivateSubnet1` : Identificador de la primera subred privada • `PrivateSubnet2` : Identificador de la segunda subred privada • `SqlFSxFCIName` : Nombre de la etiqueta	

Tarea	Descripción	Habilidades requeridas
	aplicada a los nodos principal y secundario y a Amazon FSx. • `SqlFSxServerNetBIOSName1` : Nombre del nodo de la instancia EC2 principal (15 caracteres como máximo) • `SqlFSxServerNetBIOSName2` : Nombre del nodo de la instancia EC2 secundaria (15 caracteres como máximo) • `VPC`: ID de VPC • `WorkloadInstanceType` : tipo de instancia EC2 Implemente la pila de `infra`. La pila creará todos los componentes de infraestructura necesarios para configurar la FCI de Windows SQL Server. 2. Una vez lanzados los nodos de la instancia EC2, se invocará el documento de automatización de Systems Manager para unir estas instancias a AWS Managed Microsoft AD. Puede realizar un seguimiento del progreso en la página Automatiz	

Tarea	Descripción	Habilidades requeridas
	ación de la consola de Systems Manager.	

Configure el Windows SQL Server Always On FCI

Tarea	Descripción	Habilidades requeridas
Instale las herramientas de Windows.	1. Inicie sesión en la instancia EC2 principal, que es el nodo 1. Para instalar las funciones de Windows (Active Directory y FCI Tools), ejecute el siguiente PowerShell script. `Install-WindowsFeature -Name RSAT-AD-Powershell,Failover-Clustering -IncludeManagementTools` `Install-WindowsFeature -Name RSAT-Clustering,RSAT-ADDS-Tools,RSAT-AD-Powershell,RSAT-DHCP,RSAT-DNS-Server` 2. Inicie sesión en la instancia EC2 secundaria, que es el nodo 2, y ejecute el mismo script para habilitar las funciones en el nodo 2.	AWS DevOps, DevOps ingeniero, administrador de bases de datos
Preconfigure los objetos informáticos del clúster en los servicios de dominio de Active Directory.	Para preconfigurar el objeto de nombre de clúster (CNO) en los Servicios de dominio de Active Directory (AD DS)	AWS DevOps, DBA, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
	y preconfigurar un objeto de equipo virtual (VCO) para una función agrupada, siga las instrucciones de Documentación de Windows Server.	

Tarea	Descripción	Habilidades requeridas
Cree el WSFC.	Para crear el Clúster de Conmutación por error de Windows Server (WSFC), haga lo siguiente: 1. Inicie sesión en la instancia EC2 principal, que es el nodo 1. Para crear el recurso compartido de archivos Amazon FSx y conceder acceso total a la cuenta de servicio de AD indicada, ejecute el siguiente código. `Invoke-Command -ComputerName "<FSx Windows Remote PowerShell Endpoint>" -ConfigurationName FSxRemoteAdmin -scriptblock { New-FSxSmbShare -Name "SQLDB" -Path "D:\share" -Description "SQL Databases Share" -ContinuouslyAvailable $true -FolderEnumerationMode AccessBased -EncryptData $true grant-fsxsmbshareaccess -name SQLDB -AccountName "<domain\user>" -accessRight Full }`	AWS DevOps, DBA, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
	Este comando también creará el recurso compartido de archivos disponible de forma continua (CA), que está optimizado para su uso en Microsoft SQL Server. 2. Para crear el clúster de conmutación por error en la instancia principal (nodo 1), ejecute el siguiente comando. `New-Cluster -Name <CNO Name> -Node <Node1 Name>, <Node2 Name> -StaticAddress <Node1 Secondary Private IP>, <Node2 Secondary Private IP>` El comando requiere los siguientes parámetros: • `Name`: el nombre del clúster (CNO) • `Node`: los nombres de los nodos principal y secundario, respectivamente • `StaticAddress` : las direcciones IP secundarias de los nodos principal y secundario, respectivamente	

Tarea	Descripción	Habilidades requeridas
	Importante: Un administrador de dominio o un usuario normal debe tener permiso de administrador en ambos nodos para crear el clúster de conmutación por error de Windows Server (WSFC). De lo contrario, el comando anterior fallará y devolverá el mensaje, `You do not have administrator privilege on servers`. 3. Una vez creado el clúster, ejecute el comando siguiente para adjuntar el testigo del recurso compartido de archivos. `Set-ClusterQuorum -FileShareWitness \ \<FSx Windows Remote PowerShell Endpoint> \share\witness`	

Tarea	Descripción	Habilidades requeridas
Instale el clúster de conmutación por error de SQL Server.	Una vez configurado el clúster de WSFC, instale el clúster de SQL Server en la instancia principal (node1). 1. En la unidad T de ambos nodos, cree carpetas `tempdb` y `log` Las carpetas se utilizan en los PowerShell comandos. 2. Después de copiar los archivos multimedia de SQL Server para la instalación de SQL Server en ambos nodos, ejecute el siguiente PowerShell comando en el nodo 1 para instalar SQL Server en el nodo 1. `D:\setup.exe /Q ` `/ACTION=InstallFailoverCluster ` `/IACCEPTSQLSERVERLICENSETERMS ` `/FEATURES="SQL,IS,BC,Conn" ` `/INSTALLSHAREDDIR="C:\Program Files\Microsoft SQL Server” ` `/INSTALLSHAREDWOWDIR="C:\Program Files (x86)\Microsoft SQL Server" ` `/RSINSTALLMODE="FilesOnlyMode" ` `/INSTANCEID="MSSQLSERVER" `	AWS DevOps, DBA, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
	`/INSTANCENAME="MSSQLSERVER" ` `/FAILOVERCLUSTERGROUP="SQL Server (MSSQLSERVER)" ` `/FAILOVERCLUSTERIPADDRESSES="IPv4;<2nd Sec Private Ip node1>;Cluster Network 1;<subnet mask>" ` `/FAILOVERCLUSTERNETWORKNAME="<Fail over cluster Network Name>" ` `/INSTANCEDIR="C:\Program Files\Microsoft SQL Server" ` `/ENU="True" ` `/ERRORREPORTING=0 ` `/SQMREPORTING=0 ` `/SAPWD="<Domain User password>" ` `/SQLCOLLATION="SQL_Latin1_General_CP1_CI_AS" ` `/SQLSYSADMINACCOUNTS="<domain\username>" ` `/SQLSVCACCOUNT="<domain\username>" /SQLSVCPASSWORD="<Domain User password>" ` `/AGTSVCACCOUNT="<domain\username>" /AGTSVCPASSWORD="<Domain User password>" ` `/ISSVCACCOUNT="<domain\username>" /ISSVCPASSWORD="<Domain User password>" `	

Tarea	Descripción	Habilidades requeridas
	`/FTSVCACCOUNT="NT Service\MSSQLFDLauncher" ` `/INSTALLSQLDATADIR="\\<FSX DNS name>\share\Program Files\Microsoft SQL Server" ` `/SQLUSERDBDIR="\\<FSX DNS name>\share\data" ` `/SQLUSERDBLOGDIR="\\<FSX DNS name>\share\log" ` `/SQLTEMPDBDIR="T:\tempdb" ` `/SQLTEMPDBLOGDIR="T:\log" ` `/SQLBACKUPDIR="\\<FSX DNS name>\share\SQLBackup" ` `/SkipRules=Cluster_VerifyForErrors ` `/INDICATEPROGRESS`	

Tarea	Descripción	Habilidades requeridas
Agregue un nodo secundario al clúster.	Para añadir SQL Server al nodo secundario (nodo 2), ejecute el siguiente PowerShell comando. `D:\setup.exe /Q  ` `/ACTION=AddNode ` `/IACCEPTSQLSERVERLICENSETERMS ` `/INSTANCENAME="MSSQLSERVER"  ` `/FAILOVERCLUSTERGROUP="SQL Server (MSSQLSERVER)" ` `/FAILOVERCLUSTERIPADDRESSES="IPv4;<2nd Sec Private Ip node2>;Cluster Network 2;<subnet mask>" ` `/FAILOVERCLUSTERNETWORKNAME="<Fail over cluster Network Name>" ` `/CONFIRMIPDEPENDENCYCHANGE=1 ` `/SQLSVCACCOUNT="<domain\username>"  /SQLSVCPASSWORD="<Domain User password>" ` `/AGTSVCACCOUNT="domain\username>"  /AGTSVCPASSWORD="<Domain User password>" ` `/FTSVCACCOUNT="NT Service\MSSQLFDLauncher" ` `/SkipRules=Cluster_VerifyForErrors `	AWS DevOps, DBA, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
	`/INDICATEPROGRESS`	
Pruebe la FCI de SQL Server.	1. En la instancia de Windows de uno de los nodos, en Herramientas administrativas, inicie el administrador de Clúster de conmutación por error. 2. Navegue hasta Nodos y confirme que el estado del nodo es Estado en ejecución. 3. Seleccione Roles, abra el menú contextual (haga clic con el botón derecho) de SQL Server (MSSQLSERVER) y seleccione Mover y seleccionar nodo. 4. Tras la selección del nodo, SQL Server debería estar ejecutándose en el otro nodo.	DBA, ingeniero DevOps

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Limpiar recursos.	Para limpiar los recursos, utilice el proceso de eliminación de CloudFormation pilas de AWS: 1. Abra la CloudFormation consola de AWS.	AWS DevOps, DBA, ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
	2. En la página Pilas, seleccione la pila `infra`. La pila se debe estar ejecutando en este momento. 3. En el panel de detalles de la pila, seleccione Delete (Eliminar). 4. Seleccione Delete stack (Eliminar pila) cuando se le indique. 5. Repita los pasos 2 a 4 para la pila de `ssm`. Una vez que se haya completado la eliminación de la pila, la pila estará en el estado `DELETE_COMPLETE` . De forma predeterminada, las pilas en ese `DELETE_COMPLETE` estado no se muestran en la CloudFormation consola. Para mostrar las pilas eliminadas, debe cambiar el filtro de vista de pilas tal y como se describe en Visualización de las pilas eliminadas en la consola de AWS CloudFormation . Si la eliminación ha fallado, la pila tendrá el estado `DELETE_FAILED` . Para obtener información sobre	

Tarea	Descripción	Habilidades requeridas
	las soluciones, consulte los errores al eliminar una pila en la CloudFormation documentación.	

Solución de problemas

Problema	Solución
Error de CloudFormation plantilla de AWS	Si la CloudFormation plantilla falla durante la implementación, haga lo siguiente: 1. Abra la CloudFormation consola de AWS. 2. En la página Stacks de la CloudFormation consola, selecciona la pila. 3. Elija Eventos y compruebe el estado de la pila.
Error de conexión de AWS Managed Microsoft AD	Para solucionar los problemas de unión, siga estos pasos: 1. Abra la consola de Systems Manager. 2. Seleccione la región de implementación. 3. En el panel izquierdo, elija Automatización y localice el manual de procedimientos de automatización fallida. 4. Abra el manual de automatización y compruebe Estado de la ejecución y Pasos de ejecución. 5. Investigue los detalles del paso fallido para ver el error o el fallo exactos.

Recursos relacionados

- Simplificación de las implementaciones de alta disponibilidad de Microsoft SQL Server mediante Amazon FSx para Windows File Server
- Utilización de FSx for Windows File Server con Microsoft SQL Server

Utilice las consultas de BMC Discovery para extraer datos de migración para planificar la migración

Creado por Ben Tailor-Hamblin (AWS), Simon Cunningham (AWS), Emma Baldry (AWS) y Shabnam Khan (AWS)

Entorno: producción	Origen: BMC Discovery	Destino: Plan de migración
Tipo R: volver a alojar	Carga de trabajo: todas las demás cargas de trabajo	Tecnologías: migración; gestión y gobierno; redes; nube híbrida
Servicios de AWS: AWS Migration Hub		

Resumen

Esta guía proporciona ejemplos de consultas y pasos que le ayudarán a extraer datos de su infraestructura y aplicaciones en las instalaciones mediante BMC Discovery. El patrón le muestra cómo utilizar las consultas de BMC Discovery para analizar su infraestructura y extraer información sobre el software, los servicios y las dependencias. Los datos extraídos son necesarios para las fases de evaluación y movilización de una migración a gran escala a la nube de Amazon Web Services (AWS). Puede utilizar estos datos para tomar decisiones críticas sobre qué aplicaciones migrar juntas como parte de su plan de migración.

Requisitos previos y limitaciones

Requisitos previos

- Una licencia para BMC Discovery (anteriormente BMC ADDM) o la versión de software como servicio (SaaS) de BMC Helix Discovery
- Versión en las instalaciones o SaaS de BMC Discovery, instalada (Nota: en el caso de las versiones locales de BMC Discovery, debe instalar la aplicación en una red cliente con acceso a todos los dispositivos de red y servidor que estén listos para la migración entre varios centros de datos. El acceso a la red del cliente debe proporcionarse de acuerdo con las instrucciones de instalación de la aplicación. Si es necesario escanear la información de Windows Server, debe configurar un dispositivo administrador de proxy de Windows en la red.)

- Acceso a la red para permitir que la aplicación escanee dispositivos en todos los centros de datos, si utiliza BMC Helix Discovery

Versiones de producto

- BMC Discovery 22.2 (12.5)
- BMC Discovery 22.1 (12.4)
- BMC Discovery 21.3 (12.3)
- BMC Discovery 21.05 (12.2)
- BMC Discovery 20.08 (12.1)
- BMC Discovery 20.02 (12.0)
- BMC Discovery 11.3
- BMC Discovery 11.2
- BMC Discovery 11.1
- BMC Discovery 11.0
- BMC Atrium Discovery 10.2
- BMC Atrium Discovery 10.1
- BMC Atrium Discovery 10.0

Arquitectura

El siguiente diagrama muestra cómo los administradores de activos pueden utilizar las consultas de BMC Discovery para escanear aplicaciones modeladas por BMC en entornos SaaS y en las instalaciones.

El diagrama muestra el siguiente flujo de trabajo: un administrador de activos utiliza BMC Discovery o BMC Helix Discovery para escanear las instancias de bases de datos y software que se ejecutan en servidores virtuales alojados en varios servidores físicos. La herramienta puede modelar aplicaciones con componentes que abarquen varios servidores físicos y virtuales.

Pila de tecnología

- BMC Discovery

- BMC Helix Discovery

Herramientas

- BMC Discovery es una herramienta de detección de centros de datos que le ayuda a descubrir automáticamente su centro de datos.
- BMC Helix Discovery es un sistema de descubrimiento y modelado de dependencias basado en SaaS que le ayuda a modelar dinámicamente sus activos de datos y sus dependencias.

Prácticas recomendadas

Se recomienda mapear los datos de las aplicaciones, las dependencias y la infraestructura al migrar a la nube. El mapeo le ayuda a comprender la complejidad de su entorno actual y las dependencias entre los distintos componentes.

La información sobre los activos que proporcionan estas consultas es importante por varios motivos:

1. Planificación: comprender las dependencias entre los componentes le ayuda a planificar el proceso de migración de forma más eficaz. Por ejemplo, es posible que primero deba migrar algunos componentes para asegurarse de que otros se puedan migrar correctamente.
2. Evaluación de riesgos: mapear las dependencias entre los componentes puede ayudarle a identificar cualquier riesgo o problema potencial que pueda surgir durante el proceso de migración. Por ejemplo, es posible que descubra que algunos componentes se basan en tecnologías anticuadas o no compatibles, lo que podría provocar problemas en la nube.
3. Arquitectura de nube: mapear los datos de sus aplicaciones e infraestructura también puede ayudarlo a diseñar una arquitectura de nube adecuada que satisfaga las necesidades de su organización. Por ejemplo, es posible que necesite diseñar una arquitectura de varios niveles para cumplir con los requisitos de alta disponibilidad o escalabilidad.

En general, el mapeo de los datos de las aplicaciones, las dependencias y la infraestructura es un paso crucial en el proceso de migración a la nube. El ejercicio de mapeo puede ayudarlo a comprender mejor su entorno actual, identificar cualquier problema o riesgo potencial y diseñar una arquitectura de nube adecuada.

Epics

Identifique y evalúe las herramientas de descubrimiento

Tarea	Descripción	Habilidades requeridas
Identifique a los propietarios de ITSM.	Identifique a los propietarios de la administración de servicios de TI (ITSM) (por lo general, contactando con los equipos de soporte operativo).	Líder de migración
Visitar CMDB.	Identifique el número de bases de datos de administración de la configuración (CMDB) que contienen información sobre los activos y, a continuación, identifique las fuentes de esa información.	Líder de migración
Identifique las herramientas de descubrimiento y compruebe el uso de BMC Discovery.	Si su organización utiliza BMC Discovery para enviar datos sobre su entorno a la herramienta CMDB, compruebe el alcance y la cobertura de sus escaneos. Por ejemplo, compruebe si BMC Discovery escanea todos los centros de datos y si los servidores de acceso están ubicados en zonas perimetrales.	Líder de migración
Compruebe el nivel de modelado de la aplicación.	Compruebe si las aplicaciones están modeladas en BMC Discovery. Si no es así, recomiende utilizar la herramienta BMC Discovery	Ingeniero de migraciones, jefe de migraciones

Tarea	Descripción	Habilidades requeridas
	para modelar qué instancia s de software en ejecución proporcionan una aplicación y un servicio empresarial.	

Extracción de datos de infraestructura

Tarea	Descripción	Habilidades requeridas
Extraiga datos en servidores físicos y virtuales.	Para extraer datos de los servidores físicos y virtuales escaneados por BMC Discovery, utilice Generador de consultas para ejecutar la siguiente consulta: `search Host show key as 'Serverid', virtual, name as 'HOSTNAME', os_type as 'osName', os_version as 'OS Version', num_logical_processors as 'Logical Processor Counts', cores_per_processor as 'Cores per Processor', logical_ram as 'Logical RAM', #Consumer:StorageUse:Provider:DiskDrive.size as 'Size'` Nota: Puede utilizar los datos extraídos para determina	Ingeniero de migraciones, jefe de migraciones

Tarea	Descripción	Habilidades requeridas
	r los tamaños de instancia adecuados para la migración.	
Extraiga datos de aplicaciones modeladas.	Si sus aplicaciones están modeladas en BMC Discovery , puede extraer datos sobre los servidores que ejecutan el software de la aplicación. Para obtener los nombres de los servidores, utilice Generador de consultas para ejecutar la siguiente consulta: `search SoftwareInstance show key as 'ApplicationID', #RunningSoftware:HostedSoftware:Host:Host.key as 'ReferenceID', type, name` Nota: Las aplicaciones se modelan en BMC Discovery mediante un conjunto de instancias de software en ejecución. La aplicación depende de todos los servidores que ejecutan el software de la aplicación.	Propietario de la aplicación BMC Discovery

Tarea	Descripción	Habilidades requeridas
Extraiga datos de bases de datos.	Para obtener una lista de todas las bases de datos escaneadas y los servidores en los que se ejecutan estas bases de datos, utilice Generador de consultas para ejecutar la siguiente consulta: `search Database show key as 'Key', name, type as 'Source Engine Type', #Detail:Detail:ElementWithDetail:SoftwareInstance.name as 'Software Instance', #Detail:Detail:ElementWithDetail:SoftwareInstance.product_version as 'Product Version', #Detail:Detail:ElementWithDetail:SoftwareInstance.edition as 'Edition', #Detail:Detail:ElementWithDetail:SoftwareInstance.#RunningSoftware:HostedSoftware:Host:Host.key as 'ServerID'`	Propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Extraiga datos de la comunicación con el servidor.	Para obtener información sobre todas las comunicaciones de red entre servidores recopilada por BMC Discovery a partir de los registros históricos de comunicaciones de red, utilice Generador de consultas para ejecutar la siguiente consulta: `search Host TRAVERSE InferredElement:Inference:Associate:DiscoveryAccess TRAVERSE DiscoveryAccess:DiscoveryAccessResult:DiscoveryResult:NetworkConnectionList TRAVERSE List:List:Member:DiscoveredNetworkConnection PROCESS WITH networkConnectionInfo`	Propietario de la aplicación BMC Discovery

Tarea	Descripción	Habilidades requeridas
Extraiga datos sobre el descubrimiento de aplicaciones.	Para obtener información sobre las dependencias de las aplicaciones, utilice Generador de consultas para ejecutar la siguiente consulta: `search SoftwareInstance show key as 'SRC App ID', #Dependant:Dependency:DependedUpon:SoftwareInstance.key as 'DEST App ID'`	Propietario de la aplicación BMC Discovery
Extraiga datos sobre servicios empresariales.	Para extraer datos sobre los servicios empresariales proporcionados por los hosts, utilice Generador de consultas para ejecutar la siguiente consulta: `search Host show name, #Host:HostedSoftware:AggregateSoftware:BusinessService.name as 'Name'`	Propietario de la aplicación BMC Discovery

Solución de problemas

Problema	Solución
No se puede ejecutar una consulta o contiene columnas sin rellenar.	Revise los registros de activos de BMC Discovery y determine qué campos necesita. A continuación, sustituya estos campos en la consulta mediante Generador de consultas.

Problema	Solución
Los detalles de un activo dependiente no se rellenan.	Es probable que esto se deba a los permisos de acceso o a la conectividad de la red. Es posible que la herramienta de detección no tenga los permisos necesarios para acceder a determinados activos, especialmente si se encuentran en redes o entornos diferentes. Le recomendamos que colabore estrecham ente con expertos en la materia de descubrim iento para garantizar que se identifiquen todos los activos relevantes.

Recursos relacionados

Referencias

- Derechos de BMC Discovery Licensing (documentación de BMC)
- Características y componentes de BMC Discovery (documentación de BMC)
- Guía del usuario de BMC Discovery (documentación de BMC)
- Búsqueda de datos (en BMC Discovery) (documentación de BMC)
- Descubrimiento y análisis de carteras para la migración (Recomendaciones de AWS)

Tutoriales y vídeos

- BMC Discovery: Seminario web: Mejores prácticas de consulta de informes (parte 1) (YouTube)

Reubicar

Temas

Migración de una base de datos de Amazon RDS para Oracle a otra cuenta y región de AWS mediante AWS DMS para lograr la replicación continua

Creado por Durga Prasad Cheepuri (AWS) y Eduardo Valentim (AWS)

Entorno: PoC o piloto	Origen: bases de datos: relacionales	Destino: Amazon RDS para Oracle
Tipo R: reubicar	Carga de trabajo: Oracle	Tecnologías: migración; bases de datos
Servicios de AWS: Amazon RDS		

Resumen

Advertencia: los usuarios de IAM tienen credenciales de larga duración, lo que supone un riesgo para la seguridad. Para ayudar a mitigar este riesgo, le recomendamos que brinde a estos usuarios únicamente los permisos que necesitan para realizar la tarea y que los elimine cuando ya no los necesiten.

Este patrón le guía por los pasos para migrar una base de datos fuente de Amazon Relational Database Service (Amazon RDS) para Oracle a una y diferente. Cuenta de AWS Región de AWS El patrón utiliza una instantánea de base de datos para una carga completa de datos única y permite AWS Database Migration Service (AWS DMS) la replicación continua.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS que contiene la base de datos Amazon RDS for Oracle de origen, que se ha cifrado con una clave AWS Key Management Service distinta de la predeterminada AWS KMS()
- Un activo Cuenta de AWS en una base de datos Región de AWS diferente a la de origen, para usarlo en la base de datos Amazon RDS for Oracle de destino

- Emparejamiento de nube privada virtual (VPC) entre las VPC de origen y de destino
- Familiaridad con el uso de una base de datos Oracle como fuente de AWS DMS
- Familiaridad con el uso de una base de datos Oracle como destino para AWS DMS

Versiones de producto

- Versiones de Oracle 11g (versiones 11.2.0.3.v1 y posteriores) hasta 12.2, y 18c. Para ver la lista más reciente de versiones y ediciones compatibles, consulte la AWS documentación sobre el uso de una base de datos Oracle como fuente AWS DMS y con el uso de una base de AWS DMS datos Oracle como destino. Para ver las versiones de Oracle compatibles con Amazon RDS, consulte Oracle en Amazon RDS.

Arquitectura

Pilas de tecnología de origen y destino

- Instancia de base de datos de Amazon RDS para Oracle

Arquitectura de replicación continua

Herramientas

Herramientas que se utilizan para cargar todos los datos una sola vez

- Amazon Relational Database Service (Amazon RDS) crea una instantánea del volumen de almacenamiento de la instancia de base de datos y hace copias de seguridad de toda la instancia de base de datos y no solo de bases de datos individuales. Cuando se crea una instantánea de base de datos, se debe identificar la instancia de base de datos cuya copia de seguridad se va a realizar y, a continuación, se debe asignar un nombre a la instantánea de base de datos para poder restaurarla posteriormente. El tiempo que tarda en crearse una instantánea varía en función del tamaño de sus bases de datos. Debido a que la instantánea incluye todo el volumen de almacenamiento, el tamaño de los archivos (por ejemplo, archivos temporales) también afecta la cantidad de tiempo que tarda en crearse la instantánea. Para obtener más información acerca

de la instantáneas de base de datos, consulte crear una instantánea de base de datos en la documentación de Amazon RDS.

- AWS Key Management Service (AWS KMS) crea una clave para el cifrado de Amazon RDS. Al crear una instancia de base de datos cifrada, también puede proporcionar el identificador de AWS KMSclave de su clave de cifrado. Si no especifica un identificador de AWS KMSclave, Amazon RDS utilizará la clave de cifrado predeterminada para la nueva instancia de base de datos. AWS KMScrea la clave de cifrado predeterminada para su. Cuenta de AWS Cuenta de AWS Tiene una clave de cifrado predeterminada diferente para cada uno Región de AWS. Para este patrón, la instancia de base de datos de Amazon RDS debe cifrarse con la clave que no es la predeterminada AWS KMS. Para obtener más información sobre el uso de AWS KMSclaves para el cifrado de Amazon RDS, consulte Cifrar los recursos de Amazon RDS en la documentación de Amazon RDS.

Herramientas utilizadas para la replicación continua

- AWS Database Migration Service (AWS DMS) se utiliza para replicar los cambios en curso y para mantener sincronizadas las bases de datos de origen y destino. Para obtener más información sobre AWS DMS su uso para la replicación continua, consulte Trabajar con una instancia de AWS DMS replicación en la AWS DMS documentación.

Epics

Configure su fuente Cuenta de AWS

Tarea	Descripción	Habilidades requeridas
Prepare la instancia de base de datos de origen.	Ejecute la instancia de base de datos Amazon RDS para Oracle en modo ARCHIVELOG y defina el período de retención. Para obtener más información, consulte Trabajar con una base de datos Oracle AWS gestionada como fuente de AWS DMS.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Configure el registro complementario para la instancia de base de datos de Oracle de origen.	Configure el registro suplementario a nivel de base de datos y de tabla para la instancia de base de datos Amazon RDS for Oracle. Para obtener más información, consulte Trabajar con una base de datos Oracle AWS gestionada como fuente de. AWS DMS	Administrador de base de datos
Actualice la política AWS KMS clave de la cuenta de origen.	Actualice la política de AWS KMS claves en el origen Cuenta de AWS para permitir que el destino Cuenta de AWS utilice la AWS KMS clave cifrada de Amazon RDS. Para obtener más informaci ón, consulte la AWS KMS documentación.	SysAdmin
Cree una instantánea manual de Amazon RDS de la instancia de base de datos de origen.		AWS IAM user
Comparta la instantánea manual y cifrada de Amazon RDS con el objetivo Cuenta de AWS.	Para obtener más informaci ón, consulte Compartir una instantánea de base de datos.	Usuario de AWS IAM

Configure su objetivo Cuenta de AWS

Tarea	Descripción	Habilidades requeridas
Adjunte una política.	En el destino Cuenta de AWS, adjunte una política AWS Identity and Access Management (IAM) al usuario raíz de IAM para que este pueda copiar una instantán ea de base de datos cifrada con la clave compartida. AWS KMS	SysAdmin
Cambie a la fuente. Región de AWS		Usuario de AWS IAM
Copie la instantánea compartida.	En la consola de Amazon RDS, en el panel Instantán eas, elija Shared with Me y seleccione la instantánea compartida. Copie la instantán ea en la Región de AWS misma base de datos de origen utilizando el Amazon Resource Name (ARN) como AWS KMS clave utilizada por la base de datos de origen. Para obtener más información, consulte Copiar una instantán ea de base de datos.	Usuario de AWS IAM
Cambie al destino Región de AWS y cree una AWS KMS clave nueva.		Usuario de AWS IAM
Copie la instantánea.	Cambia a la fuente Región de AWS. En la consola Amazon	Usuario de AWS IAM

Tarea	Descripción	Habilidades requeridas
	RDS, en el panel Instantán eas, elija Owned by Me y seleccione la instantánea copiada. Copie la instantánea en el destino Región de AWS mediante la AWS KMS clave del nuevo objetivo. Región de AWS	
Restaurare la instantánea.	Cambia al objetivo Región de AWS. En la consola Amazon RDS, en el panel Instantán eas, elija Owned by Me. Seleccione la instantánea copiada y restáurela en una instancia de base de datos de Amazon RDS para Oracle. Para obtener más información, consulte Restauración a partir de una instantánea de base de datos.	Usuario de AWS IAM

Prepare la base de datos de origen para la replicación continua

Tarea	Descripción	Habilidades requeridas
Cree un usuario de Oracle con los permisos adecuados.	Cree un usuario de Oracle con los privilegios necesario s para Oracle como fuente de AWS DMS. Para obtener más información, consulte la AWS DMS documentación.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Configure la base de datos de origen para Oracle LogMiner u Oracle Binary Reader.		Administrador de base de datos

Prepare la base de datos de destino para la replicación continua

Tarea	Descripción	Habilidades requeridas
Cree un usuario de Oracle con los permisos adecuados.	Cree un usuario de Oracle con los privilegios necesarios para Oracle como destino AWS DMS. Para obtener más información, consulte la AWS DMS documentación.	Administrador de base de datos

Cree AWS DMS componentes

Tarea	Descripción	Habilidades requeridas
Cree una instancia de replicación en el destino Región de AWS.	Cree una instancia de replicación en la VPC del destino. Región de AWS Para obtener más información, consulte la AWS DMS documentación.	Usuario de AWS IAM
Cree puntos de conexión de origen y destino con el cifrado necesario y pruebe las conexiones.	Para obtener más información, consulte la AWS DMS documentación.	Administrador de base de datos
Cree tareas de replicación.	1. En tipo de migración, seleccione replicación continua.	Usuario de IAM

Tarea	Descripción	Habilidades requeridas
	2. Como punto de partida de captura de datos de cambios (CDC), use el número de cambio del sistema Oracle (SCN) cuando se tomó la instantánea de Amazon RDS para la carga completa, o bien la marca temporal en la que se realizó la carga completa. 3. Para `TargetTablePrepMode`, elija DO_NOTHING. Si la tarea tiene tablas de datos de objetos binarios (LOB) de gran tamaño, elija el modo LOB limitado y establezca el tamaño máximo de LOB en el tamaño máximo de los datos de LOB de la tabla. 4. Habilitar el registro. 5. Agrupe las tablas relacionadas mediante claves en una sola tarea. Si hay tablas con una gran cantidad de datos LOB y sin relación con otras tablas, cree una tarea independiente para ellas con la configuración de LOB descrita anteriormente.	

Tarea	Descripción	Habilidades requeridas
	Para obtener más información, consulte la documentación.AWS DMS	
Inicie las tareas y monitoríc elas.	Para obtener más información, consulte la AWS DMS documentación.	Usuario de AWS IAM
Habilite la validación de la tarea si es necesario.	Tenga en cuenta que habilitar la validación afectará al rendimiento de la replicación. Para obtener más información, consulte la AWS DMS documentación.	Usuario de AWS IAM

Recursos relacionados

- Cambiar una política clave
- Crear una instantánea manual de base de datos de Amazon RDS
- Crear una instantánea manual de base de datos de Amazon RDS
- Copia de una instantánea
- Restauración desde una instantánea de base de datos de Amazon RDS
- Empezando con AWS DMS
- Uso de una base de datos Oracle como fuente para AWS DMS
- Utilizar una base de datos Oracle como destino para AWS DMS
- AWS DMS configuración mediante interconexión de VPC
- ¿Cómo comparto las instantáneas de bases de datos manuales de Amazon RDS o las instantáneas de clústeres de bases de datos con otra persona? Cuenta de AWS (Artículo del centro de conocimientos de AWS)

Migración de VMware SDDC a VMware Cloud en AWS mediante VMware HCX

Creado por Deepak Kumar (AWS)

Entorno: PoC o piloto	Origen: Networking	Destino: VMware Cloud en AWS
Tipo R: reubicar	Tecnologías: migración; infraestructura	

Resumen

Aviso: A partir del 30 de abril de 2024, VMware Cloud on AWS ya no será revendido por AWS sus socios de canal. El servicio seguirá estando disponible a través de Broadcom. Le recomendamos que se ponga en contacto con su AWS representante para obtener más información.

Este patrón describe el uso de VMware Hybrid Cloud Extension (HCX) para migrar las máquinas virtuales (VM) y las aplicaciones en las instalaciones a VMware Cloud on Amazon Web Services (AWS). La migración utiliza el software de centro de datos definido por software (SDDC) de clase empresarial de VMware en la nube de AWS para proporcionar un acceso optimizado a los servicios de AWS.

VMware Cloud en AWS integra los principales productos de virtualización de redes, almacenamiento y computación (vSphere, vSAN y VMware NSX) junto con la administración del servidor VMware vCenter y optimiza estos servicios para que se ejecuten en una infraestructura de AWS elástica y bare metal. La infraestructura resultante es de bajo mantenimiento, simplificada e hiperconvergente.

Con este servicio, los equipos de TI pueden administrar sus recursos basados en la nube con las conocidas herramientas de VMware. Para obtener más información, consulte VMware Cloud en AWS en la web de VMware.

VMware HCX admite tres tipos de migraciones a la nube:

- Hibridez (extensión del centro de datos): amplía un SDDC de VMware en las instalaciones existente a AWS para agrandar el espacio físico, ofrecer capacidad bajo demanda, un entorno de pruebas y desarrollo y escritorios virtuales.
- Evacuación de la nube (actualización de la infraestructura del centro de datos): consolida los centros de datos y pasa por completo a la nube de AWS, (incluyendo la gestión de centros de datos, coubicación o de fin de arrendamiento).
- Especificidades de la aplicación: traslada aplicaciones individuales a la nube de AWS para satisfacer necesidades empresariales específicas.

Requisitos previos y limitaciones

Requisitos previos

- Regístrese para obtener una cuenta de AWS (necesaria para crear el SDDC de VMware Cloud).
- Regístrese para obtener una cuenta de My VMware. Regístrese en https://my.vmware.com/web/vmware/ y rellene todos los campos.
- Compruebe la versión de vCenter y los hosts y recopile la cantidad de máquinas virtuales. Si es posible, solicite una exportación de RVTools para mostrar información sobre sus entornos virtuales. Recomendamos la versión 6.0 o posterior de vCenter.
- Debe implementar conmutadores virtuales distribuidos si quiere ampliar las redes de los centros de datos (L2), probar VMotion mediante HCX o analizar la dependencia de las aplicaciones mediante vRealize Network Insight.
- Elija una red de subred de administración actual en las instalaciones que no entre en conflicto para crear el SDDC en VMware Cloud en AWS.
- Valide los requisitos de HCX consultando los requisitos previos que se proporcionan en la Guía del usuario de HCX de VMware.
- Identifique y agrupe las máquinas virtuales para las ondas de migración. Compruebe si hay máquinas virtuales que pueda utilizar para las pruebas.
- Recopile cualquier dato sobre el consumo relativo de ancho de banda, la compresión de la WAN y la velocidad de transferencia de datos.

Notas

- No es necesario disponer de VMware NSX-V o NSX-T de forma en las instalaciones.

- HCX no tiene costos adicionales (está incluido en VMware Cloud en AWS).

Arquitectura

En el siguiente diagrama, se muestra la solución HCX basada en servicios de varios componentes. Cada componente admite una función específica en la solución HCX. Para obtener más información sobre cada componente de HCX, consulte la entrada del blog Migración de cargas de trabajo a VMware Cloud en AWS con Hybrid Cloud Extension (HCX).

Pila de tecnología de origen

- Máquinas virtuales y aplicaciones en las instalaciones administradas por VMware vSphere

Pila de tecnología de destino

- VMware Cloud en AWS

Herramientas

- VMware HCX: VMware HCX es una herramienta que puede utilizar para migrar sus aplicaciones y cargas de trabajo entre centros de datos y entornos de nube. Se incluye con VMware Cloud en AWS.

Epics

Planificación de la migración

Tarea	Descripción	Habilidades requeridas
Seleccione una estrategia de migración.	Decida si quiere ampliar su centro de datos (hibridez), trasladar todos sus centros de datos (evacuación de la nube) o trasladar aplicaciones específicas a AWS.	SysAdmin, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Valide los requisitos de HCX.	Para obtener información sobre la migración, consulte la Guía del usuario de VMware HCX.	SysAdmin, propietario de la aplicación

Migración a VMware Cloud en AWS

Tarea	Descripción	Habilidades requeridas
Migre sus máquinas virtuales o aplicaciones.	Para obtener más información, consulte Migración híbrida con VMware HCX en la documentación de VMware.	SysAdmin, propietario de la aplicación

Recursos relacionados

- VMware Cloud en AWS: Introducción
- Migración híbrida con VMware HCX
- Guía de usuario de VMware HCX
- Precios de VMware Cloud en AWS
- Hoja de ruta de VMware Cloud en AWS

Migre una instancia de base de datos de Amazon RDS a otra VPC o cuenta

Creado por Dhrubajyoti Mukherjee (AWS)

Entorno: PoC o piloto	Origen: Amazon RDS	Destino: Amazon RDS
Tipo R: reubicar	Tecnologías: migración; bases de datos	Servicios de AWS: Amazon RDS; Amazon VPC

Resumen

Este patrón proporciona una guía para migrar una instancia de base de datos de Amazon Relational Database Service (Amazon RDS) de una nube privada virtual (VPC) a otra en la misma cuenta de AWS, o bien de una cuenta de AWS a otra cuenta de AWS.

Este patrón le resultará útil si desea migrar sus instancias de base de datos de Amazon RDS a otra VPC o cuenta por motivos de seguridad o de separación (por ejemplo, cuando quiere tener la pila de aplicaciones y la base de datos en VPC diferentes).

La migración de una instancia de base de datos a otra cuenta de AWS conlleva ciertos pasos, como tomar una instantánea manual, compartirla y restaurar la instantánea en la cuenta de destino. En función de los cambios en la base de datos y de las tasas de transacción, este proceso puede llevar mucho tiempo. También provoca un tiempo de inactividad en la base de datos, por lo que debe planificar la migración con antelación. Considere una estrategia de implementación azul/verde para minimizar el tiempo de inactividad. Como alternativa, puede evaluar AWS Data Migration Service (AWS DMS) para minimizar el tiempo de inactividad provocado por este cambio. Sin embargo, este patrón no aborda dicha opción. Para obtener más información, consulte la documentación de AWS DMS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Permisos de AWS Identity and Access Management (IAM) para la VPC, las subredes y la consola de Amazon RDS

Limitaciones

- Los cambios en una VPC provocan el reinicio de la base de datos, lo que, a su vez, provoca interrupciones en las aplicaciones. Se recomienda que realice la migración durante las horas de menor actividad.
- Limitaciones al migrar Amazon RDS a otra VPC:
  - La instancia de base de datos a migrar debe ser una instancia única y no estar en espera. No puede formar parte de un clúster.
  - Amazon RDS no debe estar en varias zonas de disponibilidad.
  - Amazon RDS no debe tener réplicas de lectura.
  - El grupo de subredes creado en la VPC de destino debe tener subredes en la zona de disponibilidad en la que se ejecuta la base de datos de origen.
- Limitaciones al migrar Amazon RDS a otra cuenta de AWS:
  - Actualmente no es posible compartir instantáneas cifradas con la clave de servicio predeterminada de Amazon RDS.

Arquitectura

Migración a una VPC en la misma cuenta de AWS

El siguiente diagrama muestra el flujo de trabajo para migrar una instancia de base de datos de Amazon RDS a una VPC diferente en la misma cuenta de AWS.

Los pasos son los siguientes. Consulte la sección Epics para obtener instrucciones detalladas.

1. Cree un grupo de subredes de base de datos en la VPC de destino. Un grupo de subredes de base de datos es una colección de subredes que se permiten especificar una VPC concreta al crear instancias de base de datos.
2. Configure la instancia de base de datos de Amazon RDS en la VPC de origen para usar el nuevo grupo de subredes de base de datos.
3. Aplique los cambios para migrar la base de datos de Amazon RDS a la VPC de destino.

Migración a otra cuenta de AWS

El siguiente diagrama muestra el flujo de trabajo para migrar una instancia de base de datos de Amazon RDS a una cuenta diferente de AWS.

Los pasos son los siguientes. Consulte la sección Epics para obtener instrucciones detalladas.

1. Acceda a la instancia de base de datos de Amazon RDS en la cuenta de AWS de origen.
2. Cree una instantánea de Amazon RDS en la cuenta de AWS de origen.
3. Comparta la instantánea de Amazon RDS con la cuenta de AWS de destino.
4. Acceda a la instantánea de Amazon RDS en la cuenta de AWS de destino.
5. Cree una instancia de base de datos de Amazon RDS en la cuenta de AWS de destino.

Herramientas

Servicios de AWS

- Amazon Relational Database Service (Amazon RDS) le ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS.
- Amazon Virtual Private Cloud (Amazon VPC) ayuda a lanzar recursos de AWS en una red virtual que se haya definido. Esa red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Prácticas recomendadas

- Si el tiempo de inactividad de la base de datos al migrar una instancia de base de datos de Amazon RDS a otra cuenta le resulta un problema, le recomendamos que use AWS DMS. La replicación de datos proporcionada por este servicio le permite reducir la interrupción a menos de cinco minutos.

Epics

Migre a una VPC diferente en la misma cuenta de AWS

Tarea	Descripción	Habilidades requeridas
Cree una nueva VPC.	En la consola de Amazon VPC, cree una nueva VPC y subredes con las propiedad es y los rangos de direccion es IP deseados. Para obtener instrucciones detalladas, consulte la documentación de Amazon VPC.	Administrador
Creación de un grupo de subredes de base de datos.	Abra la consola de Amazon RDS: 1. Seleccione Grupos de subredes y, a continuación, Crear grupo de subredes de base de datos. 2. Introduzca el nombre, la descripción y la ID de VPC del grupo de subredes. 3. Agregue las subredes que pertenecen al grupo de subredes. Agregue subredes para cubrir, al menos, dos zonas de disponibilidad. 4. Seleccione Crear. Para obtener más información, consulte la documentación de Amazon RDS.	Administrador

Tarea	Descripción	Habilidades requeridas
Modifique la instancia de base de datos de Amazon RDS para usar el nuevo grupo de subredes.	Abra la consola de Amazon RDS: 1. En el panel de navegación, seleccione Bases de datos y, a continuación, el nombre de la instancia de base de datos de Amazon RDS que va a migrar. 2. En la sección Conectividad, elija el grupo de subredes asociado a la VPC de destino. 3. En la sección Programación de modificaciones, seleccione Aplicar inmediatamente. Cuando se completa la migración a la VPC de destino, el grupo de seguridad predeterminado de la VPC de destino se asigna a la instancia de base de datos de Amazon RDS. Puede configurar un nuevo grupo de seguridad para esa VPC con las reglas de entrada y salida necesarias para su instancia de base de datos. También puede usar la interfaz de la línea de comandos de AWS (AWS CLI)	Administrador

Tarea	Descripción	Habilidades requeridas
	para realizar la migración a la VPC de destino proporcionando explícitamente la ID del nuevo grupo de seguridad de la VPC. Por ejemplo: `aws rds modify-db-instance \ --db-instance-identifier testrds \ --db-subnet-group-name new-vpc-subnet-group \ --vpc-security-group-ids sg-idxxxx \ --apply-immediately`	

Migrar a una cuenta de AWS diferente

Tarea	Descripción	Habilidades requeridas
Cree una nueva VPC y un grupo de subredes en la cuenta de AWS de destino.	1. En la consola de Amazon VPC, cree una nueva VPC y subredes con las propiedades y los rangos de direcciones IP deseados. Para obtener instrucciones detalladas, consulte la documentación de Amazon VPC. 2. Cree subredes para la nueva VPC siguiendo las instrucciones de la	Administrador

Tarea	Descripción	Habilidades requeridas
	documentación de Amazon VPC. 3. En la consola de Amazon RDS, cree grupos de subredes de base de datos. Para obtener instrucciones, consulte la documentación de Amazon RDS.	
Cree una instantánea manual de la base de datos y compártala con la cuenta de destino.	1. Realice una instantánea manual de la base de datos de origen siguiendo las instrucciones de la documentación de Amazon RDS. 2. Comparta la instantánea con la cuenta de AWS de destino proporcionando la ID de la cuenta de destino. Para obtener más instrucciones, consulte el artículo de Re:post sobre cómo compartir instantáneas de bases de datos con otras cuentas.	Administrador
Lance una nueva instancia de base de datos en Amazon RDS.	Lance una nueva instancia de base de datos de Amazon RDS a partir de la instantánea compartida en la cuenta de AWS de destino. Para obtener instrucciones, consulte la documentación de Amazon RDS.	Administrador

Recursos relacionados

- Documentación de Amazon RDS
- Documentación de Amazon RDS
- ¿Cómo cambio la VPC de una instancia de base de datos de Amazon RDS? (artículo de AWS Re:post)
- ¿Cómo transfiero la propiedad de los recursos de Amazon RDS a otra cuenta de AWS? (artículo de AWS Re:post)
- ¿Cómo comparto las instantáneas manuales de bases de datos de Amazon RDS o las instantáneas del clúster de base de datos Aurora con otra cuenta de AWS? (artículo de AWS Re:post)
- Documentación de AWS DMS

Migre una instancia de base de datos de Amazon RDS para Oracle a otra VPC

Documento creado por Pinesh Singal (AWS)

Entorno: PoC o piloto	Origen: bases de datos: relacionales	Destino: Amazon RDS para Oracle
Tipo R: reubicar	Carga de trabajo: Oracle	Tecnologías: migración; bases de datos
Servicios de AWS: Amazon RDS		

Resumen

Este patrón de migración proporciona step-by-step orientación para migrar una instancia de base de datos (DB) de Amazon Relational Database Service (Amazon RDS) para Oracle desde una nube privada virtual (VPC) a otra VPC en la misma cuenta de Amazon Web Services (AWS). Por ejemplo, puede usar este patrón si su empresa necesita que la base de datos y el servidor de aplicaciones de Amazon Elastic Compute Cloud (Amazon EC2) se encuentren en la misma VPC.

El patrón describe una estrategia de migración en línea con poco o ningún tiempo de inactividad para una base de datos de origen Oracle de varios terabytes con un número elevado de transacciones.

Para mover una instancia de base de datos de Amazon RDS para Oracle a otra VPC, debe cambiar el grupo de subredes de Amazon RDS. Este grupo de subredes deberá estar preconfigurado con la nueva VPC y las subredes requeridas. Durante el cambio de la VPC de una red a otra, la instancia de Amazon RDS se reiniciará, por lo que no será posible acceder a la base de datos durante el traslado.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Dos VPC con subredes privadas

- Una instancia de base de datos de Amazon RDS para Oracle (en funcionamiento), configurada con grupos de seguridad entrantes y salientes

Limitaciones

- El patrón no es compatible con instancias de base de datos que abarquen varias zonas de disponibilidad (Multi-AZ). Sin embargo, este patrón proporciona una forma de evitar esta limitación.
- La instancia de base de datos no se puede migrar mientras la réplica de lectura esté activada.
- El grupo de subredes de la nueva VPC debe estar en la misma zona de disponibilidad que la base de datos.
- La migración debe realizarse durante un período de mantenimiento programado o en momentos de poco tráfico; al trasladar la base de datos a otra VPC se reinicia la base de datos, lo que provoca la interrupción de la aplicación durante unos minutos.

Versiones de producto

- Instancia de base de datos de Amazon RDS para Oracle versión 12.1.0.2 y posterior

Arquitectura

Pila de tecnología de origen

- Instancia de base de datos de Amazon RDS para Oracle 12.1.0.2.v22 en una VPC
- Una VPC configurada en una tabla de enrutamiento independiente
- Grupos de subredes de Amazon RDS configurados en una VPC
- Grupo de opciones de Amazon RDS (si es necesario)

Pila de tecnología de destino

- Una instancia de base de datos de Amazon RDS para Oracle con la versión 12.1.0.2.v22 en otra VPC
- VPC de Amazon configurada en una ruta independiente
- Grupos de subredes de Amazon RDS configurados en una nueva VPC
- Grupo de opciones de Amazon RDS (si es necesario)

Arquitectura de origen y destino

En el siguiente diagrama se muestra el uso de la consola para trasladar Amazon RDS para Oracle DB de una subred privada de una VPC a una subred privada de otra VPC diferente.

1. Use la consola para modificar la instancia de base de datos de Amazon RDS para Oracle de origen.
2. En la VPC de destino, modifique el grupo de subredes y modifique el grupo de opciones, si lo utiliza.

Herramientas

- Amazon RDS: Amazon Relational Database Service (Amazon RDS) es un servicio web que facilita la configuración, el funcionamiento y el escalado de una base de datos relacional en la nube de AWS. Proporciona una capacidad rentable y de tamaño ajustable para una base de datos relacional y se ocupa de las tareas de administración de bases de datos comunes. Este patrón utiliza Amazon RDS para Oracle.

Epics

Cambie la configuración de la base de datos de Amazon RDS para Oracle en la VPC existente

Tarea	Descripción	Habilidades requeridas
Crear un grupo de subredes.	Configure un grupo de subredes en Amazon RDS.	AWS general
Cree un grupo de opciones.	(Opcional) Configure un grupo de opciones en Amazon RDS.	AWS general
Modifique la instancia de base de datos de RDS para Oracle.	Modifique la base de datos con el grupo de subredes y el grupo de opciones.	AWS general, administrador de bases de datos
Actualice la base de datos de Oracle, si es necesario.	Para migrar la base de datos de Amazon RDS para Oracle	AWS general

Tarea	Descripción	Habilidades requeridas
	de origen, realice los siguientes cambios: • Elimine las réplicas de lectura, si existen. • Desactive la función Multi-AZ, si está activada.	

Configure la base de datos de Amazon RDS para Oracle en la VPC de destino

Tarea	Descripción	Habilidades requeridas
Crear un grupo de subredes.	En Amazon RDS, configure un grupo de subredes mediante la subred de la nueva VPC y la zona de disponibilidad de la base de datos.	AWS general
Cree un grupo de opciones.	(Opcional) Configure un grupo de opciones en Amazon RDS.	AWS general
Modificar la base de datos de Amazon RDS para Oracle.	Modifique la base de datos con un nuevo grupo de subredes y grupo de opciones de la nueva VPC. Puede aplicar estos cambios de inmediato o en un período de mantenimiento. El proceso puede tardar varios minutos en completarse. Durante la modificación, verá los siguientes cambios de estado: • moving-to-vpc	AWS general, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	• C onfiguring-enhanced-monitoring • Modificar • Disponible La modificación adjuntará el grupo de seguridad predeterminado de la nueva VPC. Adjunte un nuevo grupo de seguridad en función de las necesidades de Amazon RDS para Oracle.	
Actualice la base de datos de Amazon RDS para Oracle, si es necesario.	Tras migrar a la base de datos de Amazon RDS para Oracle de destino en la nueva VPC, realice las siguientes modificaciones, si es necesario: • Active las réplicas de lectura, si existían en la base de datos de origen. • Active la función Multi-AZ, si estaba activada en la base de datos de origen.	AWS general

Tarea	Descripción	Habilidades requeridas
Pruebe la conectividad de la aplicación.	Realice una prueba de conectividad de base de datos desde cualquier aplicación. Confirme que la base de datos de Amazon RDS para Oracle modificada de la nueva VPC esté conectada y se pueda acceder a ella desde la aplicación.	Propietario de la aplicación

Recursos relacionados

- Documentación de Amazon VPC
- VPC y subredes
- Uso de una instancia de base de datos en una VPC
- Documentación de Amazon RDS
- Oracle en Amazon RDS
- Consola de Amazon RDS
- ¿Cómo cambio la VPC de una instancia de base de datos de Amazon RDS?

Migre un clúster de Amazon Redshift a una región de AWS en China

Creado por Jing Yan (AWS)

Tipo R: reubicar	Entorno: producción	Tecnologías: bases de datos; migración
Carga de trabajo: todas las demás cargas de trabajo	Servicios de AWS: Amazon Redshift	Origen: AWS Redshift
Destino: Redshift		

Resumen

Este patrón proporciona un step-by-step enfoque para migrar un clúster de Amazon Redshift a una región de AWS en China desde otra región de AWS.

Este patrón emplea comandos SQL para recrear todos los objetos de base de datos, y usa el comando UNLOAD para mover estos datos de Amazon Redshift a un bucket de Amazon Simple Storage Service (Amazon S3) en la región de origen. A continuación, los datos se migran a un bucket de S3 en la región de AWS en China. El comando COPY carga datos del bucket de S3 y los transfiere al clúster de Amazon Redshift de destino.

Actualmente, Amazon Redshift no admite características entre regiones, como la copia de instantáneas en regiones de AWS en China. Este patrón proporciona una forma de evitar esta limitación. También puede invertir los pasos de este patrón para migrar datos de una región de AWS en China a otra región de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Cuentas de AWS activas, tanto en una región de China como en una región de AWS fuera de China
- Clústeres de Amazon Redshift existentes, tanto en una región de China como en una región de AWS fuera de China

Limitaciones

- Esta es una migración sin conexión, por lo que el clúster de Amazon Redshift de origen no podrá realizar operaciones de escritura durante la migración.

Arquitectura

Pila de tecnología de origen

- Clúster de Amazon Redshift en una región de AWS fuera de China

Pila de tecnología de destino

- Clúster de Amazon Redshift en una región de AWS en China

Arquitectura de destino

Herramientas

Herramientas

- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos que ofrece escalabilidad, disponibilidad de datos, seguridad y resultados. Puede usar Amazon S3 para almacenar datos de Amazon Redshift y copiar datos de un bucket de S3 a Amazon Redshift.
- Amazon Redshift: Amazon Redshift es un servicio de almacenamiento de datos de varios petabytes totalmente administrado en la nube.
- psql: psql es una interfaz de PostgreSQL basada en terminal.

Epics

Prepare la migración en la región de origen

Tarea	Descripción	Habilidades requeridas
Lance y configure una instancia de EC2 en la región de origen.	Inicie sesión en la consola de administración de AWS y abra la consola de Amazon	Administrador de base de datos, desarrollador

Tarea	Descripción	Habilidades requeridas
	Elastic Compute Cloud (Amazon EC2). En la barra de navegación de la parte superior de la pantalla, se muestra la región actual. Esta región no puede ser una región de AWS en China. En el panel de la consola de Amazon EC2, seleccione “Lanzar instancia ” y cree y configure una instancia de EC2. Importante: asegúrese de que sus grupos de seguridad de EC2 para reglas de entrada permitan el acceso sin restricciones al puerto TCP 22 desde su máquina de origen. Para obtener más instrucciones sobre cómo lanzar y configura r una instancia de EC2, consulte la sección “Recursos relacionados”.	
Instale la herramienta psql.	Descargue e instale PostgreSQL. Amazon Redshift no proporciona la herramien ta psql. Esta se instala con PostgreSQL. Para obtener más información sobre el uso de psql y la instalación de las herramientas de PostgreSQL, consulte la sección “Recursos relacionados”.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Registre los detalles del clúster de Amazon Redshift.	En el panel de navegación de la consola de Amazon Redshift, seleccione “Clústeres”. A continuación, seleccione el nombre del clúster de Amazon Redshift de la lista. En la pestaña “Propiedades”, en la sección “Configuración de la base de datos”, registre el “Nombre de la base de datos” y “Puerto”. Abra la sección “Detalles de conexión” y registre el “Punto de conexión”, en el formato: <port>/<databasename>”. Importante: asegúrese de que sus grupos de seguridad de Amazon Redshift para reglas de entrada permitan el acceso sin restricciones al puerto TCP 5439 desde su instancia de EC2.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Conecte psql al clúster de Amazon Redshift.	En una línea de comandos, especifique la información de conexión ejecutando el comando “psql -h <endpoint > -U <userid> -d <database name> -p <port>”. Cuando se le solicite la contraseña de psql, introduzca la contraseña del usuario “<userid>”. Estará entonces conectado al clúster de Amazon Redshift y puede ingresar comandos de forma interactiva.	Administrador de base de datos
Crear un bucket de S3.	Abra la consola de Amazon S3 y cree un bucket de S3 que contenga los archivos exportados desde Amazon Redshift. Para obtener más instrucciones sobre cómo crear un bucket de S3, consulte la sección “Recursos relacionados”.	Administrador de base de datos, AWS general

Tarea	Descripción	Habilidades requeridas
Cree una política de IAM que permita descargar datos.	Abra la consola de AWS Identity and Access Management (IAM) y seleccione “Políticas”. Seleccione “Crear política” y, a continuación, la pestaña “JSON”. Copie y pegue la política de IAM para descargar datos de la sección “Informac ión adicional”. Importante: sustituya “s3_bucket_name” por el nombre de su bucket de S3. Seleccione “Revisar política”, e introduzca un nombre y una descripción para la política. Seleccione “Crear política”.	Administrador de base de datos
Cree un rol de IAM que permita la operación UNLOAD en Amazon Redshift.	Abra la consola de IAM y seleccione “Roles”. Seleccion e “Crear rol” y elija “Servicio de AWS” en “Seleccione el tipo de entidad de confianza ”. Elija “Redshift” en el servicio, seleccione “Redshift - Personalizable” y, a continuac ión, elija “Siguiente”. Elija la política de “Descarga” que creó anteriormente y seleccion e “Siguiente”. Introduzca un “nombre de rol”, y seleccione “Crear rol”.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Asociar un rol de IAM al clúster de Amazon Redshift.	Abra la consola de Amazon Redshift y elija “Administrar roles de IAM”. Elija “Roles disponibles” en el menú desplegable y seleccione el rol que creó anteriormente. Seleccione “Aplicar cambios”. Cuando el “Estado” del rol de IAM en la sección “Administrar roles de IAM” aparezca como “Sincronizado”, puede ejecutar el comando UNLOAD.	Administrador de base de datos
Detenga las operaciones de escritura en el clúster de Amazon Redshift.	Recuerde detener todas las operaciones de escritura en el clúster de Amazon Redshift de origen hasta que se complete la migración.	Administrador de base de datos

Preparar la migración en la región de destino

Tarea	Descripción	Habilidades requeridas
Lance y configure una instancia de EC2 en la región de destino.	Inicie sesión en la consola de administración de AWS de una región de China, ya sea Pekín o Ningxia. En la consola de Amazon EC2, seleccione “Lanzar instancia ” y cree y configure una instancia de EC2. Importante: asegúrese de que sus grupos de seguridad de EC2 para reglas de entrada permitan	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	el acceso sin restricciones al puerto TCP 22 desde su máquina de origen. Para obtener más instrucciones sobre cómo lanzar y configura r una instancia de EC2, consulte la sección “Recursos relacionados”.	
Registre los detalles del clúster de Amazon Redshift.	En el panel de navegació n de la consola de Amazon Redshift, seleccione “Clústere s”. A continuación, seleccion e el nombre del clúster de Amazon Redshift de la lista. En la pestaña “Propieda des”, en la sección “Configur ación de la base de datos”, registre el “Nombre de la base de datos” y “Puerto”. Abra la sección “Detalles de conexión” y registre el “Punto de conexión”, en el formato: <port>/<databasename>”. Importante: asegúrese de que sus grupos de seguridad de Amazon Redshift para reglas de entrada permitan el acceso sin restricciones al puerto TCP 5439 desde su instancia de EC2.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Conecte psql al clúster de Amazon Redshift.	En una línea de comandos, especifique la información de conexión ejecutando el comando “psql -h <endpoint > -U <userid> -d <database name> -p <port>”. Cuando se le solicite la contraseña de psql, introduzca la contraseña del usuario “<userid>”. Estará entonces conectado al clúster de Amazon Redshift y puede ingresar comandos de forma interactiva.	Administrador de base de datos
Crear un bucket de S3.	Abra la consola de Amazon S3 y cree un bucket de S3 que contenga los archivos exportados desde Amazon Redshift. Para obtener más información sobre esta y otras explicaciones, consulte la sección “Recursos relaciona dos”.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree una política de IAM que permita copiar datos.	Abra la consola de IAM y seleccione “Políticas”. Seleccione “Crear política” y, a continuación, la pestaña “JSON”. Copie y pegue la política de IqAM para descargar datos de la sección “Información adicional ”. Importante: sustituya “s3_bucket_name” por el nombre de su bucket de S3. Seleccione “Revisar política”, e introduzca un nombre y una descripción para la política. Seleccione “Crear política”.	Administrador de base de datos
Cree un rol de IAM que permita la operación COPIAR en Amazon Redshift.	Abra la consola de IAM y seleccione “Roles”. Seleccion e “Crear rol” y elija “Servicio de AWS” en “Seleccione el tipo de entidad de confianza ”. Elija “Redshift” en el servicio, seleccione “Redshift - Personalizable” y, a continuac ión, elija “Siguiente”. Elija la política “Copiar” que creó anteriormente y seleccion e “Siguiente”. Introduzca un “nombre de rol”, y seleccione “Crear rol”.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Asociar un rol de IAM al clúster de Amazon Redshift.	Abra la consola de Amazon Redshift y elija “Administrar roles de IAM”. Elija “Roles disponibles” en el menú desplegable y seleccione el rol que creó anteriormente. Seleccione “Aplicar cambios”. Cuando el “Estado” del rol de IAM en la sección “Administrar roles de IAM” aparezca como “Sincronizado”, puede ejecutar el comando “COPIAR”.	Administrador de base de datos

Compruebe los datos de origen y la información de objeto antes de iniciar la migración

Tarea	Descripción	Habilidades requeridas
Compruebe las filas de las tablas de Amazon Redshift de origen.	Use los scripts de la sección “Información adicional” para verificar y registrar el número de filas de las tablas de Amazon Redshift de origen. Recuerde dividir los datos equitativamente para los scripts UNLOAD y COPY. Esto mejorará la eficiencia de la descarga y carga de datos, ya que la cantidad de datos incluida en cada script estará equilibrada.	Administrador de base de datos
Compruebe el número de objetos de base de datos en el	Use los scripts de la sección “Información adicional” para verificar y registrar el número	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
clúster de Amazon Redshift de origen.	de bases de datos, usuarios, esquemas, tablas, vistas y funciones definidas por el usuario (UDF) en el clúster de Amazon Redshift de origen.	
Compruebe los resultados de las instrucciones SQL antes de la migración.	Algunas instrucciones SQL de validación de datos deben clasificarse de acuerdo con las situaciones empresariales y de datos reales. Este paso verificará los datos importado s y garantizará que sean coherentes y se muestren correctamente.	Administrador de base de datos

Migre datos y objetos a la región de destino

Tarea	Descripción	Habilidades requeridas
Genere scripts DDL de Amazon Redshift.	Genere scripts de lenguaje de definición de datos (DDL) mediante los enlaces de la sección “Instrucciones de SQL para consultas en Amazon Redshift” en la sección “Información adicional ”. Estos scripts de DDL deben incluir las consultas “crear usuario”, “crear esquema”, “privilegios del usuario sobre el esquema”, “crear tabla/vis ta”, “privilegios del usuario	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	sobre los objetos” y “crear función”.	
Cree objetos en el clúster de Amazon Redshift para la región de destino.	Ejecute los scripts de DDL usando la Interfaz de la línea de comandos de AWS (AWS CLI) en la región de AWS en China. Estos guiones crean objetos en el clúster de Amazon Redshift para la región de destino.	Administrador de base de datos
Descargue los datos de origen del clúster de Amazon Redshift en el bucket de S3.	Ejecute el comando UNLOAD para descargar los datos del clúster de Amazon Redshift de la región de origen al bucket de S3.	Administrador de base de datos, desarrollador
Transfiera los datos del bucket de la región S3 de origen al bucket de la región S3 de destino.	Transfiera los datos del bucket de la región S3 de origen al bucket de la región S3 de destino. Ya que no se puede usar el comando “$ aws s3 sync”, asegúrese de seguir el proceso descrito en el artículo “Transferir datos de Amazon S3 de regiones de AWS a regiones de AWS en China” de la sección “Recursos relacionados”.	Desarrollador

Tarea	Descripción	Habilidades requeridas
Cargue los datos en el clúster de Amazon Redshift de destino.	En la herramienta psql de la región de destino, ejecute el comando COPY para cargar los datos del bucket de S3 al clúster de Amazon Redshift de destino.	Administrador de base de datos

Verifique los datos en las regiones de origen y destino tras la migración

Tarea	Descripción	Habilidades requeridas
Verifique y compare el número de filas en las tablas de origen y destino.	Verifique y compare el número de filas en las tablas de origen y destino de las regiones para asegurarse de que todas han migrado.	Administrador de base de datos
Verifique y compare el número de objetos en las bases de datos de origen y destino.	Verifique y compare todos los objetos de la base de datos en las regiones de origen y destino para asegurarse de que todos se hayan migrado.	Administrador de base de datos
Verifique y compare los resultados de los scripts SQL en las regiones de origen y destino.	Ejecute los scripts SQL preparados antes de la migración. Verifique y compare los datos para asegurarse de que los resultados de SQL sean correctos.	Administrador de base de datos
Restablezca las contraseñ as de todos los usuarios del clúster de Amazon Redshift de destino.	Una vez finalizada la migración y verificados todos los datos, debe restablec er todas las contraseñas de	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	usuario del clúster de Amazon Redshift en la región de AWS en China.	

Recursos relacionados

- Transferir datos de Amazon S3 de regiones de AWS a regiones de AWS en China
- Creating an S3 bucket (Crear un bucket de S3)
- Restablecer una contraseña de usuario de Amazon Redshift
- Documentación de psql

Información adicional

Política de IAM para descargar datos

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::s3_bucket_name"]
    },
    {
      "Effect": "Allow",
      "Action": ["s3:GetObject", "s3:DeleteObject"],
      "Resource": ["arn:aws:s3:::s3_bucket_name/*"]
    }
  ]
}
```

Política de IAM para copiar datos

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::s3_bucket_name"]
    },
    {
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
      "Resource": ["arn:aws:s3:::s3_bucket_name/*"]
    }
  ]
}
```

Instrucciones de SQL para consultas en Amazon Redshift

```
##Database

select * from pg_database where datdba>1;

##User

select * from pg_user where usesysid>1;

##Schema

SELECT n.nspname AS "Name",

  pg_catalog.pg_get_userbyid(n.nspowner) AS "Owner"

FROM pg_catalog.pg_namespace n

WHERE n.nspname !~ '^pg_' AND n.nspname <> 'information_schema'

ORDER BY 1;

##Table

select count(*) from pg_tables where schemaname not in
 ('pg_catalog','information_schema');

select schemaname,count(*) from pg_tables where schemaname not in
 ('pg_catalog','information_schema') group by schemaname order by 1;

##View
```

```
SELECT

    n.nspname AS schemaname,c.relname AS
 viewname,pg_catalog.pg_get_userbyid(c.relowner) as "Owner"

FROM

    pg_catalog.pg_class AS c

INNER JOIN

    pg_catalog.pg_namespace AS n

    ON c.relnamespace = n.oid

WHERE relkind = 'v' and n.nspname not in ('information_schema','pg_catalog');

##UDF

SELECT

   n.nspname AS schemaname,

   p.proname AS proname,

   pg_catalog.pg_get_userbyid(p.proowner) as "Owner"

FROM pg_proc p

LEFT JOIN pg_namespace n on n.oid = p.pronamespace

WHERE p.proowner != 1;
```

Secuencias de comandos SQL para generar sentencias DDL

- Script Get_schema_priv_by_user
- Script Generate_tbl_ddl
- Generate_view_ddl
- Generate_user_grant_revoke_ddl
- Generate_udf_ddl

Migración de las cargas de trabajo a VMware Cloud en AWS mediante VMware HCX

Creado por Deepak Kumar (AWS), Derek Cox (AWS) e Himanshu Gupta (AWS)

Entorno: producción	Origen: cargas de trabajo de VMware en las instalaciones	Destino: VMware Cloud en AWS
Tipo R: reubicar	Carga de trabajo: todas las demás cargas de trabajo	Tecnologías: migración; nube híbrida
Servicios de AWS: VMware Cloud en AWS; Amazon VPC		

Resumen

Aviso: A partir del 30 de abril de 2024, VMware Cloud on ya no será revendido por AWS sus socios de canal. AWS El servicio seguirá estando disponible a través de Broadcom. Le recomendamos que se ponga en contacto con su AWS representante para obtener más informaci ón.

Este patrón explica cómo puede utilizar VMware Hybrid Cloud Extension (HCX) para migrar las cargas de trabajo de su entorno VMware en las instalaciones a VMware Cloud en AWS sin cambiar la plataforma subyacente. VMware HCX agiliza la migración, ayuda a reequilibrar las cargas de trabajo, ayuda a proteger los datos y optimiza los procesos de recuperación de desastres tanto para los centros de datos en las instalaciones como para los servidores en la nube. El patrón describe los pasos para instalar, configurar, actualizar y desinstalar HCX.

HCX admite lo siguiente:

- Versiones anteriores de VMware vSphere: HCX ayuda a migrar máquinas virtuales (VM) de versiones anteriores de vSphere a VMware Cloud en AWS. Los hosts se actualizan y reparan automáticamente para eliminar las laboriosas actualizaciones de preparación de la migración.

- Migraciones masivas: Puede usar HCX con un servicio de optimización de WAN para migrar una gran cantidad de máquinas virtuales en un solo paso sin tiempo de inactividad, a fin de expandir sus redes en las instalaciones a la nube.
- Entornos de red heterogéneos: Su red actual (como vSphere, NSX, VXLAN o NSX-T) determina la complejidad de la migración. HCX extrae los aspectos básicos de su aplicación de red y amplía su red actual a la nube sin necesidad de procedimientos complicados.
- Velocidades de red lentas: Las migraciones suelen requerir velocidades de conexión superiores a 250 Mbps. HCX puede migrar las cargas de trabajo a velocidades mucho más bajas, alrededor de 100 Mbps.

HCX admite tres tipos de migraciones a la nube:

- Hibridez (extensión del centro de datos): amplía un centro de datos (SDDC) de VMware existente en las instalaciones a AWS para amplificar el espacio físico, ofrecer capacidad bajo demanda, un entorno de pruebas y desarrollo y escritorios virtuales.
- Vaciado de la nube (actualización de la infraestructura de todo el centro de datos): consolida los centros de datos y se traslada por completo a la nube de AWS (incluida la gestión de ubicación conjunta de centros de datos o de fin de arrendamiento).
- Especificidades de la aplicación: traslada aplicaciones individuales a la nube de AWS para satisfacer necesidades empresariales específicas.

Puede usar HCX para migrar cargas de trabajo bidireccionalmente entre su entorno en las instalaciones y VMware Cloud en AWS. HCX ofrece varias formas de migrar sus cargas de trabajo entre las ubicaciones de origen y destino:

- La migración en frío de HCX migra las máquinas virtuales que están fuera de línea. Este método es adecuado para las máquinas virtuales que están apagadas porque requieren un tiempo de inactividad significativo.
- HCX vMotion utiliza el protocolo VMware vMotion para trasladar las máquinas virtuales. HCX vMotion ofrece una migración sin tiempo de inactividad, pero solo puede migrar una máquina virtual cada vez.
- HCX Bulk Migration utiliza los protocolos de replicación de VMware vSphere para trasladar las máquinas virtuales al destino. Puede migrar varias máquinas virtuales en paralelo y programar una transición. El tiempo de inactividad equivale a un reinicio del servidor y la transición de todas las máquinas virtuales se produce en paralelo.

- HCX Replication Assisted vMotion (RAV) es una combinación de migración masiva de HCX y de HCX vMotion. Proporciona migraciones en paralelo, programación y cero tiempo de inactividad.
- HCX OS Assisted Migration ayuda a migrar varias máquinas virtuales de forma masiva cuando se utilizan varios hipervisores y máquinas virtuales que no son de vSphere en las instalaciones. HCX OS Assisted Migration es gratuita si se utiliza para migrar de un entorno en las instalaciones a VMware Cloud en AWS, pero requiere licencias adicionales para migrar entre dos entornos en las instalaciones o de un entorno en las instalaciones a otros proveedores de nube.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de VMware para acceder a la consola de VMware en vmware.com.
  - Los puertos siguientes de firewall son necesarios para HCX.

Origen	Destino	Puerto
HCX Manager y dispositivos IP en las instalaciones	HCX Manager y dispositivos IP en VMware Cloud en AWS	UDP 500, UDP 4500 e ICMP
HCX Manager y dispositivos IP en las instalaciones	connect.hcx.vmware.com | hybridity-depot.vmware.com	TCP 443
HCX Manager y dispositivos IP en las instalaciones	URL de la nube de HCX	TCP 443

    Si la red en las instalaciones tiene firewalls, tendrá que habilitar algunos puertos más de forma local dentro del centro de datos. Para obtener una lista completa de los requisitos de puertos para HCX, consulte la documentación de VMware HCX.
- Para configurar HCX, necesita la IP del sistema de nombres de dominio (DNS), el nombre de dominio completo (FQDN) de vCenter, el FQDN del servidor NTP, el usuario de inicio de sesión único (SSO) e información similar. Recopile estos datos con antelación para evitar demoras en la implementación.

Limitaciones

Puede usar el dispositivo Network Extension para ampliar un máximo de ocho redes entre el entorno en las instalaciones y VMware Cloud en AWS. Para obtener una lista completa de los límites del servicio de HCX, consulte la documentación de VMware HCX.

Arquitectura

Pila de tecnología de origen

- Cargas de trabajo de VMware en las instalaciones

Pila de tecnología de destino

- VMware Cloud en AWS

Herramientas

Herramientas

- VMware Cloud en AWS es un servicio diseñado conjuntamente por AWS y VMware para ayudarle a migrar y a ampliar sus entornos en las instalaciones basados en VMware vSphere a la nube de AWS.
- VMware Hybrid Cloud Extension (HCX) es un programa de utilidad de VMware para migrar las cargas de trabajo de su entorno VMware en las instalaciones a VMware Cloud en AWS sin cambiar la plataforma subyacente.

Epics

Implementar HCX

Tarea	Descripción	Habilidades requeridas
Habilite el servicio HCX en VMware Cloud en AWS	1. Inicie sesión en la consola de VMware Cloud en AWS. 2. Diríjase a su SDCC y seleccione View details (Ver detalles).	Administrador de la nube, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	3. Seleccione la pestaña Add-ons (Complementos). 4. Seleccione Open HCX. 5. Seleccione Deploy HCX y confirme para implementar. Comenzará la implement ación de HCX.	
Genere la clave de activación del HCX.	1. En la consola de VMware Cloud en AWS. 2. Diríjase a su SDCC y seleccione View details (Ver detalles). 3. Seleccione la pestaña Add-ons (Complementos). 4. Seleccione Open HCX y, a continuación, Activation keys (Claves de activación). 5. Seleccione Create activatio n key y copie la clave.	Administrador de la nube, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Agregue reglas de firewall para HCX en el SDDC de la nube.	Una vez implementado HCX Manager, se deben configura r las reglas de firewall para permitir las comunicac iones entre el entorno en las instalaciones y el SDDC. Debe crear dos reglas de firewall: Una para las comunicaciones entrantes y otra para las salientes. 1. En la consola de VMware Cloud en AWS, seleccion e su SDDC y vaya a Networking & Security (Redes y seguridad). 2. Elija Gateway Firewall y, a continuación, elija la pestaña Management Gateway. 3. Seleccione Add rule (Agregar regla) y cree una regla para la salida: a. Proporcione un nombre para la regla. b. Edite el origen y seleccione HCX. c. Edite el destino y proporcione la IP en las instalaciones y la subred desde donde se puede acceder a HCX.	Administrador de la nube, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	d. En Services (Servicios), seleccione Any (Cualquiera). e. En Action (Acción), seleccione Allow (Permitir). f. Seleccione Publish (Publicar). 4. Seleccione Add rule (Agregar regla) y cree una regla para la entrada: a. Proporcione un nombre para la regla. b. Edite el origen y proporcione la IP en las instalaciones y la subred desde donde se puede acceder a HCX. c. Edite el destino y seleccione HCX. d. En Services, seleccione SSH, HTTPS, TCP (9443) e ICMP. e. En Action (Acción), seleccione Allow (Permitir). f. Seleccione Publish (Publicar).	

Tarea	Descripción	Habilidades requeridas
Instale HCX Manager en las instalaciones.	1. Inicie sesión en vCenter de la nube y vaya a HCX desde el menú. 2. En el panel de control de HCX, seleccione Administration,System Updates (Actualizaciones del sistema). 3. Solicite el enlace de descarga del conector HCX de VMware y descargue el archivo OVA en las instalaciones. 4. Inicie sesión en vCenter en las instalaciones e implemente la plantilla de OVF mediante el archivo OVA descargado. 5. Durante la implementación de la plantilla, proporcione la IP estática, el NTP, el DNS, la lista de búsqueda de DNS y otros detalles cuando se solicite. 6. Compruebe todos los detalles para finalizar la implementación de HCX Manager.	Administrador de la nube, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Configure HCX Manager en las instalaciones.	1. Abra HCX Manager en un navegador: `https://<HCX_Manager_IP>:9433` . 2. Inicie sesión con el nombre de usuario y la contraseña proporcionados durante la implementación. 3. Teclee la clave de activación que creó anteriormente y elija Activate para activar la instancia de HCX. 4. Seleccione Confirm para continuar con el siguiente paso. 5. Seleccione la ubicación del centro de datos en las instalaciones y, a continuación, Continue. 6. En System Name (Nombre del sistema), escriba el nombre de host y, a continuación, seleccione Continue para completar la activación. 7. Especifique la información para configurar la conexión de vCenter. 8. Especifique la información para configurar los detalles de SSO/PSC.	Administrador de la nube, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	9. Seleccione Restart (Reiniciar) para que se apliquen los cambios.	

Tarea	Descripción	Habilidades requeridas
Configure el emparejamiento de sitios.	Una vez configurado HCX en la nube y en las instalaciones, siga estos pasos para configurar el emparejamiento de sitios entre ambos. 1. Inicie sesión en su vCenter en las instalaciones y vaya al panel de control de HCX. 2. En el panel de navegación de la izquierda, seleccione Site pairing (Emparejamiento de sitios) y, a continuación, Connect to Remote Site (Conectar a un sitio remoto). 3. En el cuadro de diálogo Connect to Remote Site (Conectar a un sitio remoto), añada la URL y las credenciales de de HCX en la nube y, a continuación, Connect. Cuando se complete el emparejamiento de sitios, el panel de control de emparejamiento de sitios muestra el SDDC en las instalaciones y en la nube conectados.	Administrador de la nube, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Cree un perfil de red.	Un perfil de red es una abstracción de los componentes de capa 3 de una red. Este perfil es un requisito previo para crear un perfil de computación. 1. Inicie sesión en vCenter en la nube y vaya al panel de control de HCX. 2. Seleccione Interconnect, la pestaña Network Profiles (Perfiles de red) y, a continuación, Create network profile (Crear perfil de red). 3. Configure el perfil de red: a. Seleccione el servidor de vCenter. b. Seleccione la red. c. Agregue un nombre para el perfil. d. Proporcione el grupo de IP, la longitud del prefijo, la puerta de enlace, el DND y la MTU. e. Seleccione Create (Crear). 4. Siga el mismo proceso para crear un perfil de red en las instalaciones.	Administrador de la nube, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Cree un perfil de computación.	El perfil de computación consta de detalles de red, almacenamiento y computación de HCX. HCX utiliza esta configuración cuando crea dispositivos HCX durante la creación de la malla de servicios. 1. Inicie sesión en su vCenter en las instalaciones y vaya al panel de control de HCX. 2. Seleccione Interconnect, la pestaña Compute Profiles (Perfiles de computación) y, a continuación, Create network profile (Crear perfil de red). 3. Especifique un nombre para el perfil de computación. 4. Seleccione los servicios de HCX que desea habilitar y, a continuación, Continue. 5. Seleccione los recursos del servicio. En caso de varios clústeres, seleccione cada clúster para el que desee que se activen los servicios de HCX y, a continuación, Continue. 6. Seleccione los recursos de computación y almacenamiento para implementar	Administrador de la nube, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	los dispositivos HCX y, a continuación, Continue. 7. Seleccione un perfil de red de administración que se pueda usar para acceder a la interfaz de administración de los hosts de vCenter y ESXi y, a continuación, Continue. 8. Seleccione un perfil de red de enlace ascendente que se pueda utilizar para acceder a los dispositivos de interconexión del sitio remoto y que los dispositivos del sitio remoto puedan utilizar para llegar a los dispositivos de interconexión locales y, a continuación, Continue. 9. Seleccione el perfil de red de vMotion y, a continuación, Continue. 10. Seleccione el perfil de red de vSphere y, a continuación, Continue. 11. Seleccione el conmutador distribuido adecuado para las extensiones de red y, a continuación, Continue. 12. Revise todos los puertos que se deben abrir en las conexiones WAN y LAN y,	

Tarea	Descripción	Habilidades requeridas
	a continuación, seleccione Continue. 13. Seleccione Finish (Finalizar) para crear el perfil de computación. 14. Siga los mismos pasos para crear un perfil de computación en el sitio en la nube.	

Tarea	Descripción	Habilidades requeridas
Cree una malla de servicios.	La malla de servicios proporciona la configuración del servicio HCX tanto para el sitio en las instalaciones como para el sitio en la nube. La creación de una malla de servicios inicia la implement ación de los dispositivos virtuales de interconexión HCX en ambos sitios. El servicio de interconexión se debe crear en el sitio de origen. 1. Inicie sesión en su vCenter en las instalaciones y vaya al panel de control de HCX. 2. Seleccione Interconnect, la pestaña Service Mesh (Malla de servicios) y, a continuación, Create service mesh (Crear malla de servicios). 3. Seleccione el sitio de origen y destino entre los que se creará la malla de servicios y, a continuación, Continue. 4. Seleccione el perfil de computación para los sitios de origen y destino creados anteriormente y, a continuación, Continue.	Administrador de la nube, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	5. Seleccione el servicio de HCX que desea habilitar y, a continuación, Continue. 6. Seleccione el perfil de enlace ascendente para los sitios de origen y destino y, a continuación, Continue. 7. Revise los recursos y las redes y, a continuación, seleccione Continue. 8. Proporcione un nombre para la malla de servicios y, a continuación, seleccione Finish (Finalizar). Se iniciará la implementación de la malla de servicios. Puede seguir el progreso en la pestaña Tasks (Tareas) de la malla de servicios. Una vez completada la implement ación, se mostrará el estado de todos los servicios de HCX habilitados para la malla de servicios.	

Ampliar las redes mediante HCX

Tarea	Descripción	Habilidades requeridas
Cree una extensión de red.	Puede utilizar las capacidad es de extensión de red de HCX para crear una extensión	Administrador de la nube, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	de red de nivel 2 en el sitio HCX de SDDC en la nube y conectar las redes remotas y de origen. Esto le permite migrar los servidores que están en las instalaciones a VMware Cloud en AWS y, al mismo tiempo, conservar las mismas direcciones IP. 1. Inicie sesión en su vCenter en las instalaciones y vaya al panel de control de HCX. 2. Seleccione Services, Network Extension (Extensión de red). 3. Seleccione Extend networks (Ampliar redes) o Create a network extension (Crear una extensión de red). 4. Seleccione la malla de servicios, el grupo de puertos distribuidos o el conmutador lógico NSX adecuados. 5. Proporcione la dirección IP de la puerta de enlace y, a continuación, seleccione Submit (Enviar).	

Tarea	Descripción	Habilidades requeridas
	Una vez completada la extensión de red, el sistema mostrará Extension complete.	

Configurar un trabajo de replicación mediante HCX

Tarea	Descripción	Habilidades requeridas
Configure la replicación.	Para replicar máquinas virtuales mediante HCX: 1. Inicie sesión en su vCenter en las instalaciones y vaya al panel de control de HCX. 2. Seleccione Migration y, a continuación, la pestaña Migrate (Migrar). 3. Proporcione un nombre de grupo de movilidad , seleccione la máquina virtual que desee migrar y, a continuación, Add. 4. Seleccione el contenedor informático de destino, la carpeta de almacenamiento, el tipo de migración (en frío, masiva [bulk], RAV, vMotion) y el programa de transición. 5. Seleccione Validate, espere a que se complete la validación y, a continuación,	Administrador de la nube, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	seleccione Go para iniciar la replicación.	

Actualizar HCX

Tarea	Descripción	Habilidades requeridas
Revise las recomendaciones y los pasos.	Un proyecto de migración de gran envergadura puede tener una duración de seis a ocho meses, a veces más, y VMware publica periódica mente actualizaciones de HCX que incluyen correcciones de software, actualizaciones de seguridad y correcciones de errores. Es recomendable mantener HCX y los dispositi vos actualizados para eliminar cualquier vulnerabilidad de seguridad y aprovechar las nuevas funciones. Nota: Si la versión actual de HCX es tres versiones más antigua que la última versión o una anterior, no podrá actualizar HCX y deberá que volver a implementarlo. La actualización delHCX consta de tres pasos: 1. Realice una copia de seguridad de HCX Manager	Administrador de la nube, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	en las instalaciones y en la nube. 2. Actualice HCX Manager en las instalaciones y en la nube. 3. Actualice los dispositivos de la malla de servicios en las instalaciones y en la nube. Los apartados siguientes tratan estos temas de manera detallada.	

Tarea	Descripción	Habilidades requeridas
Realice una copia de seguridad de HCX Cloud Manager.	VMware administra HCX Cloud Manager para VMware Cloud en AWS, por lo que no es posible tomar instantán eas. Para realizar una copia de seguridad de HCX Cloud Manager, se debe descargar una copia de seguridad de la consola HCX y utilizarla para restaurar la configura ción de HCX en caso de que la actualización tenga algún error o se deba volver a una etapa anterior. 1. Inicie sesión en HCX Cloud Manager en `https://<HCX_cloudmanager_ip_or_fqdn>:9433` . 2. Vaya a Administration, Troubleshooting (Solución de problemas), Backup & Restore (Respaldo y restauración). 3. En la sección Backup, seleccione Generate para crear un archivo de copia de seguridad. 4. Seleccione Download para guardar el archivo de copia de seguridad. Los dispositivos de servicio de HCX, como HCX-IX, HCX-	Administrador de la nube, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	NE y HCX-WO, no requieren copias de seguridad individua les.	

Tarea	Descripción	Habilidades requeridas
Realice una copia de seguridad del HCX Manager en las instalaciones.	Hay dos formas de realizar una copia de seguridad de HCX Manager en las instalaciones: mediante una instantánea de la máquina virtual o mediante una copia de seguridad del archivo de configuración. Para realizar una instantánea de la máquina virtual: 1. Inicie sesión en vCenter en las instalaciones. 2. Vaya a VM and templates (Máquina virtual y plantillas) de HCX Manager. 3. Seleccione Actions, Snapshots (Instantáneas) y Take Snapshot (Realizar instantánea). Para realizar una copia de seguridad del archivo de configuración: 1. Inicie sesión en HCX Cloud Manager en `https://<HCX_cloudmanager_ip_or_fqdn>:9433` . 2. Vaya a Administration, Troubleshooting (Solución de problemas), Backup	Administrador de la nube, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	& Restore (Respaldo y restauración). 3. En la sección Backup, seleccione Generate para crear un archivo de copia de seguridad. 4. Seleccione Download para guardar el archivo de copia de seguridad. Los dispositivos de servicio de HCX, como HCX-IX, HCX-NE y HCX-WO, no requieren copias de seguridad individuales.	

Tarea	Descripción	Habilidades requeridas
Actualice HCX Manager en las instalaciones y en la nube.	Primero debe actualizar HCX Manager en las instalaciones y, a continuación, actualizar HCX Cloud Manager. Para actualizar HCX Manager en las instalaciones: 1. Inicie sesión en vCenter y vaya al panel de control de HCX. 2. Seleccione System, Administration. 3. En la página Administration, seleccione la pestaña System Updates (Actualizaciones del sistema). La columna Available Service Update Versions (Versiones de actualizaciones de servicio disponibles) muestra las actualizaciones pendientes. 4. Seleccione Select Service Update (Seleccionar actualización de servicio), Download para descargar la actualización para una actualización posterior o Download & Upgrade para descargar e implementar la actualización de forma inmediata. Si seleccionó Download, seleccione	Administrador de la nube, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	Upgrade y confirme para iniciar la actualización cuando esté todo listo. 5. Cuando se complete la actualización: • En la página Administration de HCX Manager, compruebe que se muestre la versión más reciente de HCX. • En el panel de control de HCX, compruebe que el emparejamiento de sitios esté en Up (Activado). • Seleccione Infrastructure, Service Mesh (Malla de servicios) y confirme que todos los servicios de HCX están en buen estado. Siga los mismos pasos para actualizar HCX Cloud Manager.	

Tarea	Descripción	Habilidades requeridas
Actualice los dispositivos de la malla de servicios.	La malla de servicios se actualiza independientemente de HCX Manager en el sitio de origen. Los dispositivos de la malla de servicios del sitio de destino se actualizan automáticamente. Para actualizar los dispositivos de la malla de servicios en el sitio de origen: 1. Inicie sesión en vCenter y vaya al panel de control de HCX. 2. Seleccione Infrastructure y, a continuación, la pestaña Service Mesh (Malla de servicios). 3. Si se muestra el banner indicando que está disponible una nueva versión para los dispositivos de la malla de servicios. Haga clic en Update Appliances (Actualizar los dispositivos) para actualizarlos a la última versión y seleccione Update appliances. 4. En el cuadro de diálogo que muestra los dispositivos, seleccione uno o más dispositivos y, a	Administrador de la nube, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	continuación, OK (Aceptar) para iniciar el proceso de actualización. (Es recomendable actualizar todos los dispositivos de la malla de servicios). 5. Seleccione View tasks (Ver tareas) para cada malla de servicios para supervisar la actualización. 6. Cuando se complete la actualización, se mostrará un banner para cada dispositivo y servicio para confirmar que se ha completado correctamente. 7. Valide el estado del túnel después de la actualiza ción: • Seleccione Infrastructure, Service mesh (Malla de servicios) o View Appliance (Ver dispositi vo). • La columna de estado del túnel debería mostrar Up (activa) y la pantalla no debería indicar ninguna otra versión disponible del dispositivo.	

Eliminar extensiones de red HCX

Tarea	Descripción	Habilidades requeridas
Red no extendida.	En un paso anterior se explicó cómo utilizar las capacidad es de extensión de red de HCX para crear extensiones de red de nivel 2 y conservar las IP existentes durante la migración desde las instalaci ones hasta la VMware Cloud en AWS. Cuando todas las máquinas virtuales de una VLAN concreta se hayan trasladado a VMware Cloud en AWS, se debe eliminar la extensión de la red entre el sitio en las instalaciones y el SDDC en la nube y hacer que la red sea enrutable en el SDDC. Le recomendamos que elimine la red extendida tan pronto como se migren todas las máquinas virtuales de las instalaciones a VMware Cloud en AWS para evitar la latencia. 1. Inicie sesión en su vCenter en las instalaciones y vaya al panel de control de HCX. 2. En el panel de control de HCX, seleccione Services, Network Extension.	Administrador de la nube, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	3. Seleccione la red para la que desea eliminar la extensión y, a continuación, Unextend network (Eliminar extensión de la red). 4. Seleccione Connect cloud network to cloud edge gateway after unextendi ng (Conectar la red en la nube a la puerta de enlace perimetral de la nube después de eliminar la extensión). Esto activa la red en la nube.	

Tarea	Descripción	Habilidades requeridas
Enrute la red trasladada en el SDDC en la nube.	1. Inicie sesión en el portal de VMC. 2. Diríjase al SDCC y seleccione View details (Ver detalles). 3. Seleccione la pestaña Networking & Security (Redes y seguridad). 4. En la página Networking & Security: • Seleccione Network (Red), Segments y confirme que la subred cuya extensión se ha eliminado recientem ente se muestre como routable (enrutable). • Seleccione Inventory, Groups y agregue esa subred a un grupo. • Seleccione Security, Distributed firewall y confirme que el grupo forma parte de la regla de firewall prevista.	Administrador de la nube, administrador de sistemas

Desinstalar HCX

Tarea	Descripción	Habilidades requeridas
Compruebe los requisitos previos.	En caso de salida del centro de datos, le recomendamos que desinstale HCX y elimine	Administrador de la nube, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	sus componentes al final del proyecto de migración. Sin embargo, si aún conserva un espacio en las instalaciones, le recomendamos que mantenga HCX en funcionamiento. Antes de desinstalar HCX, asegúrese de lo siguiente: • No hay migraciones activas. • Se han eliminado todas las extensiones de red.	

Tarea	Descripción	Habilidades requeridas
Desinstale HCX en las instalaciones.	1. Inicie sesión en vCenter en las instalaciones y vaya a la consola de HCX. 2. Seleccione Services, Migration y confirme que no tiene migraciones activas. 3. Seleccione Services, Network extension y confirme que no haya ninguna red extendida. 4. Seleccione Infrastructure, Site pairing (Empareja miento de sitios) o Service mesh (Malla de servicios). 5. Identifique la malla de servicios y, a continuación, seleccione Delete. 6. En el mensaje de confirmac ión, seleccione Delete (Eliminar) de nuevo. Se mostrará el banner «Removing Service Mesh» en la pantalla de la malla de servicios. 7. Repita los pasos 5 y 6 para cualquier otra malla de servicio que tenga. 8. Para eliminar el emparejam iento de sitios, seleccione Infrastructure, Site pairing (Emparejamiento de sitios) y, a continuación,	Administrador de la nube, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	desconecte todos los sitios emparejados. 9. Retire el dispositivo HCX Manager: a. Inicie sesión en vCenter en las instalaciones y vaya al dispositivo de HCX. b. Seleccione Actions, Power, Power Off (Apagar). c. Seleccione Actions, Delete from Disk (Eliminar del disco).	

Tarea	Descripción	Habilidades requeridas
Borre el registro del complemento HCX del servidor vCenter en las instalaciones.	1. Inicie sesión en la interfaz de usuario MOB de vCenter en `https://<vc_fqdn>/mob` . 2. En la sección Properties, seleccione el contenido de la columna Value (Valor). 3. En la página de contenido , selecciona Extension Managerver todos los complementos registrados. 4. Anote las extensiones que comienzan por `com.vmware.hybridity` , `com.vmware.hcsp.alarm` y `com.vmware.vca.marketing.ngc.ui` . 5. Elimine las extensiones: • En la sección Métodos, selecciona UnregisterExtension. • Especifique la clave de extensión anotada en el paso 4 y, a continuación, seleccione Invoke Method (Invocar método) para eliminar la extensión . Una vez eliminadas todas las extensiones, el complemento	Administrador de la nube, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	HCX desaparecerá del cliente web de vSphere.	
Desinstale HCX en la nube.	Para eliminar la malla de servicios de HCX y el emparejamiento de sitios en la nube, repita los pasos descritos para Uninstall HCX on premises (Desinstalar HCX en las instalaciones). En VMware Cloud en AWS, VMware administra HCX Manager. No puede eliminarlo de vCenter, pero puede anular su implementación desde la interfaz de administración de VMC. Para anular la implementación de HCX Manager: 1. Inicie sesión en la interfaz de VMC management interface. 2. Elija su organización y el SDDC. 3. Seleccione Add Ons (Complementos) para ver todos los SDDC en los que se ha implementado el HCX. 4. Seleccione Undeploy HCX (Anular la implementación de HCX).	Administrador de la nube, administrador de sistemas

Resolución de problemas

Problema	Solución
No puede seleccionar los servidores que desea migrar al configurar la migración masiva (bulk) de HCX.	Causa: Se canceló la migración de estos servidores, pero la base de datos de HCX no se actualizó durante la limpieza. HCX considera que la migración de la base de datos aún está en curso, por lo que ha bloqueado el estado en «Transición en curso». Solución: Contacte con el equipo de soporte de VMware para limpiar la base de datos de HCX.
La transición es errónea, pero funciona con la opción Force Power Off.	Causa: La versión de VMware Tools no cumplía los requisitos previos para la migración masiva (bulk) de HCX, por lo que HCX no pudo cerrar la máquina virtual de origen. Solución: Actualice la herramienta de VMware a la versión recomendada para su tipo de migración.
La actualización del dispositivo de emparejamiento de sitios HCX no se procesa y aparece el error «"Operation not allowed for ongoing bulk migration» (No se permite la operación durante la migración masiva en curso) mientras la migración está en curso.	Causa: La base de datos de HCX no se actualizó después de la transición. Solución: Asegúrese de que no haya migraciones en curso. Seleccione Force upgrade (Forzar la actualización) cuando actualice el dispositivo de emparejamiento de sitios.
Se produce un error en la transición y aparece el mensaje «Low resource availability» (Baja disponibilidad de recursos).	Causa: Poco espacio de almacenamiento en la máquina virtual del host. Solución: Compruebe los recursos de almacenamiento y procesamiento antes de la migración.

Recursos relacionados

Referencias

- Características de VMware Cloud en AWS
- Descripción general y modelo operativo de VMware Cloud en AWS (Recomendaciones de AWS)
- Migración de VMware SDDC a VMware Cloud en AWS mediante VMware HCX (Recomendaciones de AWS)
- VMware HCX en VMware Cloud en AWS (documentación de VMware)
- Notas de la versión de HCX HCX (documentación de VMware)
- Guía de implementación y prácticas recomendadas del SDDC en AWS (documento técnico de AWS)

Herramientas

- Automatización de VMware Cloud dn AWS mediante PowerCLI (VMware Cloud Tech Zone)

Socios

- VMware Cloud en AWS Partner Initiative

Videos

- VMware Cloud on AWS (YouTube vídeo)

Transportar bases de datos PostgreSQL entre dos instancias de base de datos de Amazon RDS utilizando pg_transport

Creado por Raunak Rishabh (AWS) y Jitender Kumar (AWS)

Entorno: PoC o piloto	Origen: bases de datos: relacionales	Amazon RDS para PostgreSQL
Tipo R: reubicar	Carga de trabajo: código abierto	Tecnologías: Migración; bases de datos
Servicios de AWS: Amazon RDS		

Resumen

Este patrón describe los pasos para migrar bases de datos extremadamente grandes entre dos instancias de base de datos de Amazon Relational Database Service (Amazon RDS) para PostgreSQL mediante la extensión pg_transport. Esta extensión proporciona un mecanismo físico de transporte para trasladar cada base de datos. Al transmitir por streaming los archivos de base de datos con un procesamiento mínimo, proporciona un método extremadamente rápido para migrar bases de datos de gran tamaño entre instancias de base de datos con un tiempo de inactividad mínimo. Esta extensión utiliza un modelo de extracción donde la instancia de base de datos de destino importa la base de datos de la instancia de base de datos de origen.

Requisitos previos y limitaciones

Requisitos previos

- Ambas instancias de base de datos deben ejecutar la misma versión principal de PostgreSQL.
- La base de datos no debe existir en el destino. De lo contrario, el transporte devuelve un error.
- No se debe habilitar ninguna extensión que no sea pg_transport en la base de datos de origen.
- Todos los objetos de base de datos deben estar en el espacio de tablas predeterminado pg_default.
- El grupo de seguridad de la instancia de base de datos de origen debe permitir el tráfico desde la instancia de base de datos de destino.

- Instale un cliente de PostgreSQL, como psql, PgAdmino para trabajar con la instancia de base de datos PostgreSQL de Amazon RDS. Puede instalar el cliente en su sistema local o utilizar una instancia de Amazon Elastic Compute Cloud (Amazon EC2). En este patrón, utilizamos psql en una instancia EC2.

Limitaciones

- No puede transportar bases de datos entre distintas versiones principales de Amazon RDS para PostgreSQL.
- Los privilegios de acceso y la propiedad de la base de datos de origen no se transfieren a la base de datos de destino.
- No puede transportar bases de datos en réplicas de lectura ni en instancias principales de réplicas de lectura.
- No puede utilizar tipos de datos de registro en ninguna tabla de base de datos que planee transportar con este método.
- Puede ejecutar hasta 32 transportes totales al mismo tiempo en una instancia de base de datos, (incluidas tanto importaciones como exportaciones).
- No puede cambiar el nombre de las tablas ni incluirlas o excluirlas. Todo se migra tal cual.

Precaución

- Realice copias de seguridad antes de eliminar la extensión, ya que al eliminar la extensión también se eliminan los objetos dependientes y algunos datos que son fundamentales para el funcionamiento de la base de datos.
- Tenga en cuenta la clase de instancia y los procesos que se ejecutan en otras bases de datos de la instancia de origen al determinar la cantidad de trabajadores y los `work_mem` valores de pg_transport.
- Cuando se inicia el transporte, finalizan todas las conexiones de la base de datos de origen y la base de datos pasa al modo de solo lectura.

Nota: cuando el transporte se ejecuta en una base de datos, no afecta a las demás bases de datos del mismo servidor.

Versiones de producto

- Amazon RDS para PostgreSQL 10.10 y posteriores y Amazon RDS para PostgreSQL 11.5 y posteriores. Para obtener información sobre la versión más reciente, consulte Transporte de bases de datos PostgreSQL entre instancias de base de datos en la documentación de Amazon RDS.

Arquitectura

Herramientas

- pg_transport proporciona un mecanismo físico de transporte para trasladar cada base de datos. Al transmitir por streaming los archivos de la base de datos con un procesamiento mínimo, el transporte físico mueve los datos mucho más rápido que los procesos tradicionales de volcado y carga y requiere un tiempo de inactividad mínimo. Las bases de datos transportables de PostgreSQL utilizan un modelo de extracción donde la instancia de base de datos de destino importa la base de datos de la instancia de base de datos de origen. Esta extensión se instala en las instancias de base de datos al preparar los entornos de origen y destino, tal y como se explica en este patrón.
- psql le permite conectarse a sus instancias de base de datos de PostgreSQL y trabajar con ellas. Para instalar psql en su sistema, consulte la página de descargas de PostgreSQL.

Epics

Cree el grupo de parámetros de destino

Tarea	Descripción	Habilidades requeridas
Cree un grupo de parámetros para el sistema de destino.	Especifique un nombre de grupo que lo identifique como grupo de parámetros de destino; por ejemplo,v `pgtarget-param-group` . Para obtener instrucciones, consulte la Documentación de Amazon RDS.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Modifique los parámetros para el grupo de parámetros.	Establezca los siguientes parámetros: 1. Añada `pg_transport` al parámetro `shared_preload_libraries` . `shared_preload_libraries = pg_stat_statements, pg_transport` 2. Establezca el parámetro `pg_transport.num_workers` . Seleccione el número de trabajadores con los que quieres gestionar el transporte. El valor que establezca determina la cantidad de `transport.send_file` trabajadores que se crearán en la fuente. 3. Aumente el valor de `max_worker_processes` a más de tres veces el valor de`pg_transport.num_workers` . Por ejemplo, si establece el valor de `pg_transport.num_workers` en 4, el `max_worker_processes` valor debe ser al menos 13. Si esto no funciona, pg_transp	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	ort recomienda un valor mínimo. 4. Establezca `pg_transport.timing` en 1. Esta configuración permite notificar la información de tiempo durante el transporte. 5. Establezca el parámetro `pg_transport.work_mem`. Este parámetro especifica la memoria máxima que se debe asignar a cada trabajador. El valor predeterminado es 128 MB. Para obtener más información acerca de estos parámetros, consulte la documentación de Amazon RDS.	

Crear el grupo de parámetros

Tarea	Descripción	Habilidades requeridas
Cree un grupo de parámetros para el sistema de origen.	Especifique un nombre de grupo que lo identifique como grupo de parámetros de origen; por ejemplo, `pgsource-param-group`. Para obtener instrucciones,	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	consulte la Documentación de Amazon RDS.	

Tarea	Descripción	Habilidades requeridas
Modifique los parámetros para el grupo de parámetros.	Establezca los siguientes parámetros: 1. Añada `pg_transport` al parámetro `shared_preload_libraries` . `shared_preload_libraries = pg_stat_statements, pg_transport` 2. Establezca el parámetro `pg_transport.num_workers` . El valor de este parámetro definido en el objetivo determina el número de `transport.send_file` trabajadores que se van a utilizar. Si tiene una importación en ejecución en esta instancia, aumente este valor, pero tenga en cuenta la cantidad de trabajadores que ya se están ejecutando. 3. Aumente el valor de `max_worker_processes` a más de tres veces el valor del `pg_transport.num_workers` objetivo. Por ejemplo, si establece el valor de `pg_transport.num_workers` 4 en el destino, el	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`max_worker_processes` valor del origen debe ser al menos 13. Si esto no funciona, pg_transport recomienda un valor mínimo. 4. Establezca el parámetro `pg_transport.work_mem` . Este parámetro especifica la memoria máxima que se debe asignar a cada trabajador. El valor predeterminado es 128 MB. Para obtener más información acerca de estos parámetros, consulte la documentación de Amazon RDS.	

Prepare el entorno de destino

Tarea	Descripción	Habilidades requeridas
Cree una nueva instancia de base de datos de Amazon RDS para PostgreSQL a la que transportar la base de datos de origen.	Determine la clase de instancia y la versión de PostgreSQL en función de los requisitos de su empresa.	Administrador de base de datos, administrador de sistemas, arquitecto de bases de datos
Modifique el grupo de seguridad del destino para permitir las conexiones en el puerto de la instancia de base	De forma predeterminada, el puerto para la instancia de PostgreSQL es 5432. Si utiliza otro puerto, las conexione	Administrador de base de datos, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
de datos desde la instancia EC2.	s a ese puerto deben estar abiertas para la instancia EC2.	
Modifique la instancia y asigne el nuevo grupo de parámetros de destino.	Por ejemplo, `pgtarget-param-group` .	Administrador de base de datos
Reinicie la instancia de base de datos de Amazon RDS de destino.	Los parámetros `shared_preload_libraries` y `max_worker_processes` son parámetros estáticos y requieren el reinicio de la instancia.	Administrador de base de datos, administrador de sistemas
Conéctese a la base de datos desde la instancia de EC2 mediante psql.	Utilice el comando: `psql -h <rds_end_point> -p PORT -U username -d database -W`	Administrador de base de datos
Cree la extensión pg_transport.	Ejecute la siguiente consulta como usuario con el rol `rds_superuser` : `create extension pg_transport;`	Administrador de base de datos

Preparar el entorno de origen

Tarea	Descripción	Habilidades requeridas
Modifique el grupo de seguridad de la fuente para permitir las conexiones en el puerto de la instancia de base	De forma predeterminada, el puerto para la instancia de PostgreSQL es 5432. Si utiliza otro puerto, las conexione	Administrador de base de datos, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
de datos desde la instancia Amazon EC2 y la instancia de base de datos de destino	s a ese puerto deben estar abiertas para la instancia EC2.	
Modifique la instancia y asigne el nuevo grupo de parámetros de origen.	Por ejemplo, `pgsource-param-group` .	Administrador de base de datos
Reinicie la instancia de base de datos de Amazon RDS de origen.	Los parámetros `shared_preload_libraries` y `max_worker_processes` son parámetros estáticos y requieren el reinicio de la instancia.	Administrador de base de datos
Conéctese a la base de datos desde la instancia de EC2 mediante psql.	Utilice el comando: `psql -h <rds_end_point> -p PORT -U username -d database -W`	Administrador de base de datos
Cree la extensión pg_transport y elimine todas las demás extensiones de las bases de datos que se van a transportar.	El transporte fallará si hay alguna extensión que no sea pg_transport instalada en la base de datos de origen. Este comando debe ejecutarlo un usuario con el rol `rds_superuser` .	Administrador de base de datos

Realice el transporte

Tarea	Descripción	Habilidades requeridas
Ejecute una prueba.	Utilice la función `transport.import_from_serve`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`r` para realizar primero un simulacro: `SELECT transport.import_from_server( 'source-db-instance-endpoint', source-db-instance-port, 'source-db-instance-user', 'source-user-password', 'source-database-name', 'destination-user-password', 'true');` El último parámetro de esta función (establecido en`true`) define el funcionamiento en seco. Esta función muestra los errores que aparecen al ejecutar el transporte principal. Resuelva los errores antes de ejecutar el transporte principal.	

Tarea	Descripción	Habilidades requeridas
Si el simulacro se realiza correctamente, inicie el transporte de la base de datos.	Ejecute la función `transport.import_from_server` para realizar el transporte. Se conecta a la fuente e importa los datos. `SELECT transport.import_from_server( 'source-db-instance-endpoint', source-db-instance-port, 'source-db-instance-user', 'source-user-password', 'source-database-name', 'destination-user-password', false);` El último parámetro de esta función (establecido en`false`) indica que no se trata de un simulacro.	Administrador de base de datos
Realice los pasos posteriores al transporte.	Una vez finalizado el transporte de la base de datos: • Valide los datos en el entorno de destino. • Añada todos los roles y permisos al objetivo. • Habilite todas las extensiones necesarias en el destino y el origen, si es necesario. • Revierta el valor del parámetro `max_worker_processes` .	Administrador de base de datos

Recursos relacionados

- Documentación de Amazon RDS
- Documentación de pg_transport
- Migración de bases de datos mediante bases de datos transportables PostgreSQL de RDS (entrada del blog)
- Descargas de PostgreSQL
- utilidad psql
- Creación de un grupo de parámetros de base de datos
- Modificar parámetros en un grupo de parámetros de base de datos
- Descargas de PostgreSQL

Redefinir la plataforma

Temas

- Configurar enlaces entre la base de datos de Oracle y Aurora compatible con PostgreSQL
- Exportación de una base de datos de Microsoft SQL Server a Amazon S3 mediante AWS DMS
- Migre cargas de trabajo de aprendizaje automático: cree, entrene e implemente a Amazon SageMaker con las herramientas para desarrolladores de AWS
- Migre OpenText TeamSite las cargas de trabajo a la nube de AWS
- Migre valores CLOB de Oracle a filas individuales en PostgreSQL en AWS
- Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle mediante Oracle Data Pump
- Migre Oracle E-Business Suite a Amazon RDS Custom
- Migre Oracle PeopleSoft a Amazon RDS Custom
- Migre la funcionalidad ROWIdentificador de Oracle a PostgreSQL en AWS
- Migre los códigos de error de Oracle Database a una base de datos Amazon Aurora compatible con PostgreSQL
- Migración de las cargas de trabajo de Redis a Redis Enterprise Cloud en AWS
- Migre SAP ASE de Amazon EC2 a Amazon Aurora compatible con PostgreSQL mediante AWS SCT y AWS DMS
- Migración de los certificados SSL de Windows a un equilibrador de carga de aplicación mediante ACM
- Migración de una cola de mensajes de Microsoft Azure Service Bus a Amazon SQS
- Migre una EnterpriseOne base de datos de Oracle JD Edwards a AWS mediante Oracle Data Pump y AWS DMS
- Migre una PeopleSoft base de datos de Oracle a AWS mediante AWS DMS
- Migrar una base de datos MySQL en las instalaciones a Amazon RDS para MySQL
- Migración de una base de datos de Microsoft SQL Server en las instalaciones a Amazon RDS para SQL Server
- Migre datos de Microsoft Azure Blob a Amazon S3 mediante Rclone
- Migración de Couchbase Server a Couchbase Capella en AWS
- Migre de IBM WebSphere Application Server a Apache Tomcat en Amazon EC2
- Migre de IBM WebSphere Application Server a Apache Tomcat en Amazon EC2 con Auto Scaling

- Migración de una aplicación .NET de Microsoft Azure App Service a AWS Elastic Beanstalk
- Migración de un entorno de MongoDB autoalojado a MongoDB Atlas en la nube de AWS
- Migre de Oracle WebLogic a Apache Tomcat (ToMEE) en Amazon ECS
- Migración de una base de datos de Oracle de Amazon EC2 a Amazon RDS para Oracle mediante AWS DMS
- Migre una base de datos Oracle local a Amazon OpenSearch Service mediante Logstash
- Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle
- Migrar una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle mediante Oracle Data Pump
- Migre de PostgreSQL en Amazon EC2 a Amazon RDS para PostgreSQL mediante pglogical
- Migrar una base de datos PostgreSQL en las instalaciones a Aurora PostgreSQL
- Migración de una base de datos de Microsoft SQL Server en las instalaciones a Microsoft SQL Server en Amazon EC2 con Linux
- Migración de bases de datos en las instalaciones de Microsoft SQL Server a Amazon RDS para SQL Server mediante servidores vinculados
- Migre una base de datos de Microsoft SQL Server en las instalaciones a Amazon RDS para SQL Server mediante métodos nativos de copia de seguridad y restauración
- Migración de una base de datos de Microsoft SQL Server a Aurora MySQL mediante AWS DMS y AWS SCT
- Migración de una base de datos de MariaDB en las instalaciones hasta Amazon RDS para MariaDB mediante herramientas nativas
- Migrar de una base de datos de MySQL en las instalaciones a Aurora MySQL
- Migre bases de datos MySQL locales a Aurora MySQL mediante Percona, XtraBackup Amazon EFS y Amazon S3
- Migración de aplicaciones Java locales en las instalaciones a AWS mediante AWS App2Container
- Migración de sistemas de archivos compartidos en una gran migración de AWS
- Migre una base de datos Oracle a Amazon RDS for Oracle mediante adaptadores de archivos planos de GoldenGate Oracle
- Cambie las aplicaciones de Python y Perl para que admitan la migración de bases de datos de Microsoft SQL Server a una edición compatible con PostgreSQL de Amazon Aurora

Configurar enlaces entre la base de datos de Oracle y Aurora compatible con PostgreSQL

Creado por Jeevan Shetty (AWS), Bhanu Ganesh Gudivada (AWS), Sushant Deshmukh (AWS), Uttiya Gupta (AWS) y Vikas Gupta (AWS)

Entorno: PoC o piloto	Origen: base de datos de Oracle	Destino: Aurora (compatible con PostgreSQL)
Tipo R: redefinir la plataforma	Carga de trabajo: Oracle; código abierto	Tecnologías: migración; bases de datos
Servicios de AWS: Amazon Aurora; Amazon EC2 Auto Scaling; Amazon Route 53		

Resumen

Como parte de la migración a la nube de Amazon Web Services (AWS), puede modernizar sus aplicaciones para utilizar bases de datos nativas en la nube. La migración de la base de datos de Oracle a una edición compatible con PostgreSQL de Amazon Aurora es uno de esos pasos hacia la modernización. Como parte de esa migración, los enlaces de bases de datos nativas de Oracle también requieren una conversión.

Mediante un enlace de base de datos, una base de datos puede acceder a los objetos de otra base de datos. Tras la migración de la base de datos Oracle a Aurora compatible con PostgreSQL, los enlaces de base de datos del servidor de base de datos Oracle a otros servidores de base de datos Oracle deben convertirse en enlaces de base de datos PostgreSQL a Oracle.

Este patrón muestra cómo puede configurar enlaces de bases de datos desde un servidor de bases de datos Oracle a la base de datos Aurora compatible con PostgreSQL. Como los enlaces de bases de datos son unidireccionales, el patrón también incluye la conversión de enlaces de bases de datos de la base de datos PostgreSQL a una base de datos Oracle.

Tras la migración y la conversión de la base de datos Oracle a una base de datos Aurora compatible con PostgreSQL, se requieren los siguientes pasos para configurar los enlaces de bases de datos entre bases de datos:

- Para configurar un enlace de base de datos con la base de datos Oracle como origen y Aurora compatible con PostgreSQL como destino, se deben configurar Base de datos Oracle Gateways para la comunicación entre bases de datos heterogéneas.
- Si está configurando un enlace de base de datos entre la versión 12.6 y anteriores de Aurora compatibles con PostgreSQL como base de datos de origen y la base de datos Oracle como destino, la extensión **`oracle_fdw`** no está disponible de forma nativa. En su lugar, puede usar la extensión `postgres_fdw` en la base de datos Aurora compatible con PostgreSQL y configurar `oracle_fdw` en una base de datos PostgreSQL creada en Amazon Elastic Compute Cloud (Amazon EC2). Esta base de datos actúa como intermediaria entre la base de datos Aurora compatible con PostgreSQL y la base de datos Oracle. Este patrón incluye dos opciones para configurar el enlace de la base de datos con Aurora PostgreSQL 12.6 y versiones anteriores:
  - Configure la instancia EC2 en un grupo de Amazon EC2 Auto Scaling con un script de inicio de Amazon EC2 que actualice una entrada interna del Sistema de nombres de dominio (DNS) en Amazon Route 53.
  - Configure la instancia EC2 en un grupo de Amazon EC2 Auto Scaling con un equilibrador de carga de red para alta disponibilidad (HA).

Si está configurando un enlace de base de datos entre la versión 12.7 y versiones posteriores de Aurora compatibles con PostgreSQL, puede usar la extensión `oracle_fdw`.

Requisitos previos y limitaciones

Requisitos previos

- Base de datos de Amazon Aurora compatibles con PostgreSQL en una nube privada virtual (VPC)
- Conectividad de red entre las bases de datos Oracle y Aurora compatibles con PostgreSQL

Limitaciones

- Actualmente, los enlaces de bases de datos no se pueden configurar con Amazon Relational Database Service (Amazon RDS) para Oracle como base de datos de origen y Aurora compatible con PostgreSQL como base de datos de destino.

Versiones de producto

- Oracle Database versión 11g y posteriores

- Aurora (compatible con PostgreSQL 11 y versiones más recientes)

Arquitectura

Pila de tecnología de origen

Antes de la migración, la base de datos Oracle de origen puede acceder a los objetos de otras bases de datos Oracle mediante enlaces de bases de datos. Esto funciona de forma nativa entre las bases de datos de Oracle en las instalaciones o en la nube de AWS.

Pila de tecnología de destino

Opción 1

- Edición compatible con Amazon Aurora PostgreSQL
- Instancia de base de datos de PostgreSQL en Amazon EC2
- Grupo de Amazon EC2 Auto Scaling
- Amazon Route 53
- Amazon Simple Notification Service (Amazon SNS)
- AWS Identity y Access Management (IAM)
- AWS Direct Connect

Opción 2

- Edición compatible con Amazon Aurora PostgreSQL
- Instancia de base de datos de PostgreSQL en Amazon EC2
- Grupo de Amazon EC2 Auto Scaling
- Equilibrador de carga de red
- Amazon SNS
- Direct Connect

Opción 3

- Edición compatible con Amazon Aurora PostgreSQL
- Direct Connect

Arquitectura de destino

Opción 1

El siguiente diagrama muestra la configuración del enlace de la base de datos mediante las extensiones `oracle_fdw` y `postgres_fdw`, con HA proporcionada por un grupo de Amazon EC2 Auto Scaling y Route 53.

1. Una instancia de Aurora compatible con PostgreSQL con la extensión `postgres_fdw` se conecta a la base de datos PostgreSQL en Amazon EC2.
2. La base de datos PostgreSQL con la extensión `oracle_fdw` se encuentra en un grupo de escalado automático.
3. La base de datos PostgreSQL de Amazon EC2 utiliza Direct Connect para conectarse a la base de datos Oracle en las instalaciones.
4. Oracle Database se configura con Oracle Database Gateways para las conexiones desde Oracle Database a la base de datos PostgreSQL en AWS.
5. IAM concede permiso a Amazon EC2 para actualizar los registros de Route 53.
6. Amazon SNS envía alertas sobre las acciones de escalado automático.
7. El nombre de dominio configurado en Route 53 apunta a la dirección IP de la instancia Amazon EC2 de PostgreSQL.

Opción 2

El siguiente diagrama muestra la configuración del enlace de la base de datos mediante las extensiones `oracle_fdw` y `postgres_fdw`, con HA proporcionada por un grupo de escalado automático y un equilibrador de carga de red.

1. Una instancia de Aurora compatible con PostgreSQL con la extensión `postgres_fdw` se conecta al equilibrador de carga de red.
2. El equilibrador de carga de red distribuye la conexión desde la base de datos Aurora compatible con PostgreSQL a la base de datos PostgreSQL de Amazon EC2.
3. La base de datos PostgreSQL con la extensión `oracle_fdw` se encuentra en un grupo de escalado automático.

4. La base de datos PostgreSQL de Amazon EC2 utiliza Direct Connect para conectarse a la base de datos Oracle en las instalaciones.
5. Oracle Database se configura con Oracle Database Gateways para las conexiones desde Oracle Database a la base de datos PostgreSQL en AWS.
6. Amazon SNS envía alertas sobre las acciones de escalado automático.

Opción 3

El siguiente diagrama muestra la configuración del enlace de base de datos mediante la extensión `oracle_fdw` en una base de datos Aurora compatible con PostgreSQL.

1. Una instancia Aurora compatible con PostgreSQL con la extensión `oracle_fdw` utiliza Direct Connect para conectarse a base de datos Oracle.
2. Las bases de datos Oracle Gateways configuradas en Oracle Server permiten la conectividad a través de Direct Connect a la base de datos Aurora compatible con PostgreSQL.

Herramientas

Servicios de AWS

- Edición de Amazon Aurora compatible con PostgreSQL es un motor de base de datos relacional completamente administrado que le permite configurar, utilizar y escalar implementaciones de PostgreSQL.
- AWS Direct Connect vincula su red interna con una ubicación de Direct Connect a través de un cable estándar Ethernet de fibra óptica. Con esta conexión, puede crear interfaces virtuales directamente en servicios públicos de AWS y derivar a los proveedores de Internet a su ruta de acceso a la red.
- Amazon Elastic Compute Cloud (Amazon EC2) brinda capacidad de computación escalable en la Nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez. En este patrón, las opciones 1 y 2 utilizan una instancia EC2 para alojar una base de datos PostgreSQL.
- Amazon EC2 Auto Scaling lo ayuda a mantener disponible la aplicación y le permite añadir o quitar automáticamente instancias de Amazon EC2 según las condiciones que defina.

- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad.
- Amazon Simple Notification Service (Amazon SNS) permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- Elastic Load Balancing (ELB) distribuye el tráfico entrante de aplicaciones o redes entre varios destinos. Así, por ejemplo, puede distribuir el tráfico a través de instancias de Amazon Elastic Compute Cloud (Amazon EC2), contenedores y direcciones IP de una o varias zonas de disponibilidad. Este patrón utiliza un equilibrador de carga de red.

Otros servicios

- Base de datos Oracle Gateways proporciona a una base de datos Oracle la capacidad de acceder a los datos de un sistema que no es de Oracle.

Epics

Tareas de configuración habituales para las opciones 1 y 2

Tarea	Descripción	Habilidades requeridas
Cree una instancia EC2 y configure la extensión Oracle_fdw para PostgreSQL.	1. Cree una instancia EC2 con el sistema operativo Amazon Linux 2. 2. Para instalar PostgreSQL, inicie sesión en la instancia EC2 como ec2-user y ejecute los siguientes comandos. `sudo su - root` `sudo tee /etc/yum.repos.d/pgdg.repo<<EOF`	Administrador de la nube, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	<pre>[pgdg12] name=PostgreSQL 12 for RHEL/CentOS 7 - x86_64 baseurl=https://down load.postgresql.or g/pub/repos/yum/12/ redhat/rhel-7-x86_64 enabled=1 gpgcheck=0 EOF sudo yum install -y postgresql12-server sudo yum install postgresql12-devel sudo /usr/pgsql-12/ bin/postgresql-12- setup initdb sudo systemctl enable postgresql-12 sudo systemctl start postgresql-12</pre>	
	3. Descarga el código `oracle_fdw` fuente de GitHub. <pre>mkdir -p /var/lib/ pgsql/oracle_fdw/ cd /var/lib/pgsql/ oracle_fdw/ wget https://g ithub.com/laurenz/ oracle_fdw/archive /refs/heads/master .zip unzip master.zip</pre>	

Tarea	Descripción	Habilidades requeridas
	4. Instale Oracle Instant Client y configure las variables de entorno de Oracle. `yum install https://download.oracle.com/otn_software/linux/instantclient/1912000/oracle-instantclient19.12-basic-19.12.0.0.0-1.x86_64.rpm` `yum install https://download.oracle.com/otn_software/linux/instantclient/1912000/oracle-instantclient19.12-devel-19.12.0.0.0-1.x86_64.rpm` `export ORACLE_HOME=/usr/lib/oracle/19.12/client64export LD_LIBRARY_PATH=/usr/lib/oracle/19.12/client64/lib:$LD_LIBRARY_PATH` 5. Verifique que `pg_config` se refiere a la versión correcta. `which pg_config` 6. Compile `oracle_fdw` .	

Tarea	Descripción	Habilidades requeridas
	`cd /var/lib/pgsql/oracle_fdw/oracle_fdw-master` `make` `make install` Nota: Si recibe un mensaje de error que indica que `oci.h` no existe, añada lo siguiente en `Makefile`: • Para `PG_CPPFLAGS` , añada `-I/usr/include/oracle/19.12/client64` • Para `SHLIB_LINK` , añada `-L/usr/lib/oracle/19.12/client64/lib` Para obtener más información, consulte el Repositorio de oracle_fdw. 7. Inicie sesión en la base de datos PostgreSQL y cree la extensión `oracle_fdw` . `sudo su - postgres` `psql postgres` `create extension oracle_fdw;` 8. Cree un usuario de PostgreSQL que sea	

Tarea	Descripción	Habilidades requeridas
	propietario de las tablas externas. `CREATE USER pguser WITH PASSWORD '<password>'; GRANT CONNECT ON DATABASE postgres TO pguser;` 9. Cree el contenedor de datos externo. Sustituya los siguientes valores por los detalles del servidor de Oracle Database: • `<Oracle DB Server IP>` • `<Oracle DB Port>` • `<Oracle_SID>` `create server oradb foreign data wrapper oracle_fdw options (dbserver '//<Oracle DB Server IP>:<Oracle DB Port>/<Oracle_SID>'); GRANT USAGE ON FOREIGN SERVER oradb TO pguser;` 10. Para crear la asignación de usuarios y una tabla externa que se asigne a la tabla de Oracle, conéctese a la base de datos PostgreSQL como	

Tarea	Descripción	Habilidades requeridas
	`pguser` y ejecute el siguiente comando. Tenga en cuenta que, en el código de ejemplo, `DMS_SAMPLE` se utiliza como el esquema de Oracle que contiene la tabla `NAME_DATA` y `dms_sample` es su contraseña. Sustitúyalos según sea necesario. `create user mapping for pguser server oradb options (user 'DMS_SAMPLE', password 'dms_sample');` Nota: El siguiente ejemplo crea una tabla externa en PostgreSQL para una tabla de base de datos Oracle. Se debe crear una tabla externa similar para cada tabla de Oracle que requiera acceso desde la instancia de PostgreSQL. `CREATE FOREIGN TABLE name_data( name_type CHARACTER VARYING(15) NOT NULL, name CHARACTER VARYING(45) NOT NULL ) SERVER oradb OPTIONS (schema`	

Tarea	Descripción	Habilidades requeridas
	'DMS_SAMPLE', table 'NAME_DATA'); select count(*) from name_data; 11. Configure la base de datos PostgreSQL en la instancia EC2 para que pueda localizar las bibliotecas de Oracle durante el inicio de la base de datos PostgreSQL. Esto es requerido por la extensión `oracle_fdw` . `sudo systemctl stop postgresql-12` Nota: Edite el archivo `/usr/lib/systemd/system/postgresql-12.service` para incluir las variables de entorno, de modo que el startup `systemctl` encuentre las bibliotecas de Oracle que necesita `oracle_fdw` . `# Oracle Environment Variables` `Environment=ORACLE_HOME=/u01/app/oracle/product/12.2.0.1/db_1` `Environment=LD_LIBRARY_PATH=/u01/app/oracle/product/12`	

Tarea	Descripción	Habilidades requeridas
	`.2.0.1/db_1/lib:/l ib:/usr/lib` `sudo systemctl start postgresql-12`	

Opción 1: configurar un enlace de base de datos con las extensiones oracle_fdw y postgres_fdw, un grupo de escalado automático y Route 53

Tarea	Descripción	Habilidades requeridas
Configure una zona alojada privada en Amazon Route 53.	1. Cree una zona alojada privada en Amazon Route 53. Anote el Nombre de dominio, que se asociará a una instancia EC2. 2. Agregue un registro «A» mediante una política de enrutamiento sencillo que se resuelva en la dirección IP de la instancia EC2, que contiene la extensión `oracle_fdw` PostgreSQL. 3. Tras guardar el registro «A», anote el ID de zona alojada del nombre de dominio del paso 1. Esto se utilizará para crear la política de IAM adecuada.	Administrador de la nube, administrador de bases de datos
Cree un rol de IAM que se adjuntará a una instancia EC2.	Para crear un rol de IAM que se adjuntará a la instancia EC2, utilice la siguiente política. Sustituya `<Hosted`	Administrador de la nube, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	zone ID> por la información capturada en la historia anterior. `{ "Version": "2012-10-17", "Statement": [ { "Sid": "VisualEditor0", "Effect": "Allow", "Action": "route53:ChangeResourceRecordSets", "Resource": "arn:aws:route53:: :hostedzone/<Hosted zone ID>" }, { "Sid": "VisualEditor1", "Effect": "Allow", "Action": "route53:ListHostedZones", "Resource": "*" } ] }`	

Tarea	Descripción	Habilidades requeridas
Cree una plantilla de lanzamiento de EC2.	1. Cree una AMI de la instancia EC2 que contenga la extensión PostgreSQL `oracle_fdw` . 2. Utilice AMI para crear una plantilla de lanzamiento en EC2. 3. Para permitir la conexión desde la instancia Aurora compatible con PostgreSQL a la base de datos PostgreSQL de la instancia EC2, asocie el rol de IAM que creó anteriormente y adjunte grupos de seguridad. 4. En la sección User Data (Datos de usuario), añada los siguientes comandos, cambiando `Hosted zone ID` y `Domain Name` a los valores correspondientes. Elija Create launch template (Crear plantilla de lanzamiento). `#!/bin/bash` `v_zone_id='Hosted zone ID'` `v_domain_name='Domain Name'` `v_local_ipv4=$(curl -s http://169.254.169.254/late`	Administrador de la nube, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	st/meta-data/local-ipv4) aws route53 change-resource-record-sets --hosted-zone-id $v_zone_id --change-batch '{"Changes":[{"Action":"UPSERT","ResourceRecordSet":{"Name":"'$v_domain_name'","Type":"A","TTL":10,"ResourceRecords":[{"Value":"'$v_local_ipv4'"}]}}]}'	

Tarea	Descripción	Habilidades requeridas
Configure el grupo de escalado automático.	1. A continuación, cree un grupo de escalado automático mediante esa plantilla de lanzamiento. 2. Configure la VPC y las subredes adecuadas que se utilizarán para lanzar la instancia EC2. La configuración de la opción 1 no usa un equilibrador de carga. 3. Establezca la capacidad Deseada, Mínima y Máxima en 1 en las Políticas de escalado. 4. Para enviar alertas al equipo de operaciones, añada notificaciones para eventos como Launch (Lanzar) o Terminate (Finalizar). 5. Revise la configuración y seleccione Create Auto Scaling group (Crear grupo de escalado automático). Al finalizar, el grupo de escalado automático inicia la instancia EC2 que contiene la extensión PostgreSQL `oracle_fdw` , que se conecta a base de datos Oracle.	Administrador de la nube, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	Nota: Cuando necesite acceder a una nueva tabla de Oracle o cambiar la estructur a de una tabla de Oracle, esos cambios deben reflejarse en la tabla externa de PostgreSQL. Tras implementar los cambios, debe crear una nueva AMI de la instancia EC2 y utilizarla para configurar la plantilla de lanzamiento.	

Tarea	Descripción	Habilidades requeridas
Configure la extensión postgres_fdw en la instancia compatible con Aurora PostgreSQL.	1. Configure `postgres_fdw` en la instancia compatible con Aurora PostgreSQL. Esto se conecta a la base de datos PostgreSQL de Amazon EC2, que actúa como nodo intermedio entre la instancia Aurora compatible con PostgreSQL y la base de datos Oracle. 2. Conéctese a la instancia de Aurora compatible con PostgreSQLy ejecute los siguientes comandos. `create extension postgres_fdw;` `CREATE SERVER pgoradb FOREIGN DATA WRAPPER postgres_fdw OPTIONS (dbname 'postgres', host 'Domain Name', port '5432');` `CREATE USER MAPPING for postgres SERVER pgoradb OPTIONS (user 'pguser', password '<password>');` `CREATE FOREIGN TABLE data_mart.name_data( name_type CHARACTER VARYING(15) NOT NULL,`	Administrador de la nube, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	<pre>name CHARACTER VARYING(45) NOT NULL) SERVER pgoradb OPTIONS (schema_name 'public', table_name 'name_data'); select count(*) from data_mart.name_data;</pre> Esto completa la configuración de un enlace de base de datos desde Aurora compatible con PostgreSQL a base de datos Oracle. La solución proporciona una estrategia de recuperación de desastres (DR) en caso de que la instancia EC2 que aloja la base de datos PostgreSQL falle. El grupo de escalado automático inicia una nueva instancia de EC2 y actualiza el DNS con la dirección IP de la nueva instancia de EC2. Esto garantiza que las tablas externas de la instancia Aurora compatible con PostgreSQL puedan acceder a las tablas de Oracle sin intervención manual.	

Opción 2: configure un enlace de base de datos con las extensiones oracle_fdw, un grupo de escalado automático y un equilibrador de carga de red.

Tarea	Descripción	Habilidades requeridas
Cree una plantilla de lanzamiento de EC2.	1. Cree una AMI de la instancia EC2 que contenga la extensión PostgreSQL `oracle_fdw` . 2. Utilice AMI para crear una plantilla de lanzamiento en EC2.	Administrador de la nube, administrador de bases de datos
Configure un grupo objetivo, un equilibrador de carga de red y un grupo de escalado automático.	1. Para crear un grupo objetivo, elija Instancia s como tipo de destino. En Protocol (Protocolo), seleccione TCP y para Port (Puerto), elija 5432. A continuación, elija la VPC en la que desee que esté el grupo objetivo y seleccione el Comprobación de estado correspondiente. 2. Crear un equilibrador de carga de red interno en su VPC. Configure el equilibrador de carga para que escuche en el protocolo:puerto TCP:5432. Configure Default action (Acción predeterminada) como Forward to (Reenviar a), y elija el grupo de destino que ha creado.	Administrador de la nube, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	3. A continuación, cree un grupo de escalado automático mediante la plantilla de lanzamiento que ha creado. 4. Configure el grupo de escalado automático con la VPC correspondiente y las subredes adecuadas que se utilizarán para lanzar las instancias EC2. 5. Para la opción de Equilibrio de carga, elija Adjuntar a un equilibrador de carga existente y seleccione el Grupo objetivo que creó. En Health Check (Comprobación de estado), seleccione ELB. 6. Defina la capacidad Deseada y Mínima en 2 y establezca la capacidad Máxima en un número superior, según sea necesario para soportar la carga con alta disponibilidad, en Políticas de escalado. 7. Para enviar alertas al equipo de operaciones, añada notificaciones para eventos como Launch (Lanzar) o Terminate (Finalizar).	

Tarea	Descripción	Habilidades requeridas
	8. Revise la configuración y seleccione Create Auto Scaling group (Crear grupo de escalado automático). Al finalizar, el grupo de escalado automático inicia el número deseado de instancias EC2 que contienen la extensión PostgreSQL `oracle_fdw` , que se conecta a base de datos Oracle. Nota: Cuando necesite acceder a una nueva tabla de Oracle o cambiar la estructura de una tabla de Oracle, esos cambios deben reflejarse en la tabla externa de PostgreSQL. Tras implementar los cambios, debe crear una nueva AMI de la instancia EC2 y utilizarla para configurar la plantilla de lanzamiento.	

Tarea	Descripción	Habilidades requeridas
Configure la extensión postgres_fdw en la instancia compatible con Aurora PostgreSQL.	Configure `postgres_fdw` en la instancia compatible con Aurora PostgreSQL. Se conecta a la base de datos PostgreSQL en EC2 a través de un equilibrador de carga de red. Esto se conecta a la base de datos PostgreSQL de EC2, que actúa como nodo intermedio entre la instancia Aurora compatible con PostgreSQL y la base de datos Oracle. Conéctese a la instancia de Aurora compatible con PostgreSQLy ejecute los siguientes comandos. `create extension postgres_fdw;` `CREATE SERVER pgoradb FOREIGN DATA WRAPPER postgres_fdw OPTIONS (dbname 'postgres', host 'DNS name of Network Load Balancer', port '5432');` `CREATE USER MAPPING for postgres SERVER pgoradb OPTIONS (user 'pguser', password '<password>');` `CREATE FOREIGN TABLE data_mart.name_data(`	Administrador de la nube, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	<pre>name_type CHARACTER VARYING(15) NOT NULL, name CHARACTER VARYING(45) NOT NULL) SERVER pgoradb OPTIONS (schema_name 'public', table_name 'name_data'); select count(*) from data_mart.name_data;</pre> Esto completa la configuración de un enlace de base de datos desde Aurora compatible con PostgreSQL a una base de datos de Oracle. En caso de que el alojamiento EC2 de la base de datos PostgreSQL falle, el equilibrador de carga de red identifica el error y detiene el tráfico hacia la instancia EC2 que ha fallado. El grupo de escalado automático inicia una instancia EC2 nueva y la registra en el equilibrador de carga. Esto garantiza que después de que falle la instancia EC2 original, las tablas externas de la instancia Aurora compatible con PostgreSQL puedan acceder a las tablas de Oracle sin intervención manual.	

Opción 3: configurar un enlace de base de datos con la extensión oracle_fdw en una base de datos Aurora compatible con PostgreSQL

Tarea	Descripción	Habilidades requeridas
Configure la extensión oracle_fdw en la instancia compatible con Aurora PostgreSQL.	Para la versión 12.7 y posteriores de la base de datos Aurora compatible con PostgreSQL, la extensión `oracle_fdw` está disponible de forma nativa. Esto elimina la necesidad de crear la base de datos PostgreSQL intermedia en una instancia EC2. La instancia de Aurora compatible con PostgreSQL puede conectarse a la base de datos Oracle directamente. 1. Para crear la extensión `oracle_fdw` , inicie sesión en la instancia Aurora compatible con PostgreSQL y ejecute el siguiente comando. `create extension oracle_fdw;` 2. Cree el contenedor de datos externo. Sustituya los siguientes valores por los detalles del servidor de Oracle Database: • `<Oracle DB Server IP>` • `<Oracle DB Port>`	Administrador de la nube, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	• <Oracle_SID> `create server oradb foreign data wrapper oracle_fdw options (dbserver '//<Oracle DB Server IP>:<Oracle DB Port>/<Oracle_SID>');` 3. Para crear el mapeo de usuarios y una tabla externa que se asigne a la tabla de Oracle, ejecute el siguiente comando. Tenga en cuenta que, en el código de ejemplo, `DMS_SAMPLE` se utiliza como el esquema de Oracle que contiene la tabla `NAME_DATA` y `dms_sample` es su contraseña. Sustitúya los según sea necesario. Además, la tabla externa debe crearse en la instancia Aurora compatible con PostgreSQL para acceder a todas las demás tablas de Oracle. `create user mapping for postgres server oradb options (user 'DMS_SAMPLE', password 'dms_sample');`	

Tarea	Descripción	Habilidades requeridas
	`CREATE FOREIGN TABLE name_data( name_type character varying(15) OPTIONS (key 'true') NOT NULL, name character varying(45) OPTIONS (key 'true') NOT NULL )SERVER oradb OPTIONS (schema 'DMS_SAMPLE', table 'NAME_DATA');` Se debe crear una tabla externa similar para cada tabla de Oracle que requiera acceso desde la instancia de PostgreSQL.	

Configure base de datos Oracle Gateways para la conectividad desde la base de datos Oracle local a la Aurora compatible con PostgreSQL

Tarea	Descripción	Habilidades requeridas
Configure la puerta de enlace en el servidor de base de datos Oracle en las instalaciones.	1. Como usuario raíz, instale la última versión del administrador de controladores unixODBC. `sudo yum install unixODBC*` 2. Instale el controlador ODBC de PostgreSQL (`psqlODBC`).	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`sudo wget https://download.postgresql.org/pub/repos/yum/reporpms/EL-7-x86_64/pgdg-redhat-repo-latest.noarch.rpm` `sudo yum install pgdg-redhat-repo-latest.noarch.rpm` `sudo yum install postgresql12-odbc` 3. Cree un nombre de origen de datos (DSN) de ODBC para el controlador. El administrador de controladores unixODBC proporciona las utilidades de línea de comandos `odbcinst`, `odbc_config` y `isql` que se utilizan para configurar y probar el controlador. Con nuestras utilidades `odbcinst` y `odbc_config` , puede localizar los archivos del administrador de controladores unixODBC para pasar la información del controlador y crear el DSN. `odbcinst -j`	

Tarea	Descripción	Habilidades requeridas
	A continuación, se muestra un ejemplo de resultado. `unixODBC 2.3.1` `DRIVERS.....` `.......: /etc/odbc` `inst.ini` `SYSTEM DATA` `SOURCES: /etc/odbc` `.ini` `FILE DATA SOURCES..` `: /etc/ODBCDataSourc` `es` `USER DATA SOURCES..` `: /root/.odbc.ini` `SQLULEN Size.......:` `8` `SQLLEN Size........:` `8` `SQLSETPOSIROW Size.:` `8` `odbc_config --odbcini` `--odbcinstini` `/etc/odbc.ini` `/etc/odbcinst.ini` En el resultado del ejemplo, puede ver los archivos `odbcinst.ini` y `odbc.ini`. Básicamente, `odbcinst.ini` es un archivo de registro y configuración para los controladores ODBC de un entorno, mientras que `odbc.ini` es un archivo de registro y configuración	

Tarea	Descripción	Habilidades requeridas
	para los DSN de ODBC. Para habilitar los controladores, debe modificar estos dos archivos. 4. Configure las bibliotecas de controladores `psqlODBC` en el archivo del controlador ODBC `/etc/odbcinst.ini` y añada las siguientes líneas al final del archivo. Estas líneas constituyen una entrada para el controlador. `[PostgreSQL]` `Description = ODBC for PostgreSQL` `Driver = /usr/lib/psqlodbcw.so` `Setup = /usr/lib/libodbcpsqlS.so` `Driver64 = /usr/lib64/psqlodbcw.so` `Setup64 = /usr/lib64/libodbcpsqlS.so` `FileUsage = 1` 5. Cree un DSN en el archivo `/etc/odbc.ini`. El administrador del controlador lee este archivo para determinar cómo conectarse a la base de datos utilizando los detalles	

Tarea	Descripción	Habilidades requeridas
	del controlador especific ados en `odbcinst.ini` . Sustituya los siguientes parámetros por valores reales: • `<PostgreSQL Port>` • `<PostgreSQL Database Name>` • `<Aurora PostgreSQL Endpoint>` • `<PostgreSQL username>` • `<PostgreSQL password>` `[pgdsn]` `Driver=/usr/pgsql-12/lib/psqlodbc.so` `Description=PostgreSQL ODBC Driver` `Database=<PostgreSQL Database Name>` `Servername=<Aurora PostgreSQL Endpoint>` `Username=<PostgreSQL username>` `Password=<PostgreSQL password>` `Port=<PostgreSQL Port>` `UseDeclareFetch=1` `CommLog=/tmp/pgodbclink.log` `Debug=1` `LowerCaseIdentifier=1`	

Tarea	Descripción	Habilidades requeridas
	6. Con la utilidad `isql`, pruebe la conexión ODBC (`psqlODBC`) al DSN de la base de datos PostgreSQL que creó. `isql -v pgdsn` A continuación, se muestra un ejemplo de resultado. `+----------------- ------------------ ----+ | Connected! | | | | sql-statement | | help [tablename] | | quit | | | +--------------- ------------------ ------+ quit` 7. Con el DSN, cree la puerta de enlace para el controlador de servicios ODBC (HS). Como usuario `oracle`, cree un archivo `initDSN.ora` en la ubicación `$ORACLE_H`	

Tarea	Descripción	Habilidades requeridas
	OME/hs/admin . En este caso, pgdsn es el DSN, por lo que debe crear un archivo llamado initpgdsn.ora . `more initpgdsn.ora` A continuación, se muestra un ejemplo de resultado. `# This is a sample agent init file that contains the HS parameters that are # needed for the Database Gateway for ODBC # # HS init parameters # HS_FDS_CONNEC T_INFO=pgdsn HS_FDS_TRACE_L EVEL=OFF HS_FDS_TRACE_FILE_ NAME=/tmp/ora_hs_t race.log HS_FDS_SHAREABLE_N AME=/usr/lib64/lib odbc.so HS_NLS_NCHAR=UCS2 HS_LANGUAGE=AMERICA N_AMERICA.AL32UTF8 # # ODBC specific environment variables`	

Tarea	Descripción	Habilidades requeridas
	`#` `set ODBCINI=/etc/odbc.ini`	
	8. Ajuste el oyente (`$ORACLE_HOME/network/admin/listener.ora`) añadiendo la entrada DSN en `SID_LIST_LISTENER`. `more $ORACLE_HOME/network/admin/listener.ora` A continuación, se muestra un ejemplo de resultado. `SID_LIST_LISTENER = (SID_LIST = (SID_DESC= (SID_NAME = pgdsn) (ORACLE_HOME = /u01/app/oracle/product/12.2.0.1/db_1) (ENVS="LD_LIBRARY_PATH=/lib64:/usr/lib:/usr/lib64:/u01/app/oracle/product/12.2.0.1/db_1") (PROGRAM=dg4odbc) ) )`	

Tarea	Descripción	Habilidades requeridas
	9. Ajuste el `tnsname` (`$ORACLE_HOME/network/admin/tnsnames.ora`) añadiendo la entrada DSN. `more $ORACLE_HOME/network/admin/tnsnames.ora` A continuación, se muestra un ejemplo de resultado. `pgdsn=(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=localhost)(PORT=1521))(CONNECT_DATA=(SID=pgdsn))(HS=OK))` 10. Reinicie el oyente de Oracle para que las entradas relacionadas con el DSN realizadas en los archivos de red puedan surtir efecto y cambiando `<Listener Name>` por el nombre del oyente de Oracle correspondiente. `lsnrctl stop <Listener Name>` `lsnrctl start <Listener Name>` Tras reiniciar el oyente de Oracle, se creará un	

Tarea	Descripción	Habilidades requeridas
	controlador HS de Oracle con un nombre de DSN (`pgdsn`). 11. Utilice el DSN para crear un enlace a la base de datos Oracle para acceder a la base de datos PostgreSQL iniciando sesión en base de datos Oracle. `create public database link pgdb connect to "postgres" identified by "postgres" using 'pgdsn';` 12. Acceda a los datos de PostgreSQL mediante el enlace de base de datos Oracle creado. `select count(*) from "pg_tables"@pgdb;`	

Recursos relacionados

- Amazon Aurora PostgreSQL
- Amazon Elastic Compute Cloud (Amazon EC2)
- AWS Identity and Access Management (IAM)
- Lanzar una instancia desde una plantilla de lanzamiento
- Grupos de escalado automático
- Amazon Route 53
- Amazon Simple Notification Service (SNS)

- Equilibrador de carga de red de AWS
- Bases de datos Oracle Gateways

Información adicional

Si bien la extensión `oracle_fdw` está disponible con la versión 12.7 y posteriores Aurora compatibles con PostgreSQL, este patrón incluye soluciones para versiones anteriores de bases de datos Aurora compatibles con PostgreSQL, ya que muchos clientes admiten versiones anteriores de bases de datos Aurora compatibles con PostgreSQL, y la actualización de una base de datos implica varios niveles de pruebas de rendimiento y aplicaciones. Además, la característica de enlace a bases de datos se utiliza ampliamente y el objetivo de este artículo es proporcionar opciones para todas las versiones de Aurora compatibles con PostgreSQL.

Exportación de una base de datos de Microsoft SQL Server a Amazon S3 mediante AWS DMS

Creado por Sweta Krishna (AWS)

Entorno: PoC o piloto	Origen: Microsoft SQL Server	Destino: Amazon S3
Tipo R: redefinir la plataforma	Carga de trabajo: Microsoft	Tecnologías: migración; bases de datos
Servicios de AWS: AWS DMS; Amazon S3		

Resumen

Con frecuencia, las organizaciones necesitan copiar bases de datos a Amazon Simple Storage Service (Amazon S3) para la migración de bases de datos, la copia de seguridad y la restauración, el archivado y el análisis de datos. Este patrón describe cómo puede exportar una base de datos de Microsoft SQL Server a Amazon S3. La base de datos de origen se puede alojar de forma en las instalaciones o en Amazon Elastic Compute Cloud (Amazon EC2) o en Amazon Relational Database Service (Amazon RDS) para Microsoft SQL Server en la nube de Amazon Web Services (AWS).

Los datos se exportan mediante AWS Database Migration Service (AWS DMS). De forma predeterminada, AWS DMS escribe los datos de captura de datos de carga completa y cambios (CDC) en formato de valores separados por comas (.csv). Para un almacenamiento más compacto y opciones de consulta más rápidas, este patrón utiliza la opción de formato Apache Parquet (.parquet).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un rol de AWS Identity and Access Management (IAM) para la cuenta con acceso de escritura, eliminación y etiquetado al bucket de S3 de destino, y se ha agregado AWS DMS (`dms.amazonaws.com`) como entidad de confianza a este rol de IAM

- Una base de datos Microsoft SQL Server en las instalaciones (o Microsoft SQL Server en una instancia EC2 o una base de datos Amazon RDS para SQL Server)
- Conectividad de red entre la nube privada virtual (VPC) de AWS y la red en las instalaciones proporcionada por AWS Direct Connect o una red privada virtual (VPN)

Limitaciones

- Actualmente, las versiones de AWS DMS anteriores a la 3.4.7 no admiten un bucket S3 habilitado para VPC (VPC de puerta de enlace).
- No se admiten cambios en la estructura de la tabla de origen durante la carga completa.
- No se admite el modo de objetos binarios grandes (LOB) completo de AWS DMS.

Versiones de producto

- Versiones de Microsoft SQL Server 2005 o posterior, para las ediciones Enterprise, Standard, Workgroup y Developer.
- La compatibilidad con Microsoft SQL Server versión 2019 como origen está disponible en las versiones 3.3.2 y posteriores de AWS DMS.

Arquitectura

Pila de tecnología de origen

- Una base de datos Microsoft SQL Server en las instalaciones (o Microsoft SQL Server en una instancia EC2 o una base de datos Amazon RDS para SQL Server)

Pila de tecnología de destino

- AWS Direct Connect
- AWS DMS
- Amazon S3

Arquitectura de destino

Herramientas

- AWS Database Migration Service (AWS DMS) le permite migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones.
- AWS Direct Connect vincula su red interna con una ubicación de AWS Direct Connect a través de un cable estándar Ethernet de fibra óptica. Con esta conexión, puede crear interfaces virtuales directamente en servicios públicos de AWS derivando a los proveedores de Internet a su ruta de acceso a la red.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Epics

Preparar la migración

Tarea	Descripción	Habilidades requeridas
Valide la versión de la base de datos.	Valide la versión de la base de datos de origen y asegúrese de que es compatible con AWS DMS. Para obtener información sobre las versiones de bases de datos de SQL Server compatibles, consulte Uso de una base de datos de Microsoft SQL Server como fuente de AWS DMS.	Administrador de base de datos
Crear una VPC y un grupo de seguridad.	En su cuenta de AWS, cree una VPC y un grupo de seguridad. Para obtener más información, consulte la documentación de Amazon VPC.	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Cree un usuario para la tarea de AWS DMS.	Cree un usuario de AWS DMS en la base de datos de origen y concédale permisos de LECTURA. AWS DMS utilizará este usuario.	Administrador de base de datos
Pruebe la conectividad de la base de datos.	Pruebe la conectividad con la instancia de base de datos SQL Server desde el usuario de AWS DMS.	Administrador de base de datos
Crear un bucket de S3.	Crear el bucket S3 objetivo. Este bucket contendrá los datos de la tabla migrados.	Administrador de sistemas
Crear una política y un rol de IAM.	1. Para crear una política de IAM con permisos de bucket, use el código de la sección Información adicional. 2. Cree un rol AWS DMS y asocie la política a dicho rol.	Administrador de sistemas

Migre los datos mediante AWS DMS

Tarea	Descripción	Habilidades requeridas
Cree una instancia de replicación de AWS DMS.	Inicie sesión en la Consola de administración de AWS y abra la consola de AWS DMS. En el panel de navegación, seleccione Instancias de replicación y Crear instancia de replicación. Para obtener	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	instrucciones, consulte el paso 1 de la documentación de AWS DMS.	
Crear los puntos de conexión de origen y de destino.	Crear los puntos de conexión de origen y de destino. Pruebe la tarea desde la instancia de replicación a los puntos de conexión de origen y destino. Para obtener instrucciones, consulte el paso 2 de la documentación de AWS DMS.	Administrador de base de datos
Crear una tarea de replicación.	Cree una tarea de replicación y seleccione carga completa o carga completa con captura de datos de cambios (CDC) para migrar los datos de SQL Server al bucket S3. Para obtener instrucciones, consulte el paso 3 de la documentación de AWS DMS.	Administrador de base de datos
Iniciar la tarea de replicación.	Inicie la tarea de replicación y supervise los registros para detectar cualquier error.	Administrador de base de datos

Valide los datos

Tarea	Descripción	Habilidades requeridas
Valide los datos migrados.	En la consola de Amazon S3, acceda a su bucket. Abra la subcarpeta que tiene el mismo nombre que la base de datos	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	de origen. Confirme que la carpeta contiene todas las tablas que se migraron de la base de datos de origen.	

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Cierre y elimine los recursos temporales de AWS.	Cierre los recursos temporales de AWS que haya creado para la migración de datos, como la instancia de replicación de AWS DMS, y elimínelos después de validar la exportación.	Administrador de base de datos

Recursos relacionados

- Guía de usuario del servicio de migración de bases de datos de AWS
- Uso de una base de datos de Microsoft SQL Server como origen para AWS DMS
- Uso de Amazon S3 como destino para el servicio de migración de bases de datos de AWS
- Uso de un bucket S3 como destino de AWS DMS (AWS re:POST)

Información adicional

Utilice el siguiente código para añadir una política de IAM con permisos de bucket S3 para la función DMS de AWS. Reemplace `bucketname` con el nombre de su bucket.

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Effect": "Allow",
```

```
            "Action": [
                "s3:PutObject",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::bucketname*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::bucketname*"
            ]
        }
    ]
}
```

Migre cargas de trabajo de aprendizaje automático: cree, entrene e implemente a Amazon SageMaker con las herramientas para desarrolladores de AWS

Creado por Scot Marvin (AWS)

Tipo R: redefinir la plataforma	Origen: Machine Learning	Objetivo: Amazon SageMaker
Creado por: AWS	Entorno: PoC o piloto	Tecnologías: aprendizaje automático e inteligencia artificial DevOps; migración
Servicios de AWS: Amazon SageMaker		

Resumen

Este patrón proporciona orientación para migrar una aplicación de aprendizaje automático (ML) local que se ejecuta en servidores Unix o Linux para capacitarla e implementarla en AWS mediante Amazon. SageMaker Esta implementación utiliza una canalización de integración continuas (CI/CD). El patrón de migración se implementa mediante una CloudFormation pila de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa que utilice AWS Landing Zone
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada en un servidor Unix o Linux
- Un repositorio de código fuente de aprendizaje automático GitHub en AWS CodeCommit o Amazon Simple Storage Service (Amazon S3)

Limitaciones

- Solo se pueden implementar 300 canalizaciones individuales en una región de AWS.

- Este patrón está pensado para cargas de trabajo de aprendizaje automático supervisadas con train-and-deploy código en Python.

Versiones de producto

- Docker versión 19.03.5, compilación 633a0ea, con Python 3.6x

Arquitectura

Pila de tecnología de origen

- Instancia informática de Linux en las instalaciones con datos en el sistema de archivos local o en una base de datos relacional

Arquitectura de origen

Pila de tecnología de destino

- AWS CodePipeline se implementó con Amazon S3 para el almacenamiento de datos y Amazon DynamoDB como almacén de metadatos para rastrear o registrar las ejecuciones de las canalizaciones

Arquitectura de destino

Arquitectura de migración de aplicaciones

- Paquete de Python nativo y CodeCommit repositorio de AWS (y un cliente SQL, para conjuntos de datos locales en una instancia de base de datos)

Herramientas

- Python

- Git
- AWS CLI: la CLI de AWS implementa la CloudFormation pila de AWS y mueve los datos al bucket de S3. El bucket de S3, a su vez, conduce al objetivo.

Epics

Planificar la migración

Tarea	Descripción	Habilidades requeridas
Valide el código fuente y los conjuntos de datos.		Científico de datos
Identifique los tipos y tamaños de las instancias de creación, entrenamiento e implement ación de destino.		Ingeniero de datos, científico de datos
Cree una lista de capacidades y requisitos de capacidad.		
Identifique los requisitos de la red.		Administrador de base de datos, administrador de sistemas
Identifique requisitos de seguridad para acceder a la red o al host para las aplicacio nes de origen y destino.		Ingeniero de ML, ingeniero de datos, administrador de sistemas
Determine la estrategia de copia de seguridad.		Ingeniero de ML, administr ador de sistemas
Determine los requisitos de disponibilidad.		Ingeniero de ML, administr ador de sistemas

Tarea	Descripción	Habilidades requeridas
Identifique la estrategia de migración o transición de aplicaciones.		Científico de datos, ingeniero de machine learning

Configure la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC).		Ingeniero de ML, administr ador de sistemas
Creación de los grupos de seguridad.		Ingeniero de ML, administr ador de sistemas
Configure un bucket de Amazon S3 y ramas de CodeCommit repositorio de AWS para el código de aprendizaje automático.		Ingeniero de ML

Cargue los datos y el código

Tarea	Descripción	Habilidades requeridas
Utilice herramientas nativas de MySQL o herramientas de terceros para migrar, entrenar, validar y probar conjuntos de datos al bucket de S3 aprovisionado.	Esto es necesario para la implementación de AWS CloudFormation Stack.	Ingeniero de datos, ingeniero de machine learning
Package el tren de aprendiza je automático y el código de alojamiento como paquetes de	Necesita el nombre de la rama del repositorio para implement	Científico de datos, ingeniero de machine learning

Tarea	Descripción	Habilidades requeridas
Python y envíelos al repositor io aprovisionado en AWS CodeCommit o GitHub.	ar la CloudFormation plantilla de AWS para la migración.	

Migración de aplicaciones

Tarea	Descripción	Habilidades requeridas
Siga la estrategia de migración de la carga de trabajo de ML.		Propietario de la aplicación, ingeniero de machine learning
Implemente la CloudFormation pila de AWS.	Utilice la CLI de AWS para crear la pila declarada en la plantilla YAML proporcionada con esta solución.	Científico de datos, ingeniero de machine learning

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Cambiar los clientes de la aplicación a la nueva infraestr uctura.		Propietario de la aplicación, científico de datos, ingeniero de machine learning

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cerrar los recursos temporale s de AWS.	Cierre todos los recursos personalizados de la CloudFormation plantilla de AWS (por ejemplo, cualquier	Científico de datos, ingeniero de machine learning

Tarea	Descripción	Habilidades requeridas
	función de AWS Lambda que no se esté utilizando).	
Revise y valide los documentos del proyecto.		Propietario de la aplicación, científico de datos
Valide los resultados y las métricas de evaluación del modelo de ML con los operadores.	Asegúrese de que el rendimiento del modelo cumpla con las expectativas de los usuarios de la aplicación y sea comparable al estado en las instalaciones.	Propietario de la aplicación, científico de datos
Cerrar el proyecto y enviar comentarios.		Propietario de la aplicación, ingeniero de machine learning

Recursos relacionados

- AWS CodePipeline
- AWS CodeBuild
- Amazon SageMaker
- Amazon S3
- Amazon DynamoDB
- AWS Lambda

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Migre OpenText TeamSite las cargas de trabajo a la nube de AWS

Creado por Battulga Purevragchaa (AWS), Michael Stewart y Carlos Marruenda Molina

Entorno: producción	Origen: en las instalaciones	Destino: AWS
Tipo R: redefinir la plataforma	Carga de trabajo: todas las demás cargas de trabajo	Tecnologías: migración; aplicaciones web y móviles
Servicios de AWS: Amazon EC2; Amazon RDS		

Resumen

> Advertencia: este escenario requiere que los usuarios de IAM dispongan de acceso programát ico y credenciales de larga duración, lo que supone un riesgo para la seguridad. Para ayudar a mitigar este riesgo, le recomendamos que brinde a estos usuarios únicamente los permisos que necesitan para realizar la tarea y que los elimine cuando ya no los necesiten. Las claves de acceso se pueden actualizar si es necesario. Para obtener más información, consulte Actualiza ción de las claves de acceso en la guía del usuario de IAM.

Muchas instancias de OpenText Experience Platform se alojan de forma local o en soluciones de alojamiento tradicionales con capacidad fija y modelos de costes tradicionales. La migración de las cargas de trabajo de OpenText Experience Platform a la nube de Amazon Web Services (AWS) proporciona capacidades y valor adicionales al aumentar la agilidad empresarial y las oportunidades de integración, además de reducir el coste total de propiedad.

Este patrón proporciona los pasos y una plantilla para migrar OpenText TeamSitelas cargas de trabajo a la nube de AWS. El patrón le ayuda a entender cómo planificar y presupuestar sus proyectos de migración, ya que incluye una sección detallada de Epics que le guía a lo largo del proceso de OpenText TeamSite migración.

Este patrón fue desarrollado por AWS y TBSCG, un socio de AWS, y acompaña a la guía Migración OpenText TeamSite y administración de contenido multimedia a la nube de AWS en el sitio web de AWS Prescriptive Guidance.

Requisitos previos y limitaciones

Requisitos previos

- Al menos una cuenta de AWS activa.
- OpenText Carga de trabajo alojada en un centro de datos local o en otro proveedor de nube
- Licencias activas OpenText

El proceso de migración también requiere las funciones y responsabilidades que se describen en la siguiente tabla.

Rol	Responsabilidades
Patrocinador	Patrocinio interno
Encargado de entrega	Entrega de la migración
Arquitectura de soluciones	Defina la arquitectura actual y la nueva
DevOps ingeniero	DevOps actividades
Comprobador de calidad	Pruebas a nivel de sistema
Propietario del producto	Priorización de tareas en función de los requisitos empresariales
TeamSite autores	Pruebas de aceptación de usuario (UAT) de migración
TeamSite administrador	Migración UAT
OpenText liderar	OpenText especialista en productos
OpenText desarrollador	OpenText especialista en productos
Especialista en precios	AWS y las OpenText licencias
Seguridad de TI	Línea de base de TI
Desarrollador de integración de terceros	Rediseño de las integraciones existentes

Desarrollador de aplicaciones front-end	Realice cambios en el código de front-end migrado
Administrador de base de datos	Configuración de las bases de datos

Limitaciones

- Garantice la compatibilidad con los sistemas operativos (SO) de destino. Puede utilizar la matriz de compatibilidad de las notas de lanzamiento del producto de la versión OpenText del producto que vaya a migrar.

Arquitectura

Pila de tecnología de origen

- OpenText soluciones de experiencia de cliente alojadas en las instalaciones o en otro proveedor de nube:
  - OpenText TeamSite
  - OpenText LiveSite
  - OpenText Gestión de contenido multimedia
  - OpenText MediaBin

Pila de tecnología de destino

- Una plataforma de experiencia OpenText del cliente alojada en la nube de AWS y que utiliza los siguientes servicios de AWS:
  - Amazon Elastic Compute Cloud (Amazon EC2)
  - Amazon Elastic Container Service (Amazon ECS)
  - OpenSearch Servicio Amazon
  - Elastic Load Balancing
  - AWS Lambda
  - Amazon API Gateway
  - Amazon Relational Database Service (Amazon RDS)
  - Amazon Elastic Block Store (Amazon EBS)

- Amazon Simple Storage Service (Amazon S3)

Arquitectura de destino

Herramientas

- AWS Database Migration Service (AWS DMS) es un servicio en la nube que facilita la migración de bases de datos relacionales, almacenes de datos, bases de datos NoSQL y otros tipos de almacenes de datos.
- AWS Application Migration Service automatiza la conversión de sus servidores de origen para que se ejecuten de forma nativa en AWS. También simplifica la modernización de las aplicaciones con opciones de optimización integradas y personalizadas.

Epics

Descubrimiento y evaluación

Tarea	Descripción	Habilidades requeridas
Organice talleres sobre los requisitos de descubrimiento.	Organice talleres con equipos empresariales y técnicos para descubrir el panorama actual, recopilar los requisito s y validar la estrategia de migración. Según la complejidad y el alcance de la migración, es posible que su organización necesite varios talleres. Duración: dos semanas	Patrocinador (opcional), gerente de entrega, arquitecto de soluciones, OpenText líder, propietario del producto
Analice los requisitos de solución y migración.	Analice y documente los requisitos empresariales, funcionales y técnicos que influyen en el diseño de la	Arquitecto de soluciones, OpenText líder, propietario del producto

Tarea	Descripción	Habilidades requeridas
	solución planificada y el proceso de migración. Duración: una semana	
Documente su OpenText arquitectura actual.	Documente su OpenText arquitectura actual, incluidos los componentes principal es y todas las aplicaciones y servicios relacionados. Duración: una semana	Arquitecto de soluciones, OpenText director y propietar io del producto
Defina la arquitectura de AWS planificada.	Defina la arquitectura de AWS planificada en función de los componentes identificados, los requisitos y el uso de la matriz de OpenText compatibilidad. Puede encontrar la matriz de OpenText compatibilidad en las notas de lanzamiento de su OpenText TeamSite versión. Duración: una semana	Arquitecto de soluciones, OpenText líder, propietario del producto, seguridad de TI
Evalúe el tamaño de la arquitectura de AWS planifica da.	Los requisitos de tamaño varían para los distintos componentes de la arquitect ura en función de la carga de trabajo y otros requisitos no funcionales. Duración: dos días	Arquitecto de soluciones, OpenText director

Tarea	Descripción	Habilidades requeridas
Calcular el costo total de la propiedad (TCO):	Calcule el costo total de propiedad (TCO) de la solución propuesta. Duración: dos días	Arquitecto de soluciones, especialista en precios
Defina la estrategia de migración de cada component e.	Defina y documente cuáles de las siete estrategias de migración comunes (7 R) se deben utilizar para cada componente principal o adicional que se debe migrar a la nube de AWS. Duración: una semana	Arquitecto de soluciones, OpenText líder, propietario del producto
Defina el proceso de migración de los component es.	Defina el proceso de migración detallado para cada uno de los componentes de la carga de trabajo. Duración: una semana	Arquitecto de soluciones, OpenText líder, propietario del producto, seguridad de TI
Defina el proceso de migración global y las dependencias.	Cree un proceso y un calendario de migración global que incluya los detalles de la migración de los component es, las dependencias y la continuidad empresarial. Duración: tres días	Arquitecto de soluciones, OpenText líder, propietario del producto, seguridad de TI

Actividades de seguridad y conformidad

Tarea	Descripción	Habilidades requeridas
Cree políticas de seguridad.	Configure las políticas de seguridad administradas por el cliente en sus cuentas de AWS. Deberían incluir la complejidad y la rotación de las contraseñas, además de desactivar automáticamente las cuentas no utilizadas. Para obtener más información sobre las políticas administr adas por el cliente, consulte Políticas administradas por el cliente en la documentación de AWS Identity and Access Management (IAM).	Arquitectura de soluciones
Cree usuarios de IAM.	Cree los usuarios de IAM que requieren acceso a la consola de administración de AWS, a la Interfaz de la línea de comandos de AWS (AWS CLI) y al SDK de AWS. Para obtener más informaci ón acerca de cómo crear un usuario de IAM, consulte Creación de un usuario de IAM en su cuenta de AWS en la documentación de IAM.	Arquitectura de soluciones
Cree grupos de IAM.	Cree los grupos de usuarios de IAM necesarios (por ejemplo, grupos de administr	Arquitectura de soluciones

Tarea	Descripción	Habilidades requeridas
	adores o desarrolladores) y añada usuarios de IAM a esos grupos. Para obtener más información sobre los grupos de usuarios de IAM, consulte Grupos de usuarios de IAM en la documentación de IAM.	
Adjuntar políticas de seguridad	Adjunte políticas de seguridad a los grupos o roles de IAM. Para obtener más información, consulte Adjuntar una política a un grupo de usuarios de IAM en la documentación de IAM.	Arquitectura de soluciones
Active la facturación detallada.	Para obtener más información sobre la facturación, consulte Supervisión del uso y los costos en la documentación de Administración de facturación y costos de AWS.	Arquitectura de soluciones

Tarea	Descripción	Habilidades requeridas
Compruebe los detalles de contacto de sus cuentas.	Asegúrese de que los datos de contacto de sus cuentas estén actualizados y correspondan a más de una persona de su organización. Para obtener más informaci ón, consulte Administración de una cuenta de AWS en la documentación de Administr ación de facturación y costos de AWS.	Arquitecto de soluciones, propietario del producto
Agregue información de contacto de seguridad.	Configure su información de contacto con su información de contacto de seguridad. Para obtener más informaci ón, consulte Administración de una cuenta de AWS en la documentación de Administr ación de facturación y costos de AWS.	Arquitecto de soluciones, seguridad de TI
Configurar roles de IAM para instancias EC2.	Configure los roles de IAM para las instancias de EC2. Para obtener más información, consulte Roles de IAM para Amazon EC2 en la documenta ción de Amazon EC2.	Arquitectura de soluciones

Tarea	Descripción	Habilidades requeridas
Configure el acceso a AWS Support.	Adjunte una política de IAM a los usuarios de IAM que necesiten acceso a AWS Support for Support Center y para crear casos de soporte. Para obtener más información al respecto, consulte Permisos de acceso para AWS Support en la documentación de AWS Support.	Arquitectura de soluciones
Habilitar CloudTrail.	Habilite AWS automátic amente CloudTrail en todas sus regiones de AWS. Para obtener más informaci ón al respecto, consulte Uso `create-trail` en la CloudTrail documentación de AWS.	Arquitectura de soluciones
Habilite la validación de los archivos de CloudTrail registro.	Habilite la validación de los archivos de CloudTrail registro. Para obtener más información al respecto, consulte Habilitar la validación de la integrida d de los archivos de registro CloudTrail en la CloudTrail documentación de AWS.	Arquitectura de soluciones

Tarea	Descripción	Habilidades requeridas
Restrinja el acceso a cualquier depósito de S3 que contenga CloudTrail registros.	Aplique una política de depósitos que restrinja el acceso a los depósitos de S3 que contienen archivos de CloudTrail registro. Para obtener más informaci ón al respecto, consulte la política de buckets de Amazon S3 CloudTrail en la CloudTrail documentación de AWS.	Arquitectura de soluciones
Intégrelo CloudTrail con CloudWatch Logs	Integre las rutas CloudTrai l generadas por Amazon CloudWatch Logs. Para obtener más informaci ón al respecto, consulte Envío de eventos a CloudWatch registros en la CloudTrail documentación de AWS	Arquitectura de soluciones
Habilite AWS Config en todas las regiones requeridas.	Habilite automáticamente AWS Config en todas las regiones requeridas. Puede configurar AWS Config mediante la CLI de AWS. Para obtener más informaci ón, consulte Configuración de AWS Config con la CLI de AWS en la documentación de AWS Config.	Arquitectura de soluciones

Tarea	Descripción	Habilidades requeridas
Habilite el registro de acceso al bucket de S3	Automatice el registro de acceso al bucket de S3 con CloudTrail. Para obtener más información al respecto, consulte Habilitar el registro de CloudTrail eventos para buckets y objetos de S3 en la documentación de Amazon S3.	Arquitectura de soluciones
Configure las políticas clave de AWS KMS para CloudTrail.	Automatice la configuración de las políticas clave de AWS Key Management Service (AWS KMS) para CloudTrail. Para obtener más información al respecto, consulte Configurar las políticas clave de AWS KMS CloudTrail en la CloudTrail documentación de AWS.	Arquitectura de soluciones

Tarea	Descripción	Habilidades requeridas
Cifre CloudTrail los registros en reposo.	Configure el cifrado de los CloudTrail registros en el servidor mediante claves administradas por el cliente que se encuentran en AWS KMS. Para obtener más informaci ón al respecto, consulte Cifrar archivos de CloudTrail registro con claves administradas por AWS KMS (SSE-KMS) en la documentación de AWS. CloudTrail	Arquitectura de soluciones
Rote automáticamente las claves de KMS.	Configure la rotación de las claves de AWS KMS. Para obtener más informaci ón al respecto, consulte Cómo habilitar y deshabilitar la rotación automática de claves en la documentación de AWS KMS.	Arquitectura de soluciones

Tarea	Descripción	Habilidades requeridas
Configure las alarmas. CloudWatch	Configure las CloudWatch alarmas de Amazon que se inician por eventos específicos. Por ejemplo, las solicitudes no autorizadas a las API o el uso de la cuenta raíz. Para obtener más información al respecto, consulte Cómo recibir notificaciones cuando se utilizan las claves de acceso raíz de su cuenta de AWS en el blog de seguridad de AWS.	Arquitectura de soluciones
Configuración de grupos de seguridad.	Configure los grupos de seguridad para garantizar que no se permita el tráfico entrante sin restricciones en los puertos 22 y 3389.	Arquitectura de soluciones
Active el registro de flujo de VPC.	Capture el tráfico IP rechazado hacia y desde las interfaces de red de su nube privada virtual (VPC) y configúrelo CloudWatch para capturarlo. Para obtener más información, consulte Crear un registro de flujo en la documentación de Amazon VPC.	Arquitectura de soluciones

Tarea	Descripción	Habilidades requeridas
Modifique el grupo de seguridad predeterminado para limitar todo el tráfico.	Modifique el grupo de seguridad predeterminado de cada VPC para que el tráfico se deniegue de forma predeterminada y el acceso se conceda de forma explícita a través de sus grupos de seguridad. Para obtener más información, consulte Grupos de seguridad de su VPC en la documentación de Amazon VPC.	Arquitectura de soluciones
Configure las tablas de enrutamiento entre las VPC.	Configure las tablas de enrutamiento para la interconexión de VPC con el mínimo acceso necesario. Para obtener más información, consulte Actualización de las tablas de ruteo para una conexión de emparejamiento de VPC en la documentación de Amazon VPC.	Arquitectura de soluciones

Actividades de configuración para la nueva infraestructura de AWS

Tarea	Descripción	Habilidades requeridas
Aprovisione la infraestructura AWS.	Cree las cuentas y los recursos de AWS. Duración: dos semanas	DevOps ingeniero, arquitecto de soluciones

Tarea	Descripción	Habilidades requeridas
Configure DevOps herramientas y procesos.	Configure DevOps herramientas y procedimientos, como las canalizaciones de integración y entrega continuas (CI/CD) y los marcos de pruebas automatizados.	DevOps ingeniero, arquitecto de soluciones
Automatice la migración de los componentes principales.	Utilice las plantillas o scripts existentes para automatizar la instalación y configuración de OpenText los productos TeamSite, incluidos LiveSite, OpenDeploy y MediaBin. Duración: una semana	DevOps ingeniero, arquitecto de soluciones, OpenText director
Automatice la migración de los componentes principales.	Analice y automatice la migración de aplicaciones adicionales que estén integradas con los componentes OpenText principales (por ejemplo, bases de datos adicionales, componentes de comunicación, monitoreo o caché). Duración: dos semanas	DevOps ingeniero, arquitecto de soluciones, OpenText director
Adapte los componentes principales.	Realice los cambios necesarios en las personalizaciones de los componentes OpenText principales (por ejemplo, las integraciones).	Arquitecto de soluciones, director OpenText , OpenText desarrollador, desarrollador de integraciones externo, desarrollador de front-end

Tarea	Descripción	Habilidades requeridas
Implemente y configure servicios adicionales.	Aprovisione, configure e implemente cualquier servicio nuevo de AWS, como las funciones de Lambda de AWS o Amazon API Gateway.	DevOps ingeniero, arquitecto de soluciones, desarrollador de integración externo, desarrollador front-end
Migre o refactorice otros componentes.	Migre los componentes adicionales, incluida cualquier refactorización necesaria. Esto incluye aplicaciones externas, como portales de informes personalizados o capas de integración de API existentes.	DevOps ingeniero, arquitecto de soluciones, desarrollador de integración externo, desarrollador front-end
Realice la migración en un entorno de desarrollo.	Actividades de migración automatizadas para el entorno de desarrollo, que incluyen el aprovisionamiento del sistema, la migración de datos, la migración de aplicaciones, la instalación y la configuración.	DevOps ingeniero
Realice la migración en un entorno de producción.	Actividades de migración automatizadas para el entorno de desarrollo, que incluyen el aprovisionamiento del sistema, la migración de datos, la migración de aplicaciones, la instalación y la configuración.	DevOps ingeniero

Actividades de creación de redes

Tarea	Descripción	Habilidades requeridas
Defina bloques de CIDR para cada VPC.	Defina el bloque de enrutamie nto entre dominios sin clases (CIDR) (el rango de IP y la máscara) para cada VPC que no sea la predeterminada. Duración: menos de una semana	DevOps ingeniero, arquitecto de soluciones
Defina las subredes y las zonas de disponibilidad.	Defina las subredes y las zonas de disponibilidad que se utilizan en cada VPC no predeterminada. Duración: menos de una semana	DevOps ingeniero, arquitecto de soluciones
Defina los grupos de seguridad.	Defina los grupos de seguridad y las reglas de los grupos de seguridad para controlar la seguridad de los recursos de AWS. Duración: menos de una semana	DevOps ingeniero, arquitecto de soluciones
Defina las ACL de red.	Defina las listas de control de acceso (ACL) de red para controlar la seguridad en los límites de la subred. Duración: menos de una semana	DevOps ingeniero, arquitecto de soluciones

Migración de bases de datos

Tarea	Descripción	Habilidades requeridas
Prepare la base de datos de origen.	Utilice AWS DMS para preparar cada base de datos de origen para la replicación continua en la nube de AWS.	DevOps ingeniero, arquitecto de soluciones
Cree las bases de datos para los componentes OpenText principales.	Cree las bases de datos requeridas por el Opentext y TeamSite LiveSite MediaBin los componentes. Asegúrese de que los usuarios y los derechos de acceso estén configurados correctamente de acuerdo con la documenta ción de OpenText instalación.	OpenText Arquitecto, director y OpenText desarrollador de soluciones
Copie datos de los servidores de bases de datos de origen.	Automatice el proceso de copia de datos de los componentes OpenText principales del servidor de base de datos de origen al servidor de base de datos de destino.	OpenText Arquitecto, director y OpenText desarrollador de soluciones
Sincronice los datos de los servidores de bases de datos.	Automatice el proceso de sincronización regular de datos desde las bases de datos de origen a las bases de datos de destino.	OpenText desarrollador

Actividades de migración de contenido

Tarea	Descripción	Habilidades requeridas
Copia los almacenes de OpenText TeamSite contenido .	Automatice el proceso de copiar los almacenes de contenido del OpenText TeamSite servidor de origen al OpenText TeamSite servidor de destino.	Arquitecto, OpenText líder y OpenText desarrollador de soluciones
Mapeo de usuarios y grupos.	Mapeo interno de los ID de los OpenText TeamSite usuarios internos con los ID del sistema de destino.	OpenText plomo
Sincronice los almacenes OpenText TeamSite de contenido.	Automatice el proceso de sincronización regular de los almacenes de contenido de origen y destino. Esto se implementa como parte del proceso de migración y control de calidad.	OpenText desarrollador
Copie datos de servidores web.	Automatice el proceso de copiar datos de los servidores web de origen a los servidores web de destino.	Arquitecto de soluciones, OpenText líder, OpenText desarrollador
Sincronice los datos del servidor web.	Automatice el proceso de sincronización regular de los almacenes de contenido de los servidores web de origen y destino.	OpenText desarrollador
Copie los datos del sistema de archivos del servidor web.	Automatice el proceso de copiar contenido y otros activos web desde el sistema	Arquitecto de soluciones, OpenText líder, OpenText desarrollador

Tarea	Descripción	Habilidades requeridas
	de archivos del servidores web de origen a los servidores web de destino.	
Sincronice los sistemas de archivos del servidor web.	Automatice el proceso de sincronización regular del contenido y otros activos web desde el sistema de archivos del servidor web de origen con los servidores web de destino.	OpenText desarrollador
Genere feeds e índices.	Automatice el proceso de ejecutar cualquier proceso que genere feeds u otros índices (por ejemplo, búsquedas en la web) que utilice OpenText TeamSite el contenido del servidor web como fuente de datos.	OpenText Arquitecto, director y desarrollador de soluciones OpenText
Sincronice la generación de feeds e índices.	Automatice el proceso de regeneración periódica de fuentes e índices después de la sincronización de datos.	OpenText desarrollador

Actividades de prueba y control de calidad

Tarea	Descripción	Habilidades requeridas
Realice el control de calidad de la migración.	Pruebe el entorno, las aplicaciones y los servicios de AWS de destino para asegurarse de que los procesos de migración	DevOps ingeniero, OpenText jefe, probador de control de calidad

Tarea	Descripción	Habilidades requeridas
	automatizada se hayan creado y configurado correctamente.	
Realice pruebas de rendimiento.	Pruebe el rendimiento en términos de capacidad de respuesta y estabilidad bajo una carga de trabajo determinada. Investigue, mida, valide o verifique otros atributos de calidad del sistema de destino, como la escalabilidad y la fiabilidad. Para que esta prueba sea útil, debe tener un entorno de pruebas del mismo tamaño que su entorno de producción. Duración: entre una y dos semanas	DevOps ingeniero, líder OpenText

Tarea	Descripción	Habilidades requeridas
Pruebas de seguridad.	Análisis de vulnerabilidades y pruebas de penetración para revelar posibles fallos en los mecanismos de seguridad de una aplicación que protegen los datos y mantienen la funcionalidad necesaria. Para que esta prueba resulte útil, debe disponer de un entorno de pruebas equivalente al entorno de producción en términos de redes y seguridad. Duración: entre una y dos semanas	DevOps ingeniero, OpenText líder

Actividades de integración operativa

Tarea	Descripción	Habilidades requeridas
Compruebe la preparación operativa.	Comprenda cómo realiza actualmente las operaciones de TI y cómo operará en la nube de AWS. Una forma de lograr este resultado empresarial es definir un modelo operativo en la nube. Duración: una semana	DevOps ingeniero, OpenText líder, gerente de prestación de servicios
Invierta en la automatización de las operaciones.	Invierta en automatización para ofrecer un modelo operativo de AWS.	DevOps ingeniero, OpenText líder, gerente de prestación de servicios

Tarea	Descripción	Habilidades requeridas
Integre las operaciones.	Continúe utilizando las herramientas de TI actuales y amplíelas mediante la integración en la nube de AWS.	DevOps ingeniero, OpenText líder, gerente de prestación de servicios

Actividades de transición

Tarea	Descripción	Habilidades requeridas
Cambie de DNS.	Cambie manualmente el sistema de nombres de dominio (DNS) de los hosts existentes a los basados en la nube de AWS. Duración: una hora	DevOps ingeniero, OpenText líder
Pruebe la recuperación de desastres.	Pruebe la recuperación de desastres, las copias de seguridad, restaure y ejecute sus pruebas automatizadas. Duración: un día	DevOps ingeniero, director, OpenText probador de control de calidad
Valide la supervisión y el análisis.	Valide que la supervisión y los análisis funcionen. Duración: dos horas	DevOps ingeniero, líder OpenText
Apague el entorno anterior y solicite el cierre del servidor.	Duración: tres días	DevOps ingeniero, OpenText líder

Recursos relacionados

- Políticas administradas por el cliente
- Creación de un usuario de IAM en su cuenta de AWS
- Grupos de usuarios de IAM
- Asociación de una política a un grupo de usuarios de IAM
- Monitorización del uso y de los costos
- Administración de una cuenta de AWS
- Roles de IAM para Amazon EC2
- Permisos de acceso para AWS Support
- Uso de create-trail
- Habilitar la validación de la integridad del archivo de registro para CloudTrail
- Política de bucket de Amazon S3 para CloudTrail
- Envío de eventos a CloudWatch Logs
- Configuración de AWS Config con la CLI de AWS
- Habilitar CloudTrail el registro de eventos para cubos y objetos de S3
- Configurar las políticas clave de AWS KMS para CloudTrail
- Cifrado de archivos de CloudTrail registro con claves administradas por AWS KMS (SSE-KMS)
- Cómo habilitar y desactivar la rotación automática de claves
- Cómo recibir notificaciones cuando se utilizan las claves de acceso raíz de su cuenta de AWS
- Crear un registro de flujo
- Grupos de seguridad de su VPC
- Actualización de las tablas de ruteo para una conexión de emparejamiento de VPC

Migre valores CLOB de Oracle a filas individuales en PostgreSQL en AWS

Creado por Sai Krishna Namburu (AWS) y Sindhusha Paturu (AWS)

Entorno: PoC o piloto	Origen: base de datos de Oracle	Destino: Compatible con Aurora PostgreSQL o Amazon RDS para PostgreSQL
Tipo R: redefinir la plataforma	Carga de trabajo: Oracle; código abierto	Tecnologías: migración; almacenamiento y copia de seguridad; bases de datos
Servicios de AWS: Amazon Aurora; AWS DMS; Amazon S3; Amazon RDS		

Resumen

Este patrón describe cómo dividir valores de objetos grandes (CLOB) de Oracle en filas individuales en Amazon Aurora compatible con PostgreSQL y Amazon Relational Database Service (Amazon RDS) para PostgreSQL. PostgreSQL no admite el tipo de datos CLOB.

Las tablas con particiones de intervalos se identifican en la base de datos Oracle de origen, y el nombre de la tabla, el tipo de partición, el intervalo de partición y otros metadatos se registran y cargan en la base de datos de destino. Puede cargar datos CLOB de tamaño inferior a 1 GB en tablas de destino como texto mediante AWS Database Migration Service (AWS DMS), o bien puede exportar los datos en formato CSV, cargarlos en un bucket de Amazon Simple Storage Service (Amazon S3) y migrarlos a su base de datos PostgreSQL de destino.

Tras la migración, puede usar el código de PostgreSQL personalizado proporcionado con este patrón para dividir los datos CLOB en filas individuales en función del nuevo identificador de caracteres de línea (`CHR(10)`) y rellenar la tabla de destino.

Requisitos previos y limitaciones

Requisitos previos

- Una tabla de base de datos de Oracle con particiones de intervalos y registros con tipo de datos CLOB.
- Una base de datos de Aurora compatible con PostgreSQL o Amazon RDS para PostgreSQL con una estructura de tabla similar a la tabla de origen (las mismas columnas y tipos de datos).

Limitaciones

- El valor de CLOB no puede superar 1 GB.
- Cada fila de la tabla de destino debe tener un nuevo identificador de caracteres de línea.

Versiones de producto

- Oracle 12c
- Aurora PostgreSQL 11.6

Arquitectura

El siguiente diagrama muestra una tabla de origen de Oracle con datos CLOB, y la tabla PostgreSQL equivalente en Aurora compatible con PostgreSQL versión 11.6.

Herramientas

Servicios de AWS

- La edición Amazon Aurora PostgreSQL-Compatible es un motor de base de datos relacional, compatible con ACID y completamente administrado que le permite configurar, administrar y escalar implementaciones de PostgreSQL.
- Amazon Relational Database Service (Amazon RDS) para PostgreSQL le ayuda a configurar, utilizar y escalar una base de datos relacional de PostgreSQL en la nube de AWS.
- AWS Database Migration Service (AWS DMS) le permite migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Otras herramientas

Puede usar las siguientes herramientas de cliente para conectarse, acceder y gestionar sus bases de datos de Aurora compatible con PostgreSQL y Amazon RDS para PostgreSQL. (Estas herramientas no se usan en este patrón).

- pgAdmin es una herramienta de gestión de código abierto para PostgreSQL. Proporciona una interfaz gráfica que permite crear, mantener y utilizar objetos de bases de datos.
- DBeaver es una herramienta de base de datos de código abierto para desarrolladores y administradores de bases de datos. Esta herramienta le permite manipular, supervisar, analizar, administrar y migrar sus datos.

Prácticas recomendadas

Para conocer las prácticas recomendadas para migrar su base de datos de Oracle a PostgreSQL, consulte la publicación del blog de AWS Prácticas recomendadas para migrar una base de datos de Oracle a Amazon RDS PostgreSQL o Amazon Aurora PostgreSQL: consideraciones sobre el proceso de migración y la infraestructura.

Para obtener más información sobre las prácticas recomendadas para configurar la tarea de AWS DMS de migración de grandes objetos binarios, consulte Migración de grandes objetos binarios (LOB) en la documentación de AWS DMS.

Epics

Identifique los datos de CLOB

Tarea	Descripción	Habilidades requeridas
Analice los datos de CLOB.	En la base de datos Oracle de origen, analice los datos de CLOB para comprobar si contienen encabezados de columna y así poder determinar el método de carga de los datos en la tabla de destino.	Desarrollador

Tarea	Descripción	Habilidades requeridas
	Para analizar los datos de entrada, ejecute la siguiente consulta. `SELECT * FROM clobdata_or;`	
Cargue los datos de CLOB en la base de datos de destino.	Migre la tabla que contiene datos de CLOB a una tabla provisional (transitoria) en la base de datos de destino de Aurora o Amazon RDS. Puede usar AWS DMS o cargar los datos en formato de archivo CSV a un bucket de Amazon S3. Para obtener más informaci ón sobre el uso de AWS DMS para esta tarea, consulte Uso de una base de datos Oracle como fuente y Uso de una base de datos PostgreSQL como destino en la documenta ción de AWS DMS. Para obtener más información sobre el uso de Amazon S3 para esta tarea, consulte Uso de Amazon S3 como destino en la documentación de AWS DMS.	Ingeniero de migraciones, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
Valide la tabla PostgreSQL de destino.	Valide los datos de destino, incluidos los encabezados, comparándolos con los datos de origen. Para ello, ejecute las siguientes consultas en la base de datos de destino. `SELECT * FROM clobdata_pg;` `SELECT * FROM clobdatatarget;` Compare los resultados con los resultados de las consultas a la base de datos de origen (desde el primer paso).	Desarrollador
Divida los datos de CLOB en filas independientes.	Ejecute el código PostgreSQL personalizado que se proporciona en la sección Información adicional para dividir los datos CLOB e insertarlos en filas independientes en la tabla PostgreSQL de destino.	Desarrollador

Valide los datos.

Tarea	Descripción	Habilidades requeridas
Valide los datos en la tabla de destino.	Valide los datos insertados en la tabla de destino ejecutando las siguientes consultas.	Desarrollador

Tarea	Descripción	Habilidades requeridas
	`SELECT * FROM clobdata_pg;` `SELECT * FROM clobdatatarget;`	

Recursos relacionados

- Tipo de datos CLOB (documentación de Oracle)
- Tipos de datos (documentación de PostgreSQL)

Información adicional

Función de PostgreSQL para dividir datos CLOB

```
do
$$
declare
totalstr varchar;
str1 varchar;
str2 varchar;
pos1 integer := 1;
pos2 integer ;
len integer;


begin
        select rawdata||chr(10) into totalstr from clobdata_pg;
        len :=  length(totalstr) ;
        raise notice 'Total length : %',len;
        raise notice 'totalstr : %',totalstr;
        raise notice 'Before while loop';


        while pos1 < len  loop


                select position (chr(10) in totalstr) into pos2;
```

```
                 raise notice '1st position of new line : %',pos2;


                str1 := substring (totalstr,pos1,pos2-1);
                raise notice 'str1 : %',str1;


                   insert into clobdatatarget(data) values (str1);
                   totalstr := substring(totalstr,pos2+1,len);
                   raise notice 'new totalstr :%',totalstr;
                len :=  length(totalstr) ;


        end loop;
end
$$
LANGUAGE 'plpgsql' ;
```

Ejemplos de entrada y salida

Puede usar los siguientes ejemplos para probar el código PostgreSQL antes de migrar los datos.

Cree una base de datos Oracle con tres líneas de entrada.

```
CREATE TABLE clobdata_or (
id INTEGER GENERATED ALWAYS AS IDENTITY,
rawdata clob  );


insert into clobdata_or(rawdata) values (to_clob('test line 1') || chr(10) ||
 to_clob('test line 2') || chr(10) || to_clob('test line 3') || chr(10));
COMMIT;


SELECT * FROM clobdata_or;
```

Se mostrarán los siguientes valores.

id	rawdata
1	test line 1 test line 2 test line 3

Cargue los datos de origen en una tabla transitoria de PostgreSQL (`clobdata_pg`) para su procesamiento.

```
SELECT * FROM clobdata_pg;

CREATE TEMP TABLE clobdatatarget (id1 SERIAL,data VARCHAR );

<Run the code in the additional information section.>

SELECT * FROM clobdatatarget;
```

Se mostrarán los siguientes valores.

id1	datos
1	Línea de prueba 1
2	Línea de prueba 2
3	Línea de prueba 3

Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle mediante Oracle Data Pump

Creado por Rizwan Wangde (AWS)

Entorno: producción	Origen: Base de datos de Oracle en las instalaciones	Destino: Amazon RDS para Oracle
Tipo R: redefinir la plataforma	Carga de trabajo: Oracle	Tecnologías: Migración; bases de datos
Servicios de AWS: AWS DMS; AWS Direct Connect; Amazon RDS		

Resumen

Numerosos patrones cubren la migración de bases de datos de Oracle en las instalaciones a Amazon RDS para Oracle mediante Oracle Data Pump, una utilidad nativa de Oracle que es la forma preferida de migrar grandes cargas de trabajo de Oracle. Estos patrones suelen implicar la exportación de tablas o esquemas de aplicaciones a archivos de volcado, la transferencia de los archivos de volcado a un directorio de base de datos en Amazon RDS para Oracle y, a continuación, la importación de los esquemas de aplicación y los datos de los archivos de volcado.

Con este enfoque, la migración puede tardar más en función del tamaño de los datos y del tiempo que se tarde en transferir los archivos de volcado a la instancia de Amazon RDS. Además, los archivos de volcado residen en el volumen Amazon Elastic Block Store (Amazon EBS) de la instancia de Amazon RDS, que debe ser lo suficientemente grande para la base de datos y los archivos de volcado. Si los archivos volcados se eliminan tras la importación, no se puede recuperar el espacio vacío, por lo que tendrá que pagar por el espacio no utilizado.

Este patrón mitiga estos problemas al realizar una importación directa en la instancia de Amazon RDS mediante la API de Oracle Data Pump (`DBMS_DATAPUMP`) a través de un enlace de base de datos. El patrón inicia una canalización de exportación e importación simultánea entre las bases de datos de origen y destino. Este patrón no requiere ajustar el tamaño de un volumen de EBS para los archivos de volcado porque no se crea ni almacena ningún archivo de volcado en el volumen. Este enfoque ahorra el costo mensual del espacio en disco no utilizado.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de Amazon Web Services (AWS) activa.
- Una nube privada virtual (VPC) configurada con subredes privadas en al menos dos zonas de disponibilidad, para proporcionar la infraestructura de red para la instancia de Amazon RDS.
- Una base de datos de Oracle en un centro de datos en las instalaciones.
- Una instancia de Oracle de Amazon RDS en una única zona de disponibilidad. El uso de una única zona de disponibilidad mejora el rendimiento de escritura durante la migración. Se puede habilitar una implementación Multi-AZ entre 24 y 48 horas antes de la transición.
- AWS Direct Connect (recomendado para bases de datos de gran tamaño).
- La conectividad de red y las reglas de firewall locales están configuradas para permitir una conexión entrante desde la instancia de Amazon RDS a la base de datos de Oracle en las instalaciones.

Limitaciones

- El límite de tamaño de la base de datos en Amazon RDS para Oracle es de 64 TiB (en diciembre de 2022).

Versiones de producto

- Base de datos de origen: base de datos de Oracle 10g, versión 1 y posteriores.
- Base de datos de destino: para obtener la lista más reciente de versiones y ediciones compatibles en Amazon RDS, consulte Amazon RDS para Oracle en la documentación de AWS.

Arquitectura

Pila de tecnología de origen

- Base de datos de Oracle autoadministrada en las instalaciones o en la nube

Pila de tecnología de destino

- Amazon RDS para Oracle

Arquitectura de destino

El siguiente diagrama muestra la arquitectura para migrar de una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle en un entorno Single-AZ. Las direcciones de las flechas representan el flujo de datos en la arquitectura. El diagrama no muestra qué componente está iniciando la conexión.

1. La instancia de Amazon RDS para Oracle se conecta a la base de datos de Oracle de origen en las instalaciones para realizar una migración a plena carga a través del enlace de la base de datos.
2. AWS DMS se conecta a la base de datos de Oracle de origen en las instalaciones para realizar una replicación continua mediante la captura de datos de cambios (CDC).
3. Los cambios de los CDC se aplican a la base de datos de Amazon RDS para Oracle.

Herramientas

Servicios de AWS

- AWS Database Migration Service (AWS DMS) le permite migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones. Este patrón usa CDC y la configuración Replicar solo cambios de datos.
- AWS Direct Connect vincula su red interna con una ubicación de Direct Connect a través de un cable estándar Ethernet de fibra óptica. Con esta conexión, puede crear interfaces virtuales directamente en servicios públicos de AWS omitiendo a los proveedores de servicios de Internet en su ruta de acceso a la red.
- Amazon Relational Database Service (Amazon RDS) para Oracle le ayuda a configurar, utilizar y escalar una base de datos relacional de Oracle en la nube de AWS.

Otras herramientas

- Oracle Data Pump le ayuda a trasladar datos y metadatos de una base de datos a otra a altas velocidades.
- Se utilizan herramientas de cliente como Oracle Instant Client o SQL Developer para conectar y ejecutar consultas SQL en la base de datos.

Prácticas recomendadas

Si bien AWS Direct Connect utiliza conexiones de red privadas y dedicadas entre la red local y AWS, considere las siguientes opciones para aumentar la seguridad y el cifrado de datos de los datos en tránsito:

- Una red privada virtual (VPN) con Amazon Site-to-Site VPN o una conexión de IPSec VPN desde la red en las instalaciones a la red de AWS
- El cifrado de red nativo de la base de datos de Oracle configurado en la base de datos de Oracle en las instalaciones
- Cifrado con TLS

Epics

Prepare la base de datos en las instalaciones de origen

Tarea	Descripción	Habilidades requeridas
Configurar la conectividad de red desde la base de datos de destino a la base de datos de origen.	Configure el firewall y la red en las instalaciones para permitir la conexión entrante desde la instancia de Amazon RDS de destino a la base de datos de Oracle de origen en las instalaciones.	Administrador de redes, ingeniero de seguridad
Crear un usuario de base de datos con los privilegios adecuados.	Cree un usuario de base de datos en la base de datos de Oracle de origen en las instalaciones con privilegios para migrar datos entre el origen y el destino mediante Oracle Data Pump. `GRANT CONNECT to <migration_user>;`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`GRANT DATAPUMP_EXP_FULL_DATABASE to <migration_user>;` `GRANT SELECT ANY TABLE to <migration_user>;`	

Tarea	Descripción	Habilidades requeridas
Prepare la base de datos en las instalaciones de origen para la migración a AWS DMS CDC.	(Opcional) Prepare la base de datos de Oracle de origen en las instalaciones para la migración a AWS DMS CDC tras finalizar la carga completa de Oracle Data Pump: 1. Configure los privilegios adicionales necesarios para gestionar FLASHBACK durante la migración a Oracle Data Pump. `GRANT FLASHBACK ANY TABLE to <migration_user>;` `GRANT FLASHBACK ARCHIVE ADMINISTER to <migration_user>;` 2. Para configurar los privilegios de cuenta de usuario necesarios en una base de datos de origen autogestionada Oracle para AWS DMS, consulte la documentación de AWS DMS. 3. Para preparar una base de datos origen autogestionada de Oracle para los CDC mediante AWS DMS, consulte la documentación de AWS DMS.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Instalar y configurar SQL Developer.	Instale y configure SQL Developer para conectar y ejecutar consultas SQL en las bases de datos de origen y destino.	Administrador de base de datos, ingeniero de migracion es
Generar un script para crear los espacios de tabla.	Utilice el siguiente ejemplo de consulta SQL para generar el script en la base de datos de origen. `SELECT 'CREATE TABLESPACE ' tablespace_name ' DATAFILE SIZE 1G AUTOEXTEND ON MAXSIZE UNLIMITED;' from dba_tablespaces where tablespace_name not in ('SYSTEM', 'SYSAUX','TEMP','UNDOTBS1') order by 1;` El script se aplicará en la base de datos de destino.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Generar un script para crear usuarios, perfiles, roles y privilegios.	Para generar un script para crear los usuarios, perfiles, funciones y privilegios de la base de datos, utilice los scripts del documento de Oracle Support Cómo extraer DDL para usuario, incluidos los privilegios y roles mediante dbms_metadata.get_ddl (ID de documento 2739952.1) (se requiere una cuenta de Oracle). El script se aplicará en la base de datos de destino.	Administrador de base de datos

Preparación de la instancia de Amazon RDS para Oracle

Tarea	Descripción	Habilidades requeridas
Crear un enlace de base de datos a la base de datos origen y verificar la conectividad.	Para crear un enlace de base de datos a la base de datos en las instalaciones de origen, puede usar el comando de ejemplo siguiente. `CREATE DATABASE LINK link2src CONNECT TO <migration_user_account> IDENTIFIED BY <password> USING '(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=<dns`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	or ip address of remote db>) (PORT=<listener port>))(CONNECT_DATA=(SID=<remote SID>)))'; Para comprobar la conectividad, ejecute el comando de SQL siguiente. select * from dual@link2src; La conectividad es correcta si la respuesta es X.	
Ejecute los scripts para preparar la instancia de destino.	Ejecute los scripts generados anteriormente para preparar la instancia de Amazon RDS para Oracle: 1. Espacios de tabla 2. Perfiles 3. Roles Esto ayuda a garantizar que la migración de Oracle Data Pump pueda crear los esquemas y sus objetos.	Administrador de base de datos, ingeniero de migraciones

Realizar una migración a plena carga mediante Oracle Data Pump Import a través de un enlace de base de datos

Tarea	Descripción	Habilidades requeridas
Migre los esquemas necesarios.	Para migrar los esquemas necesarios de la base de datos en las instalaciones de origen a la instancia de Amazon RDS de destino, utilice el código de la sección de información adicional: • Para migrar un único esquema, ejecute el código 1 desde la sección de información adicional. • Para migrar múltiples esquemas, ejecute el código 2 desde la sección de información adicional. Para ajustar el rendimiento de la migración, puede ajustar el número de procesos paralelos ejecutando el siguiente comando. `DBMS_DATAPUMP.SET_PARALLEL (handle => v_hdnl, degree => 4);`	Administrador de base de datos
Recopile estadísticas de esquema para mejorar el rendimiento.	El comando Recopilar estadísticas del esquema devuelve las estadísticas del optimizador de consultas de Oracle recopiladas para	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	los objetos de la base de datos. Con esta informaci ón, el optimizador puede seleccionar el mejor plan de ejecución para cualquier consulta relacionada con estos objetos. `EXECUTE DBMS_STAT S.GATHER_SCHEMA_ST ATS(ownname => '<schema_name>');`	

Realizar una migración a plena carga y una replicación de CDC mediante Oracle Data Pump y AWS DMS

Tarea	Descripción	Habilidades requeridas
Capturar el SCN en la base de datos en las instalaciones de origen de Oracle.	Capture el número de cambio del sistema (SCN) en la base de datos de Oracle en las instalaciones de origen. Debe utilizar el SCN para la importación a plena carga y como punto de partida para la replicación de los CDC. Para generar el SCN actual de la base de datos de origen, introduzca la siguiente instrucción SQL. `SELECT current_scn FROM V$DATABASE;`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Realizar la migración a plena carga de los esquemas.	Para migrar los esquemas necesarios (`FULL LOAD`) de la base de datos en las instalaciones de origen a la instancia de Amazon RDS de destino, haga lo siguiente: • Para migrar un único esquema, ejecute el código 3 desde la sección de información adicional. • Para migrar múltiples esquemas, ejecute el código 4 desde la sección de información adicional. En el código, sustituya `<CURRENT_SCN_VALUE_IN_SOURCE_DATABASE>` por el SCN que capturó de la base de datos de origen. `DBMS_DATAPUMP.SET_PARAMETER (handle => v_hdnl, name => 'FLASHBACK_SCN', value => <CURRENT_SCN_VALUE_IN_SOURCE_DATABASE>);` Para ajustar el rendimiento de la migración, puede configurar el número de procesos paralelos ejecutando el siguiente comando.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`DBMS_DATAPUMP.SET_PARALLEL (handle => v_hdnl, degree => 4);`	
Deshabilitar los desencadenadores en los esquemas migrados.	Antes de comenzar la tarea AWS DMS solo de CDC, desactive los `TRIGGERS` en los esquemas migrados.	Administrador de base de datos
Recopile estadísticas de esquema para mejorar el rendimiento.	El comando Recopilar estadísticas del esquema devuelve las estadísticas del optimizador de consultas de Oracle recopiladas para los objetos de la base de datos. Con esta información, el optimizador puede seleccionar el mejor plan de ejecución para cualquier consulta relacionada con estos objetos. `EXECUTE DBMS_STATS.GATHER_SCHEMA_STATS(ownname => '<schema_name>');`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Utilizar AWS DMS para realizar una replicación continua desde el origen hasta el destino.	Utilice AWS DMS para realizar una replicación continua desde la base de datos de Oracle de origen a la instancia de Amazon RDS para Oracle de destino. Para obtener más información, consulte Cómo crear tareas de replicación continua mediante AWS DMS y la entrada del blog Cómo trabajar con el soporte nativo para CDC en AWS DMS.	Administrador de base de datos, ingeniero de migracion es

Cómo hacer la transición a Amazon RDS para Oracle

Tarea	Descripción	Habilidades requeridas
Habilitar la opción Multi-AZ en la instancia 48 horas antes de la transición.	Si se trata de una instancia de producción, recomendamos habilitar la implementación Multi-AZ en la instancia de Amazon RDS para ofrecer las ventajas de la alta disponibi lidad (HA) y la recuperación de desastres (DR).	Administrador de base de datos, ingeniero de migracion es
Detenga la tarea AWS DMS solo de CDC (si CDC estaba activado).	1. Asegúrese de que la latencia de origen y la latencia de destino en las CloudWatch métricas de Amazon de la tarea de AWS DMS muestren 0 segundos.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	2. Detenga la tarea AWS DMS solo de CDC.	
Habilitar los desencade nadores.	Habilite los DESENCADE NADORES que desactivó antes de crear la tarea de los CDC.	Administrador de base de datos

Recursos relacionados

AWS

- Preparación de una base de datos de origen autogestionada de Oracle para los CDC mediante AWS DMS
- Creación de tareas para la replicación continua con AWS DMS
- Implementaciones Multi-AZ para alta disponibilidad
- Cómo trabajar con el soporte nativo de los CDC en AWS DMS (entrada del blog)

Documentación de Oracle

- DBMS_DATAPUMP

Información adicional

Código 1: migración a plena carga solo, esquema de aplicación única

```
DECLARE
    v_hdnl NUMBER;
BEGIN
    v_hdnl := DBMS_DATAPUMP.OPEN(operation => 'IMPORT', job_mode  => 'SCHEMA',
 remote_link => '<DB LINK Name to Source Database>', job_name  => null);
    DBMS_DATAPUMP.ADD_FILE( handle => v_hdnl, filename  => 'import_01.log',  directory
 => 'DATA_PUMP_DIR', filetype  => dbms_datapump.ku$_file_type_log_file);
    DBMS_DATAPUMP.METADATA_FILTER(v_hdnl,'SCHEMA_EXPR','IN (''<schema_name>'')');  --
 To migrate one selected schema
```

```
    DBMS_DATAPUMP.METADATA_FILTER (hdnl, 'EXCLUDE_PATH_EXPR','IN (''STATISTICS'')'); --
 To prevent gathering Statistics during the import
    DBMS_DATAPUMP.SET_PARALLEL (handle => v_hdnl, degree => 4);  -- Number of parallel
 processes performing export and import
    DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
/
```

Código 2: migración a plena solo, esquemas de aplicación múltiples

```
DECLARE
    v_hdnl NUMBER;
BEGIN
    v_hdnl := DBMS_DATAPUMP.OPEN(operation => 'IMPORT', job_mode  => 'SCHEMA',
 remote_link => '<DB LINK Name to Source Database>', job_name  => null);
    DBMS_DATAPUMP.ADD_FILE( handle => v_hdnl, filename  => 'import_01.log',  directory
 => 'DATA_PUMP_DIR', filetype  => dbms_datapump.ku$_file_type_log_file);
    DBMS_DATAPUMP.METADATA_FILTER (v_hdnl, 'SCHEMA_LIST',
 '''<SCHEMA_1>'',''<SCHEMA_2>'', ''<SCHEMA_3>'''); -- To migrate multiple schemas
    DBMS_DATAPUMP.METADATA_FILTER (v_hdnl, 'EXCLUDE_PATH_EXPR','IN (''STATISTICS'')');
 -- To prevent gathering Statistics during the import
    DBMS_DATAPUMP.SET_PARALLEL (handle => v_hdnl, degree => 4);  -- Number of parallel
 processes performing export and import
    DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
/
```

Código 3: migración a plena carga antes de una tarea solo de CDC, esquema de aplicación única

```
DECLARE
    v_hdnl NUMBER;
BEGIN
    v_hdnl := DBMS_DATAPUMP.OPEN(operation => 'IMPORT', job_mode  => 'SCHEMA',
 remote_link => '<DB LINK Name to Source Database>', job_name  => null);
    DBMS_DATAPUMP.ADD_FILE( handle => v_hdnl, filename  => 'import_01.log',  directory
 => 'DATA_PUMP_DIR', filetype  => dbms_datapump.ku$_file_type_log_file);
    DBMS_DATAPUMP.METADATA_FILTER(v_hdnl,'SCHEMA_EXPR','IN (''<schema_name>'')');  --
 To migrate one selected schema
    DBMS_DATAPUMP.METADATA_FILTER (v_hdnl, 'EXCLUDE_PATH_EXPR','IN (''STATISTICS'')');
 -- To prevent gathering Statistics during the import
    DBMS_DATAPUMP.SET_PARAMETER (handle => v_hdnl, name => 'FLASHBACK_SCN', value =>
 <CURRENT_SCN_VALUE_IN_SOURCE_DATABASE>); -- SCN required for AWS DMS CDC only task.
```

```
    DBMS_DATAPUMP.SET_PARALLEL (handle => v_hdnl, degree => 4);  -- Number of parallel
 processes performing export and import
    DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
/
```

Código 4: migración a plena carga antes de una tarea solo de CDC, esquemas de aplicación múltiples

```
DECLARE
    v_hdnl NUMBER;
BEGIN
    v_hdnl := DBMS_DATAPUMP.OPEN (operation => 'IMPORT', job_mode  => 'SCHEMA',
 remote_link => '<DB LINK Name to Source Database>', job_name  => null);
    DBMS_DATAPUMP.ADD_FILE (handle => v_hdnl, filename  => 'import_01.log',  directory
 => 'DATA_PUMP_DIR', filetype  => dbms_datapump.ku$_file_type_log_file);
    DBMS_DATAPUMP.METADATA_FILTER (v_hdnl, 'SCHEMA_LIST',
 '''<SCHEMA_1>'',''<SCHEMA_2>'', ''<SCHEMA_3>'''); -- To migrate multiple schemas
    DBMS_DATAPUMP.METADATA_FILTER (v_hdnl, 'EXCLUDE_PATH_EXPR','IN (''STATISTICS'')');
 -- To prevent gathering Statistics during the import
    DBMS_DATAPUMP.SET_PARAMETER (handle => v_hdnl, name => 'FLASHBACK_SCN', value =>
 <CURRENT_SCN_VALUE_IN_SOURCE_DATABASE>); -- SCN required for AWS DMS CDC only task.
    DBMS_DATAPUMP.SET_PARALLEL (handle => v_hdnl, degree => 4);  -- Number of parallel
 processes performing export and import
    DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
/
```

Escenario en el que un enfoque de migración mixto puede funcionar mejor

En raras ocasiones, en las que la base de datos de origen contiene tablas con millones de filas y columnas LOBSEGMENT de gran tamaño, este patrón ralentizará la migración. Oracle migra los LOBSEGMENTs a través del enlace de red de uno en uno. Extrae una sola fila (junto con los datos de la columna LOB) de la tabla de origen e inserta la fila en la tabla de destino, repitiendo el proceso hasta que se migren todas las filas. Oracle Data Pump a través del enlace de la base de datos no admite los mecanismos de carga masiva o de carga por ruta directa para LobSegments.

En las siguientes situaciones, se recomienda:

- Omitir las tablas identificadas durante la migración de Oracle Data Pump añadiendo el siguiente filtro de metadatos.

```
dbms_datapump.metadata_filter(handle =>h1, name=>'NAME_EXPR', value => 'NOT IN
 (''TABLE_1'',''TABLE_2'')');
```

- Utilizar una tarea de AWS DMS (migración a plena carga, con replicación de CDC si es necesaria) para migrar las tablas identificadas. AWS DMS extraerá varias filas de la base de datos de Oracle de origen y las insertará en un lote en la instancia de Amazon RDS de destino, lo que mejora el rendimiento.

Migre Oracle E-Business Suite a Amazon RDS Custom

Creado por Simon Cunningham (AWS), Jaydeep Nandy (AWS), Nitin Saxena (AWS) y Vishnu Vinnakota (AWS)

Entorno: producción	Origen: Amazon EC2 o en las instalaciones	Destino: Amazon RDS Custom
Tipo R: redefinir la plataforma	Carga de trabajo: Oracle	Tecnologías: migración; bases de datos; infraestructura
Servicios de AWS: AWS EFS; Amazon RDS; AWS Secrets Manager		

Resumen

Oracle E-Business Suite es una solución de planificación de recursos empresariales (ERP) que automatiza procesos de toda la empresa, como finanzas, recursos humanos, cadena de suministro y fabricación. Ofrece una arquitectura de tres niveles: cliente, aplicación y base de datos. Anteriormente, tenía que ejecutar la base de datos de Oracle E-Business Suite en una instancia de Amazon Elastic Compute Cloud (Amazon EC2) autogestionada, pero ahora puede beneficiarse de Amazon Relational Database Service (Amazon RDS) Custom.

Amazon RDS Custom para Oracle es un servicio de base de datos administrado para aplicaciones heredadas, personalizadas y empaquetadas que requieren acceso al sistema operativo y al entorno de base de datos subyacentes. Amazon RDS Custom automatiza las tareas y operaciones de administración de bases de datos y le permite, como administrador de bases de datos, acceder y personalizar el entorno de base de datos y el sistema operativo. Cuando migra su base de datos de Oracle a Amazon RDS Custom, Amazon Web Services (AWS) se encarga de las tareas más pesadas, como aquellas de respaldo, y garantiza una alta disponibilidad para que usted pueda centrarse en mantener la aplicación y la funcionalidad de Oracle E-Business Suite. Para obtener una lista completa de los factores clave a tener en cuenta durante el proceso de migración, consulte Estrategiqas de migración de bases de datos de Oracle en Recomendaciones de AWS.

Este patrón se centra en los pasos para migrar una base de datos Oracle independiente de Amazon EC2 a Amazon RDS Custom creando una copia de seguridad de RMAN y un sistema de archivos compartidos de Amazon EFS entre la instancia de EC2 y Amazon RDS Custom. Este patrón emplea una copia de seguridad completa en RMAN (denominada, en ocasiones, copia de seguridad de nivel 0). Por motivos de simplicidad, usa una copia de seguridad en frío en la que la aplicación se cierra y la base de datos se monta y no se abre. (También puede usar la duplicación de Oracle Data Guard o RMAN para realizar copias de seguridad. Sin embargo, este patrón no aborda dichas opciones).

Para obtener más información sobre cómo diseñar la arquitectura de Oracle E-Business Suite en AWS para conseguir una alta disponibilidad y recuperación de desastres, consulte el patrón Configurar una arquitectura HA/DR para Oracle E-Business Suite en Amazon RDS Custom con una base de datos en espera activa.

Nota: este patrón proporciona enlaces a las notas de soporte de Oracle. Necesitará una cuenta de Oracle Support para acceder a estos documentos.

Requisitos previos y limitaciones

Requisitos previos

- Base de datos de origen Oracle versión 12.1.0.2 o 19c (mínimo 19.3), ejecutada en Amazon EC2 con Oracle Linux 7 o Red Hat Enterprise Linux (RHEL) versión 7.x. Este patrón presupone que el nombre de la base de datos de origen es `VIS`, y que el nombre de la base de datos de contenedor adicional de Oracle 19c es `VISCDB`, pero puede usar otros nombres.

  Nota: también puede usar este patrón con bases de datos de origen Oracle en las instalaciones, siempre que tenga una conectividad de red adecuada entre la red en las instalaciones y Amazon Virtual Private Cloud (Amazon VPC).
- Una aplicación de Oracle E-Business Suite, versión 12.2.x (instancia visual). Este procedimiento se ha probado en la versión 12.2.11.
- Un único nivel de aplicación de Oracle E-Business Suite. Sin embargo, puede adaptar este patrón para que funcione con varios niveles de aplicación.
- Para Oracle 12.1.0.2, Amazon RDS Custom se ha configurado con, al menos, 16 GB de espacio de intercambio. De lo contrario, la CD de ejemplo de 12c muestra una advertencia. (Oracle 19c no requiere la CD de ejemplo, como se menciona más adelante en este documento).

Antes de empezar la migración, realice los siguientes pasos:

1. En la consola de Amazon RDS, cree una instancia de base de datos Amazon RDS Custom para Oracle con el nombre de base de datos `VIS` (o el nombre de su base de datos de origen). Para obtener más instrucciones, consulte Trabajar con Amazon RDS Custom en la documentación de AWS, y la publicación del blog Amazon RDS Custom para Oracle: nuevas capacidades de control en entornos de base de datos. Este paso garantiza que la base de datos tenga el mismo nombre que la base de datos de origen. (Si se deja en blanco, la instancia de EC2 y el nombre de la base de datos se definirán como `ORCL`). Asegúrese de crear su versión de motor personalizada (CEV) con, como mínimo, los parches que se han aplicado al origen. Para obtener más información, consulte Preparar la creación de una CEV en la documentación de Amazon RDS.

   Nota para Oracle 19c: actualmente es posible personalizar el nombre de la base de datos de contenedor de Amazon RDS en Oracle 19c. El valor predeterminado es `RDSCDB`. Asegúrese de crear la instancia de Oracle personalizada de RDS con la misma ID de sistema (SID) que la instancia de EC2 de origen. Por ejemplo, este patrón presupone que la SID de Oracle 19c es `VISCDB` en la instancia de origen. Por lo tanto, la SID de Oracle 19c de destino en Amazon RDS Custom también debería ser `VISCDB`.
2. Configure la instancia de base de datos de Amazon RDS Custom con el suficiente almacenamiento, vCPU y memoria según la base de datos de origen de Amazon EC2. Para ello, puede equiparar los tipos de instancia de Amazon EC2 en función de la vCPU y la memoria.
3. Para crear una instancia de Amazon EC2 y montar el sistema de archivos de Amazon EFS. Para obtener más instrucciones, consulte la publicación del blog Integrar Amazon RDS Custom para Oracle con Amazon EFS. Este patrón presupone que ha montado el volumen de Amazon EFS en `/RMAN` tanto en la instancia de base de datos Amazon EC2 de origen como en la instancia de Amazon RDS Custom de destino, y que existe conectividad de red entre el origen y el destino. También puede usar el mismo método mediante Amazon FSx o cualquier unidad compartida.

Supuestos

Este patrón presupone que la aplicación y la base de datos usan nombres de host lógicos, lo que reduce el número de pasos de migración. Puede ajustar estos pasos para usar nombres de host físicos, pero los nombres de host lógicos reducen la complejidad del proceso de migración. Para obtener más información acerca de las ventajas de usar nombres de host lógicos, consulte las siguientes notas de soporte:

- Para 12c, nota de soporte de Oracle 2246690.1
- Para 19c, nota de soporte de Oracle 2617788.1

Este patrón no abarca el escenario de actualización de Oracle 12c a 19c, sino que se centra en la migración de la misma versión de base de datos de Oracle que se ejecuta en Amazon EC2 a Amazon RDS Custom para Oracle.

Amazon RDS Custom para Oracle admite la personalización de Oracle Home. (Oracle Home almacena los archivos binarios de Oracle). Puede cambiar la ruta predeterminada `/rdsdbbin/oracle` por una ruta especificada por usted, como `/d01/oracle/VIS/19c`. Para mayor simplicidad, en las instrucciones de este patrón se asume la ruta predeterminada `/rdsdbbin/oracle`.

Limitaciones

Este patrón no es compatible con las siguientes características y configuraciones:

- Establecer el parámetro `ARCHIVE_LAG_TARGET` de la base de datos en un valor fuera del rango de 60 a 7200
- Inhabilitar el modo de registro de la instancia de base de datos (`NOARCHIVELOG`)
- Desactivar el atributo `EBS-optimized` de la instancia de EC2
- Modificar los volúmenes originales de Amazon Elastic Block Store (Amazon EBS) adjuntos a la instancia de EC2
- Añadir nuevos volúmenes de EBS o cambiar el tipo de volumen de `gp2` a `gp3`
- Soporte para TNS ifile
- Cambiar la ubicación y el nombre de `control_file` (debe ser `/rdsdbdata/db/VISCDB_A/controlfile/control-01.ctl`, dónde `VISCDB` es el nombre del CDB)

Para obtener información adicional sobre estas y otras configuraciones no compatibles, consulte Corregir configuraciones no compatibles en la documentación de Amazon RDS.

Versiones de producto

Para ver las versiones de Oracle Database y clases de instancia compatibles con Amazon RDS Custom, consulte Disponibilidad y requisitos de Amazon RDS Custom para Oracle.

Arquitectura

El siguiente diagrama de arquitectura representa un sistema Oracle E-Business Suite ejecutado en una única zona de disponibilidad en AWS. Se accede al nivel de aplicación a través de un

Equilibrador de carga de aplicación. Tanto la aplicación como las bases de datos se encuentran en subredes privadas, y el nivel de base de datos Amazon RDS Custom y Amazon EC2 emplea un sistema de archivos compartidos Amazon EFS para almacenar y acceder a los archivos de copia de seguridad de RMAN.

Herramientas

Servicios de AWS

- Amazon RDS Custom para Oracle es un servicio de base de datos administrado para aplicaciones heredadas, personalizadas y empaquetadas que requieren acceso al sistema operativo y al entorno de base de datos subyacentes. Amazon RDS Custom automatiza las tareas y operaciones de administración de bases de datos y le permite, como administrador de bases de datos, acceder y personalizar el entorno de base de datos y el sistema operativo.
- Amazon Elastic File System (Amazon EFS) es un sistema de archivos elástico, sencillo y sin servidor que permite añadir y eliminar archivos sin necesidad de administración ni aprovisionamiento. Este patrón emplea un sistema de archivos compartidos de Amazon EFS para almacenar y acceder a los archivos de copia de seguridad de RMAN.
- AWS Secrets Manager es un servicio administrado por AWS que le permite rotar, administrar y recuperar credenciales de bases de datos, claves de API y otra información secreta con facilidad. Amazon RDS Custom almacena el par de claves y las credenciales del usuario de la base de datos en Secrets Manager al crear la base de datos. En este patrón se recuperan las contraseñas de usuario de la base de datos de Secrets Manager para crear los usuarios `RDSADMIN` y `ADMIN` y cambiar las contraseñas de sys y sistema.

Otras herramientas

- RMAN es una herramienta que proporciona soporte de copia de seguridad y recuperación para bases de datos Oracle. Este patrón usa RMAN para realizar una copia de seguridad en frío de la base de datos Oracle de origen en Amazon EC2 que, posteriormente, se restaura en Amazon RDS Custom.

Prácticas recomendadas

- Use nombres de host lógicos. Esto reduce considerablemente la cantidad de scripts a ejecutar tras la clonación. Para obtener más información, consulte el documento de soporte de Oracle 2246690.1.
- Amazon RDS Custom usa Oracle Automatic Memory Management (AMM) de forma predeterminada. Si desea usar el kernel hugemem, puede configurar Amazon RDS Custom para que emplee gestión automática de memoria compartida (ASMM) en su lugar.
- El parámetro de `memory_max_target` no está habilitado de forma predeterminada. El marco usa este parámetro en segundo plano para crear réplicas de lectura.
- Habilite la base de datos Oracle Flashback. Esta característica resulta útil en escenarios de pruebas de conmutación por error (no de transición) para restablecer el modo de espera.
- En los parámetros de inicialización de la base de datos, personalice el PFILE estándar proporcionado por la instancia de base de datos de Amazon RDS Custom para Oracle E-Business Suite en lugar de usar el SPFILE de la base de datos Oracle de origen. El motivo de esto es que los espacios en blanco y los comentarios causan problemas al crear réplicas de lectura en Amazon RDS Custom. Para obtener más información acerca del parámetro de inicialización de la base de datos, consulte documento de soporte de Oracle 396009.1.

En la siguiente sección Épica, proporcionamos instrucciones independientes para las versiones 12.1.0.2 y 19c de Oracle.

Epics

Cierre la aplicación de origen

Tarea	Descripción	Habilidades requeridas
Cierre la aplicación.	Para cerrar la aplicación de origen, ejecute estos comandos: `$ su - applmgr` `$ cd $INST_TOP/admin/scripts` `$ ./adstpall.sh`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree el archivo .zip.	Cree el archivo `appsutil.zip` en el nivel de aplicación de origen. Usará este archivo más adelante para configurar el nodo de base de datos de Amazon RDS Custom. `$ perl $AD_TOP/bin/admkappsutil.pl`	Administrador de base de datos
Copie el archivo .zip en Amazon EFS.	Copie `appsutil.zip` desde `$INST_TOP/admin/out` a su volumen compartido de Amazon EFS (`/RMAN/appsutil`). Puede transferir el archivo manualmente mediante una copia segura (SCP) u otro mecanismo de transferencia.	Administrador de base de datos

Realice una clonación previa de la base de datos de origen

Tarea	Descripción	Habilidades requeridas
Realice una clonación previa del nivel de base de datos en Amazon EC2.	Inicie sesión como usuario de Oracle y ejecute: `$ cd $ORACLE_HOME/appsutil/scripts/$CONTEXT_NAME` `$ perl adpreclone.pl dbTier` Compruebe el archivo de registro generado para	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	confirmar que la operación se ha realizado correctamente.	
Copie el archivo appsutil.zip en el sistema de archivos de Amazon EFS.	Cree una copia de seguridad en formato tar y copie `$ORACLE_HOME/appsutil` en el sistema de archivos de Amazon EFS compartido (por ejemplo, `/RMAN/appsutil`): `$ cd $ORACLE_HOME` `$ tar cvf sourceappsutil.tar appsutil` `$ cp sourceappsutil.tar /RMAN/appsutil`	Administrador de base de datos

Realice una copia de seguridad completa RMAN en frío de la base de datos Amazon EC2 de origen

Tarea	Descripción	Habilidades requeridas
Cree un script de copia de seguridad.	Realice una copia de seguridad completa RMAN de la base de datos de origen en el sistema de archivos Amazon EFS compartido. Para mayor simplicidad, este patrón realiza una copia de seguridad RMAN en frío. Sin embargo, puede modificar estos pasos para realizar una copia de seguridad de RMAN activa con Oracle Data Guard	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	a fin de reducir el tiempo de inactividad. 1. Inicie la base de datos Amazon EC2 de origen en modo de montaje: `$ sqlplus / as sysdba` `$ SQL> shutdown immediate` `$ SQL> startup mount` 2. Cree un script de copia de seguridad RMAN (use uno de los siguientes ejemplos, según su versión de Oracle, o ejecute uno de sus scripts RMAN existentes) para hacer una copia de seguridad de la base de datos en el sistema de archivos Amazon EFS que ha montado (en este ejemplo, `/RMAN`). Para Oracle 12.1.0.2: `$ vi FullRMANColdBackup.sh` `#!/bin/bash` `. /home/oracle/.bash_profile` `export ORACLE_SID=VIS` `export ORACLE_HOME=/d01/oracle/VIS/12.1.0` `export DATE=$(date +%y-%m-%d_%H%M%S)`	

Tarea	Descripción	Habilidades requeridas

```
rman target / log=/RMAN
/VISDB_${DATE}.log <<
 EOF
run
{
allocate channel ch1
 device type disk format
 '/RMAN/visdb_full_
bkp_%u';
allocate channel ch2
 device type disk format
 '/RMAN/visdb_full_
bkp_%u';
crosscheck backup;
delete noprompt
 obsolete;
BACKUP AS COMPRESSED
 BACKUPSET DATABASE PLUS
 ARCHIVELOG;
backup archivelog all;
release channel ch1;
release channel ch2;
}
EOF
```

Para Oracle 19c:

```
$ vi FullRMANColdBackup
.sh
#!/bin/bash
. /home/oracle/.bash
_profile

export ORACLE_SI
D=VISCDB
export ORACLE_HOME=/
d01/oracle/VIS/19c
export DATE=$(date +
%y-%m-%d_%H%M%S)
```

Tarea	Descripción	Habilidades requeridas
	`rman target / log=/RMAN /VISDB_${DATE}.log << EOF run { allocate channel ch1 device type disk format '/RMAN/visdb_full_ bkp_%u'; allocate channel ch2 device type disk format '/RMAN/visdb_full_ bkp_%u'; crosscheck backup; delete noprompt obsolete; BACKUP AS COMPRESSED BACKUPSET DATABASE PLUS ARCHIVELOG; backup archivelog all; backup current controlfile format '/ RMAN/cntrl.bak'; release channel ch1; release channel ch2; } EOF`	
Ejecute el script de copia de seguridad.	Cambie los permisos, inicie sesión como usuario de Oracle y ejecute el script: `$ chmod 755 FullRMANC oldBackup.sh $ ./FullRMANColdBack up.sh`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Compruebe que no haya errores y anote el nombre del archivo de copia de seguridad.	Compruebe si hay errores en el archivo RMAN. Si todo está correcto, enumere la copia de seguridad del archivo de control. Nombre del archivo de salida. Para Oracle 12.1.0.2: `RMAN> connect target /` `RMAN> list backup of controlfile;` `BS Key Type LV Size Device Type Elapsed Time Completion Time` `------- ---- -- ---------- --------- ---------- ---------------` `9 Full 1.11M DISK 00:00:04 23-APR-22` `BP Key: 9 Status: AVAILABLE Compressed: YES Tag: TAG20220423T121011` `Piece Name: /RMAN/visdb_full_bkp_100rlsbt` `Control File Included: Ckp SCN: 122045953 96727 Ckp time: 23-APR-22` Usará el archivo de copia de seguridad `/RMAN/visdb_full_bkp_100rls`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`bt` más adelante, cuando restaure la base de datos en Amazon RDS Custom. Para Oracle 19c: `RMAN> connect target /` `RMAN> list backup of controlfile;` `BS Key  Type LV Size       Device Type Elapsed Time Completion Time` `------- ---- -- ---------- ----------- ------------ ---------------` `38      Full    17.92M     DISK        00:00:01     25-NOV-22` `        BP Key: 38   Status: AVAILABLE  Compressed: NO  Tag: TAG20221125T095014` `        Piece Name: /RMAN/cntrl.bak` `  Control File Included: Ckp SCN: 12204620188873   Ckp time: 23-NOV-22` Usará el archivo de copia de seguridad `/RMAN/cntrl.bak` más adelante, cuando restaure la base de datos en Amazon RDS Custom.	

Configure la base de datos Amazon RDS Custom de destino

Tarea	Descripción	Habilidades requeridas
Cambie el archivo de hosts y defina el nombre del host.	Nota: los comandos de esta sección deben ejecutarse como usuario raíz. 1. Edite el archivo `/etc/hosts` en la instancia de base de datos de Amazon RDS Custom. Una forma sencilla de hacerlo es copiar las entradas de la base de datos y del host de la aplicación del archivo de hosts de la base de datos Amazon EC2 de origen. `<IP-address> OEBS-app01.localdomain OEBS-app01 OEBS-app01log.localdomain OEBS-app01log` `<IP-address> OEBS-db01.localdomain OEBS-db01 OEBS-db01log.localdomain OEBS-db01log` `<IP-address>` es la dirección IP del nodo de la base de datos, que debe sustituir por la dirección IP de Amazon RDS Custom. Los nombres de host lógicos se adjuntan a `*log`. 2. Cambie el nombre de host de la base de datos ejecutand	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	o el comando `hostnamectl` : `$ sudo hostnamectl set-hostname --static persistent-hostname` Por ejemplo: `$ sudo hostnamectl set-hostname --static OEBS-db01log` Para obtener información adicional, consulte el artículo del Centro de conocimiento sobre asignación de nombres de host estáticos. 3. Reinicie una instancia de base de datos de Amazon RDS Custom. No se preocupe por cerrar la base de datos, ya que la eliminará en un paso posterior. `$ reboot` 4. Cuando la instancia de base de datos de Amazon RDS Custom vuelva a funcionar, inicie sesión y compruebe que el nombre de host ha cambiado: `$ hostname`	

Tarea	Descripción	Habilidades requeridas
	`oebs-db01`	
Instale el software Oracle E-Business Suite.	Instale los RPM recomendados por Oracle E-Business Suite en la ubicación de inicio de Oracle, en la instancia de base de datos de Amazon RDS Custom. Para obtener más información, consulte la nota de soporte de Oracle #1330701.1. Lo siguiente es una lista parcial de los resultados. La lista de RPM cambia en cada versión, por lo que deberá asegurarse de instalar todos los RPM necesarios. Como usuario raíz, ejecute: `$ sudo yum -y update` `$ sudo yum install -y elfutils-libelf-devel*` `$ sudo yum install -y libXp-1.0.2-2.1*.i686` `$ sudo yum install -y libXp-1.0.2-2.1*` `$ sudo yum install -y compat-libstdc++-*` Compruebe que todos los parches necesarios estén instalados antes de continuar con el siguiente paso.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Instale el servidor VNC.	Nota: puede omitir este paso en Oracle 19c, ya que la CD de ejemplos no es necesaria; consulte la nota de soporte de Oracle 2782085.1. Para Oracle 12.1.0.2: Instale el servidor VNC y sus paquetes de escritorio dependientes. Este paso es necesario para instalar la CD de ejemplos de 12c en el siguiente paso. 1. Como usuario raíz, ejecute: `$ sudo yum install -y tigervnc-server` `$ sudo yum install -y *kde*` `$ sudo yum install -y *xorg*` 2. Inicie el servidor VNC para el usuario `rdsdb` y establezca la contraseña de VNC: `$ su - rdsdb` `$ vncserver :1` `$ vncpassword`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Instale la CD de ejemplos de 12c.	Nota: puede omitir este paso en Oracle 19c, ya que la CD de ejemplos no es necesaria; consulte la nota de soporte de Oracle 2782085.1. Para Oracle 12.1.0.2: 1. Descargue los archivos de instalación de https://edelivery.oracle.com/. Para Oracle E-Business Suite 12.2.11 – Oracle Database 12c versión 1 (12.1.0.2), busque Examples for Linux x86-64 V100102-01.zip. 2. Cree un directorio para almacenar la CD de ejemplos: `$ mkdir /RMAN/12c examples` 3. Copie el archivo .zip de la CD de ejemplos a este directorio mediante el mecanismo de transferencia que prefiera (por ejemplo, SCP): `V100102-01.zip` 4. Cambie la propiedad a `rdsdb`:	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`$ chown -R rdsdb:rdsdb /RMAN/12cexamples` 5. Como usuario `rdsdb`, descomprima el archivo: `$ unzip V10010201.zip` 6. Conéctese desde un cliente que tenga acceso al cliente de VNC y a Amazon RDS Custom. Asegúrese de tener abiertos los puertos de firewall y contar con la conectividad de red necesaria para permitir el acceso de VNC. Por ejemplo, un servidor VNC que se ejecute en `display :1` necesitará abrir el puerto 5901 en el grupo de seguridad asociado al host EC2 de Amazon RDS Custom. 7. Acceda al directorio en el que ha copiado la CD de ejemplos: `$ cd /RMAN/12cexamples/examples` 8. Ejecute el instalador. Asegúrese de comprobar la ubicación del archivo `oraInst.loc` .	

Tarea	Descripción	Habilidades requeridas
	`./runInstaller -invPtrLoc /rdsdbbin/oracle.12.1.custom.r1.EE.1/oraInst.loc` 9. Use los siguientes parámetros durante la instalación de la CD de ejemplos: `Skip Software Updates` `Downloads` `Select Oracle Home 12.1.0.2 (Oracle Base = /rdsdbbin)` `(Software Location = /rdsdbbin/oracle/12.1.custom.r1.EE.1)` 10. El programa de instalación incluye cinco pasos con instrucciones. Siga los pasos hasta completar la instalación.	

Elimine la base de datos inicial y cree los directorios para almacenar los archivos de la base de datos

Tarea	Descripción	Habilidades requeridas
Pause el modo de automatización.	Debe pausar el modo de automatización en su instancia de base de datos de Amazon RDS Custom antes de continuar con los siguientes pasos. Así evitará que la	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	automatización interfiera con la actividad de RMAN. Pause la automatización ejecutando el siguiente comando en la Interfaz de la línea de comandos de AWS (AWS CLI). (Asegúrese de haber configurado la AWS CLI antes). `aws rds modify-db-instance \ --db-instance-id entifier VIS \ --automation-mode all-paused \ --resume-full-au tomation-mode-minute 360 \ --region eu-west-1` Cuando especifique la duración de la pausa, asegúrese de dejar tiempo suficiente para la restauración de RMAN. Este tiempo dependerá del tamaño de la base de datos de origen, por lo que deberá modificar el valor 360 en consecuencia.	

Tarea	Descripción	Habilidades requeridas
Elimine la base de datos inicial.	Elimine la base de datos Amazon RDS Custom existente. Como usuario raíz de Oracle, ejecute los siguientes comandos. (El usuario por defecto es `rdsdb`, a menos que lo haya personalizado). `$ sqlplus / as sysdba` `SQL> shutdown immediate ;` `SQL> startup nomount restrict;` `SQL> alter database mount;` `SQL> drop database;` `SQL> exit`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree directorios para almacenar los archivos de la base de datos.	Para Oracle 12.1.0.2: Cree directorios para la base de datos, el archivo de control, los archivos de datos y el registro en línea. Use el directorio principal del parámetro `control_files` en el comando anterior (en este caso, `VIS_A`). Como usuario particular de Oracle (valor predeterminado, `rdsdb`), ejecute los siguientes comandos. `$ mkdir -p /rdsdbdata/db/VIS_A/controlfile` `$ mkdir -p /rdsdbdata/db/VIS_A/datafile` `$ mkdir -p /rdsdbdata/db/VIS_A/onlinelog` Para Oracle 19c: Cree directorios para la base de datos, el archivo de control, los archivos de datos y el registro en línea. Use el directorio principal del parámetro `control_files` en el comando anterior (en este caso, `VISCDB_A`). Como usuario particular de Oracle (valor predeterminado, `rdsdb`), ejecute los siguientes comandos.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`$ mkdir -p /rdsdbdata/db/cdb/VISCDB_A/controlfile` `$ mkdir -p /rdsdbdata/db/cdb/VISCDB_A/datafile` `$ mkdir -p /rdsdbdata/db/cdb/VISCDB_A/onlinelog` `$ mkdir -p /rdsdbdata/db/cdb/VISCDB_A/onlinelog/arch` `$ mkdir /rdsdbdata/db/pdb/VISCDB_A`	

Tarea	Descripción	Habilidades requeridas
Cree y modifique el archivo de parámetros de Oracle E-Business Suite.	En este paso, no copiará el archivo de parámetros del servidor (SPFILE) de la base de datos de origen. En su lugar, usará el archivo de parámetros estándar (PFILE) creado con la instancia de base de datos de Amazon RDS Custom y añadirá los parámetros que necesite para Oracle E-Business Suite. Al eliminar la base de datos, la automatización de Amazon RDS crea una copia de seguridad del archivo `init.ora`, que se asocia a la base de datos de Amazon RDS Custom. Este archivo se llama `oracle_pfile` y se encuentra en `/rdsdbdata/config`. Para Oracle 12.1.0.2: 1. Copie `/rdsdbdata/config/oracle_pfile` en `$ORACLE_HOME`. `$ cp /rdsdbdata/config/oracle_pfile $ORACLE_HOME/dbs/initVIS.ora` 2. Edite el archivo `initVIS.ora` en la instancia de base de datos de Amazon RDS	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Custom. Valide todos los parámetros de origen y añada los parámetros que necesite. Para obtener más información, consulte la nota de soporte de Oracle 396009.1. Importante: asegúrese de que no haya comentarios en los parámetros que añada. Los comentarios causarán problemas con la automatiz ación, como la creación de réplicas de lectura y la emisión de point-in-time recuperac iones (PITRs). 3. Añada al archivo `initVIS.ora` parámetros similares a los siguientes, en función de sus necesidades: `*.workarea_size_po licy='AUTO'` `*.plsql_code_ty pe='INTERPRETED'` `*.cursor_sharing='E XACT'` `*._b_tree_bitmap_plan s=FALSE` `*.session_cached_cu rsors=500` `*.optimizer_adapt ive_features=false` `*.optimizer_secur e_view_merging=false` `*.SQL92_SECURITY=TRUE`	

Tarea	Descripción	Habilidades requeridas
	*.temp_undo_enabled= true _system_trig_enabled = TRUE nls_language = american nls_territory = america nls_numeric_characters = "." nls_comp = binary nls_sort = binary nls_date_format = DD-MON-RR nls_length_semantics = BYTE aq_tm_processes = 1 _sort_eliminatio n_cost_ratio =5 _like_with_bind _as_equality = TRUE _fast_full_scan_enabled = FALSE _b_tree_bitmap_plans = FALSE optimizer_secure_view _merging = FALSE _optimizer_autostats_ job = FALSE parallel_max_servers = 8 parallel_min_servers = 0 parallel_degree_policy = MANUAL sec_case_sensitive_l ogon = FALSE compatible = 12.1.0 o7_dictionary_access ibility = FALSE utl_file_dir =/tmp	

Tarea	Descripción	Habilidades requeridas
	4. Modifique lo siguiente. Los valores dependerán de su sistema de origen. Revíselos en función de su configuración actual. `*.open_cursors=500` `*.undo_tablespace='APPS_UNDOTS1` 5. Elimine la referencia SPFILE. `*.spfile='/rdsdbbin/oracle/dbs/spfileVIS.ora'` Notas: • No modifique los valores proporcionados por el PFILE de Amazon RDS Custom para `control_files` y `db_unique_name`. Amazon RDS espera estos valores. Si los modifica, surgirán problemas en caso de que trate de crear una réplica de lectura en el futuro. • Amazon RDS Custom utiliza Oracle Automatic Memory Management (AMM) de forma predeterminada. Si desea usar el hugemem, puede configurar Amazon	

Tarea	Descripción	Habilidades requeridas
	RDS Custom para que emplee gestión automática de memoria compartida (ASMM) en su lugar. • El parámetro de `memory_max_target` no está habilitado de forma predeterminada. El marco Amazon RDS utiliza este parámetro en segundo plano para crear réplicas de lectura. 6. Confirme que no hay problemas con el archivo `initVIS.ora` ejecutando el comando `startup nomount`: `SQL> startup nomount pfile=/rdsdbbin/oracle/dbs/initVIS.ora;` `SQL> create spfile='/rdsdbdata/admin/VIS/pfile/spfileVIS.ora' from pfile;` `SQL> exit` 7. Cree un enlace simbólico para SPFILE. `$ ln -s /rdsdbdata/admin/VIS/pfile/spfileVIS.ora $ORACLE_HOME/dbs/` Para Oracle 19c:	

Tarea	Descripción	Habilidades requeridas
	1. Copie `/rdsdbdata/config/oracle_pfile` en `$ORACLE_HOME` . `$ cp /rdsdbdata/config/oracle_pfile $ORACLE_HOME/dbs/initVISCDB.ora` 2. Edite el archivo `initVISCDB.ora` en la instancia de base de datos de Amazon RDS Custom. Valide todos los parámetros de origen y añada los parámetros que necesite. Para obtener más información, consulte la nota de soporte de Oracle 396009.1. Importante: asegúrese de que no haya comentarios en los parámetros que añada. Si hay comentarios, se producirán problemas con la automatización, como la creación de réplicas de lectura y la emisión de point-in-time recuperaciones (PITRs). 3. Añada al archivo `initVISCDB.ora` parámetros similares a los siguientes, en función de sus necesidades.	

Tarea	Descripción	Habilidades requeridas
	*.instance_name=VI SCDB *.sec_case_sensit ive_logon= FALSE *.result_cache_ma x_size = 600M *.optimizer_adaptive_p lans =TRUE *.optimizer_adaptive_ statistics = FALSE *.pga_aggregate_limit = 0 *.temp_undo_enabled = FALSE *._pdb_name_case_sens itive = TRUE *.event='10946 trace name context forever, level 8454144' *.workarea_size_p olicy='AUTO' *.plsql_code_t ype='INTERPRETED' *.cursor_sharing=' EXACT' *._b_tree_bitmap_pla ns=FALSE *.session_cached_c ursors=500 *.optimizer_secu re_view_merging=false *.SQL92_SECURITY=TRUE _system_trig_enabled = TRUE nls_language = american nls_territory = america nls_numeric_charact ers = "." nls_comp = binary nls_sort = binary	

Tarea	Descripción	Habilidades requeridas
	nls_date_format = DD-MON-RR nls_length_semantics = BYTE aq_tm_processes = 1 _sort_eliminatio n_cost_ratio =5 _like_with_bind _as_equality = TRUE _fast_full_scan_enable d = FALSE _b_tree_bitmap_plans = FALSE optimizer_secure_view _merging = FALSE _optimizer_autostats_ job = FALSE parallel_max_servers = 8 parallel_min_servers = 0 parallel_degree_policy = MANUAL 4. Modifique lo siguiente. Los valores dependerán de su sistema de origen. Revíselos en función de su configuración actual. *.open_cursors=500 *.undo_tablespace ='UNDOTBS1' 5. Elimine la referencia SPFILE:	

Tarea	Descripción	Habilidades requeridas
	`*.spfile='/rdsdbbin/oracle/dbs/spfileVISCDB.ora'` Notas: • No modifique los valores proporcionados por el PFILE de Amazon RDS Custom para `control_files` y `db_unique_name`. Amazon RDS espera estos valores. Si los modifica, surgirán problemas en caso de que trate de crear una réplica de lectura en el futuro. • Amazon RDS Custom utiliza Oracle Automatic Memory Management (AMM) de forma predeterminada. Si desea usar el hugemem, puede configurar Amazon RDS Custom para que emplee gestión automática de memoria compartida (ASMM) en su lugar. • El parámetro de `memory_max_target` no está habilitado de forma predeterminada. El marco Amazon RDS utiliza este parámetro en segundo plano para crear réplicas de lectura.	

Tarea	Descripción	Habilidades requeridas
	6. Confirme que no hay problemas con el archivo `initVISCDB.ora` ejecutando el comando `startup nomount`: `SQL> startup nomount pfile=/rdsdbbin/oracle/dbs/initVISCDB.ora;` `SQL> create spfile='/rdsdbdata/admin/VISCDB/pfile/spfileVISCDB.ora' from pfile;` `SQL> exit` 7. Cree un enlace simbólico para SPFILE. `$ ln -s /rdsdbdata/admin/VISCDB/pfile/spfileVISCDB.ora $ORACLE_HOME/dbs/`	

Tarea	Descripción	Habilidades requeridas
Restaure la base de datos Amazon RDS Custom a partir de la copia de seguridad.	Para Oracle 12.1.0.2: 1. Restaure el archivo de control usando el archivo de copia de seguridad de origen que capturó anteriormente: `RMAN> connect target /` `RMAN> RESTORE CONTROLFILE FROM '/RMAN/visdb_full_bkp_100rlsbt';` `Starting restore at 10-APR-22` `using target database control file instead of recovery catalog` `allocated channel: ORA_DISK_1` `channel ORA_DISK_1: SID=201 device type=DISK` `channel ORA_DISK_1: restoring control file` `channel ORA_DISK_1: restore complete, elapsed time: 00:00:01` `output file name=/rdsdbdata/db/VIS_A/controlfile/control-01.ctl` `Finished restore at 10-APR-22` 2. Catalogue las piezas de copia de seguridad para emitir un `RMAN restore`:	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`RMAN> alter database mount;` `RMAN> catalog start with '/RMAN/visdb';` 3. Cree un script para restaurar la base de datos: `$ vi restore.sh` `rman target / log=/home/rdsdb/rman.log << EOF` `run` `{` `set newname for database to '/rdsdbdata/db/VIS_A/datafile/%b';` `restore database;` `switch datafile all;` `switch tempfile all;` `}` `EOF` 4. Restaure el origen en la base de datos Amazon RDS Custom de destino. Deberá cambiar los permisos del script para permitir su ejecución y, a continuación, ejecutar el script `restore.sh` para restaurar la base de datos. `$ chmod 755 restore.sh` `$ nohup ./restore.sh &` Para Oracle 19c:	

Tarea	Descripción	Habilidades requeridas
	1. Restaure el archivo de control usando el archivo de copia de seguridad de origen que capturó anteriormente: `RMAN> connect target /` `RMAN> RESTORE CONTROLFILE FROM '/RMAN/cntrl.bak';` `Starting restore at 07-JUN-23` `using target database control file instead of recovery catalog` `allocated channel: ORA_DISK_1` `channel ORA_DISK_1: SID=201 device type=DISK` `channel ORA_DISK_1: restoring control file` `channel ORA_DISK_1: restore complete, elapsed time: 00:00:01` `output file name=/rdsdbdata/db/cdb/VISCDB_A/controlfile/control-01.ctl` `Finished restore at 07-JUN-23` 2. Catalogue las piezas de copia de seguridad para emitir un RMAN `restore`: `RMAN> alter database mount;` `RMAN> catalog start with '/RMAN/visdb';`	

Tarea	Descripción	Habilidades requeridas
	Si tiene problemas con el comando `start with`, puede añadir las piezas de copia de seguridad de forma individual; por ejemplo: `RMAN> catalog backuppiece '/RMAN/visdb_full_bkp_1d1e507m';` y, a continuación, ejecutar de nuevo el comando para cada pieza de copia de seguridad. 3. Cree un script para restaurar la base de datos. Modifique el nombre de la base de datos conectable en función de sus requisitos. Asigne canales paralelos en función de la cantidad de VCPU disponibles para acelerar el proceso de restauración. `$ vi restore.sh` `rman target / log=/home/rdsdb/rmancdb.log <<` `EOF` `run {` `allocate channel c1` `type disk;` `allocate channel c2` `type disk;` `.... .... ....` `allocate channel c<N>` `type disk;`	

Tarea	Descripción	Habilidades requeridas
	`set newname for database to '/rdsdbdata/db/cdb/VISCDB_A/datafile/%b';` `set newname for database root to '/rdsdbdata/db/cdb/VISCDB_A/datafile/%f_%b';` `set newname for database "PDB$SEED" to '/rdsdbdata/db/cdb/pdbseed/%f_%b';` `set newname for pluggable database VIS to '/rdsdbdata/db/pdb/VISCDB_A/%f_%b';` `restore database;` `switch datafile all;` `switch tempfile all;` `release channel c1;` `release channel c2;` `release channel c3;` `.... .... ....` `release channel c<N>;` `}` `EOF` 4. Restaure el origen en la base de datos Amazon RDS Custom de destino. Deberá cambiar los permisos del script para permitir su ejecución y, a continuación, ejecutar el script `restore.sh` para restaurar la base de datos. `$ chmod 755 restore.sh`	

Tarea	Descripción	Habilidades requeridas
	`$ nohup ./restore.sh &`	

Tarea	Descripción	Habilidades requeridas
Compruebe los archivos de registro en busca de posibles problemas.	Para Oracle 12.1.0.2: 1. Revise el archivo `rman.log` para comprobar que no hay problemas: `$ cat /home/rdsdb/rman.log` 2. Confirme la ruta de los archivos de registro registrados en el archivo de control: `SQL> select member from v$logfile;` `MEMBER` `----------` `/d01/oracle/VIS/data/log1.dbf` `/d01/oracle/VIS/data/log2.dbf` `/d01/oracle/VIS/data/log3.dbf` 3. Cambie el nombre de los archivos de registro para que coincidan con la ruta del archivo de destino. Sustituya la ruta de modo que coincida con el resultado del paso anterior:	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`SQL> ALTER DATABASE RENAME FILE '/d01/oracle/VIS/data/log1.dbf' TO '/rdsdbdata/db/VIS_A/onlinelog/log1.dbf';` `SQL> ALTER DATABASE RENAME FILE '/d01/oracle/VIS/data/log2.dbf' TO '/rdsdbdata/db/VIS_A/onlinelog/log2.dbf';` `SQL> ALTER DATABASE RENAME FILE '/d01/oracle/VIS/data/log3.dbf' TO '/rdsdbdata/db/VIS_A/onlinelog/log3.dbf';` Para Oracle 19c: 1. Revise el archivo `rmancdb.log` para comprobar que no hay problemas: `$ cat /home/rdsdb/rmancdb.log` 2. Confirme la ruta de los archivos de registro registrados en el archivo de control: `SQL> select member from v$logfile;` `MEMBER` `----------` `----------` `----------`	

Tarea	Descripción	Habilidades requeridas
	`` ------------------ -------- /d01/oracle/VIS/or adata/VISCDB/redo0 3.log /d01/oracle/VIS/orada ta/VISCDB/redo02.log /d01/oracle/VIS/ oradata/VISCDB/re do01.log ```	
	3. Cambie el nombre de los archivos de registro para que coincidan con la ruta del archivo de destino. Sustituya la ruta de modo que coincida con el resultado del paso anterior: ``` SQL> ALTER DATABASE RENAME FILE '/d01/ora cle/VIS/oradata/VI SCDB/redo01.log' TO '/rdsdbdata/db/cdb/ VISCDB_A/onlinelog/ log1.dbf'; SQL> ALTER DATABASE RENAME FILE '/d01/ora cle/VIS/oradata/VI SCDB/redo02.log' TO '/rdsdbdata/db/cdb/ VISCDB_A/onlinelog/ log2.dbf'; SQL> ALTER DATABASE RENAME FILE '/d01/ora cle/VIS/oradata/VI SCDB/redo03.log' TO '/rdsdbdata/db/cdb/ ```	

Tarea	Descripción	Habilidades requeridas
	`VISCDB_A/onlinelog/ log3.dbf';` 4. Confirme la ruta, el estado de los archivos de registro y el número de grupo registrado en el archivo de control: `SQL> column REDOLOG_F ILE_NAME format a50 SQL> SELECT a.GROUP#, a.status, b.MEMBER AS REDOLOG_FILE_NAME, (a.BYTES/1024/1024) AS SIZE_MB FROM v$log a JOIN v$logfile b ON a.Group#=b.Group# ORDER BY a.GROUP#;` `GROUP# STATUS REDOLOG_F ILE_NAME SIZE_MB 1 CURRENT /rdsdbdat a/db/cdb/VISCDB_A/ onlinelog/log1.dbf 512 2 INACTIVE /rdsdbdat a/db/cdb/VISCDB_A/ onlinelog/log2.dbf 512 3 INACTIVE /rdsdbdat a/db/cdb/VISCDB_A/ onlinelog/log3.dbf 512`	

Tarea	Descripción	Habilidades requeridas
Confirme que puede abrir la base de datos de Amazon RDS Custom y crear archivos de registro OMF.	Amazon RDS Custom para Oracle simplifica las operaciones mediante Oracle Managed Files (OMF). Puede convertir las réplicas de lectura en instancias independientes, pero primero deberá crear los archivos de registro mediante OMF. Este paso garantiza que se use la ruta correcta al promover la instancia. Para obtener más información sobre cómo promover réplicas de lectura, consulte la documentación de Amazon RDS. Si no se usan los archivos OMF, es posible que se produzcan problemas al intentar promover las réplicas de lectura. 1. Abra la base de datos con `resetlogs` : `SQL> alter database open resetlogs;` Note: si recibe el error ORA-00392: log xx of thread 1 is being cleared, operation not allowed, siga los pasos de la sección Solución de problemas para ORA-00392.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	2. Confirme que la base de datos está abierta: `SQL> select open_mode from v$database;` `OPEN_MODE` `--------------------` `READ WRITE` 3. Cree los archivos de registro OMF. Cambie los números de grupo, el número y el tamaño de los grupos según sus necesidades usando el resultado de la anterior consulta del archivo de registro. El siguiente ejemplo comienza en el grupo 4 y agrega tres grupos para mayor simplicidad. `SQL> alter database add logfile group 4 size 512M;` `Database altered.` `SQL> alter database add logfile group 5 size 512M;` `Database altered.` `SQL> alter database add logfile group 6 size 512M;` `Database altered.` 4. Elimine los archivos anteriores que no sean OMF. Puede personalizar este	

Tarea	Descripción	Habilidades requeridas
	ejemplo en función de sus necesidades y del resultado de la consulta de los pasos anteriores: `SQL> alter database drop logfile group 1;` `System altered.` `SQL> alter database drop logfile group 2;` `System altered.` `SQL> alter database drop logfile group 3;` `System altered.` Nota: si recibe un error ORA-01624 al intentar eliminar los archivos de registro, consulta la sección de Solución de problemas. 5. Confirme que puede ver los archivos OMF creados. (La ruta del directorio varía para las versiones 12.1.0.2 y 19c de Oracle, pero el concepto es el mismo). `SQL> select member from v$logfile;` `MEMBER` `----------` `----------` `----------` `/rdsdbdata/db/cdb/` `VISCDB_A/onlinelog/` `o1_mf_4_ksrbslny_.log`	

Tarea	Descripción	Habilidades requeridas
	`/rdsdbdata/db/cdb/VIS CDB_A/onlinelog/o1 _mf_5_ksrchw0k_.log /rdsdbdata/db/cdb/ VISCDB_A/onlinelog/ o1_mf_6_ksrcnl9v_.log` 6. Reinicie la base de datos y confirme que la instancia está ejecutando SPFILE: `SQL> shutdown immediate SQL> startup SQL> show parameter spfile` En el caso de Oracle 12.1.0.2, esta consulta devuelve: `spfile /rdsdbbin /oracle/dbs/spfile VIS.ora` En Oracle 19c, la consulta devuelve: `spfile /rdsdbbin /oracle/dbs/spfile VISCDB.ora` 7. Solo en Oracle 19c, compruebe el estado de la base de datos del contenedor y ábralo si es necesario: `SQL> show pdbs`	

Tarea	Descripción	Habilidades requeridas
	<pre>CON_ID CON_NAME OPEN MODE RESTRICTED ---------- --------- ---------- --------- - 2 PDB$SEED READ ONLY NO 3 VIS MOUNTED NO SQL> alter session set container=VIS; Session altered. SQL> alter database open; Database altered. SQL> alter database save state; Database altered. SQL> show pdbs CON_ID CON_NAME OPEN MODE RESTRICTED ---------- --------- ---------- ---------- ----- 3 VIS READ WRITE NO SQL> exit</pre> 8. Elimine el archivo `init.ora` de `$ORACLE_HOME/dbs`, ya que no está usando el PFILE:	

Tarea	Descripción	Habilidades requeridas
	`$ cd $ORACLE_HOME/dbs` En Oracle 12.1.0.2, ejecute el comando: `$ pwd` `/rdsdbbin/oracle/dbs` `$ rm initVIS.ora` En Oracle 19c, ejecute el comando: `$ pwd` `/rdsdbbin/oracle/dbs` `$ rm initVISCDB.ora`	

Recupere contraseñas de Secrets Manager, cree usuarios y cambie contraseñas

Tarea	Descripción	Habilidades requeridas
Recupere contraseñas de Secrets Manager.	Puede llevar a cabo estos pasos en la consola o mediante la CLI de AWS. Los siguientes pasos proporcionan las instrucciones para hacerlo en la consola. 1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	2. En el panel de navegación, seleccione Bases de datos y, luego, la base de datos RDS. 3. Seleccione Configuración y anote el ID de recurso de la instancia (tendrá el formato: `db-WZ4WLCK6AOQ6TJG ZKMGRCDCI3Y`). 4. Abra la consola de Secrets Manager de AWS en https://console.aws.amazon.com/secretsmanager/. 5. Seleccione el secreto que tenga el mismo nombre que `do-not-delete-cust om-<resource_id>` . `resource-id` es la ID de instancia que anotó en el paso 3. 6. Seleccionar Retrieve secret value (Recuperar valor secreto).	

Tarea	Descripción	Habilidades requeridas
Cree el usuario RDSADMIN.	`RDSADMIN` es un usuario de base de datos de supervisión y orquestación en la instancia de base de datos de Amazon RDS Custom. Ya que la base de datos inicial se ha eliminado y la base de datos de destino se ha restaurado desde el origen mediante RMAN, deberá volver a crear este usuario tras la operación de restauración para asegurarse de que la supervisión de Amazon RDS Custom funciona según lo previsto. También deberá crear un perfil y un espacio de tabla independientes para el usuario `RDSADMIN`. Las instrucciones son ligeramente diferentes para Oracle 12.1.0.2 y 19c. Para Oracle 12.1.0.2: 1. En la pregunta de SQL, escriba los comandos siguientes: `SQL> set echo on feedback on serverout on SQL> @?/rdbms/admin/utlpwdmg.sql`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	SQL> ALTER PROFILE DEFAULT LIMIT FAILED_LOGIN_ATTEMPTS UNLIMITED PASSWORD_LIFE_TIME UNLIMITED PASSWORD_VERIFY_F UNCTION NULL; 2. Cree el perfil RDSADMIN: SQL> create profile RDSADMIN LIMIT COMPOSITE_LIMIT UNLIMITED SESSIONS_PER_USER UNLIMITED CPU_PER_SESSION UNLIMITED CPU_PER_CALL UNLIMITED LOGICAL_READS_PER _SESSION UNLIMITED LOGICAL_READS_PER_CALL UNLIMITED IDLE_TIME UNLIMITED CONNECT_TIME UNLIMITED PRIVATE_SGA UNLIMITED FAILED_LOGIN_ATTEMPTS 10 PASSWORD_LIFE_TIME UNLIMITED PASSWORD_REUSE_TIME UNLIMITED PASSWORD_REUSE_MAX UNLIMITED PASSWORD_VERIFY_F UNCTION NULL PASSWORD_LOCK_TIME 86400/86400	

Tarea	Descripción	Habilidades requeridas
	`PASSWORD_GRACE_TIME 604800/86400;` 3. Configure los perfiles de usuario `SYS`, `SYSTEM` y `DBSNMP` como `RDSADMIN`: `SQL> set echo on feedback on serverout on` `SQL> alter user SYS profile RDSADMIN;` `SQL> alter user SYSTEM profile RDSADMIN;` `SQL> alter user DBSNMP profile RDSADMIN;` 4. Cree el espacio de tabla `RDSADMIN`: `SQL> create bigfile tablespace rdsadmin datafile size 7M autoextend on next 1m Logging online permanent blocksize 8192 extent management local autoallocate default nocompress segment space management auto;` 5. Crear el usuario `RDSADMIN`. Sustituya la contraseña `RDSADMIN` por la contraseña que obtuvo anteriormente de Secrets Manager:	

Tarea	Descripción	Habilidades requeridas
	`SQL> create user rdsadmin identified by xxxxxxxxxx` `Default tablespace rdsadmin` `Temporary tablespace temp` `profile rdsadmin ;` 6. Otorgue privilegios a `RDSADMIN`: `SQL> grant select on sys.v_$instance to rdsadmin;` `SQL> grant select on sys.v_$archived_log to rdsadmin;` `SQL> grant select on sys.v_$database to rdsadmin;` `SQL> grant select on sys.v_$database_incarnation to rdsadmin;` `SQL> grant select on dba_users to rdsadmin;` `SQL> grant alter system to rdsadmin;` `SQL> grant alter database to rdsadmin;` `SQL> grant connect to rdsadmin with admin option;` `SQL> grant resource to rdsadmin with admin option;` `SQL> alter user rdsadmin account unlock identified by xxxxxxxxxxx;`	

Tarea	Descripción	Habilidades requeridas
	`SQL> @?/rdbms/admin/use rlock.sql` `SQL> @?/rdbms/admin/utl rp.sql` Para Oracle 19c: 1. En la pregunta de SQL, escriba los comandos siguientes: `SQL> set echo on feedback on serverout on` `SQL> @?/rdbms/admin/utl pwdmg.sql` `SQL> alter profile default LIMIT FAILED_LOGIN_ATTEMPTS UNLIMITED PASSWORD_LIFE_TIME UNLIMITED PASSWORD_VERIFY_F UNCTION NULL;` 2. Para crear el perfil `RDSADMIN`. Nota: `RDSADMIN` tiene un prefijo `C##` en Oracle 19c. Esto se debe a que el parámetro `common_us er_prefix` de la base de datos está establecido en `C##`. `RDSADMIN` no tiene prefijo en Oracle 12.1.0.2.	

Tarea	Descripción	Habilidades requeridas
	`SQL> create profile C##RDSADMIN LIMIT COMPOSITE_LIMIT UNLIMITED SESSIONS_PER_USER UNLIMITED CPU_PER_SESSION UNLIMITED CPU_PER_CALL UNLIMITED LOGICAL_READS_PER _SESSION UNLIMITED LOGICAL_READS_PER_CALL UNLIMITED IDLE_TIME UNLIMITED CONNECT_TIME UNLIMITED PRIVATE_SGA UNLIMITED FAILED_LOGIN_ATTEMPTS 10 PASSWORD_LIFE_TIME UNLIMITED PASSWORD_REUSE_TIME UNLIMITED PASSWORD_REUSE_MAX UNLIMITED PASSWORD_VERIFY_F UNCTION NULL PASSWORD_LOCK_TIME 86400/86400 PASSWORD_GRACE_TIME 604800/86400;`  3. Configure los perfiles de usuario SYS, SYSTEM y DBSNMP como RDSADMIN:  `SQL> alter user SYS profile C##RDSADMIN; SQL> alter user SYSTEM profile C##RDSADMIN;`	

Tarea	Descripción	Habilidades requeridas
	`SQL> alter user DBSNMP profile C##RDSADMIN;` 4. Cree el espacio de tabla `RDSADMIN`: `SQL> create bigfile tablespace rdsadmin datafile size 7M autoextend on next 1m Logging online permanent blocksize 8192 extent management local autoallocate default nocompress segment space management auto;` 5. Crear el usuario `RDSADMIN`. Sustituya la contraseña `RDSADMIN` por la contraseña que obtuvo anteriormente de Secrets Manager. `SQL> create user C##rdsadmin identified by xxxxxxxxxx profile C##rdsadmin container=all;` 6. Otorgue privilegios a `RDSADMIN`: `SQL> grant select on sys.v_$instance to c##rdsadmin;`	

Tarea	Descripción	Habilidades requeridas
	SQL> grant select on sys.v_$archived_log to c##rdsadmin; SQL> grant select on sys.v_$database to c##rdsadmin; SQL> grant select on sys.v_$database_incarnation to c##rdsadmin; SQL> grant select on dba_users to c##rdsadmin; SQL> grant alter system to C##rdsadmin; SQL> grant alter database to C##rdsadmin; SQL> grant connect to C##rdsadmin with admin option; SQL> grant resource to C##rdsadmin with admin option; SQL> alter user C##rdsadmin account unlock identified by xxxxxxxxxxx; SQL> @?/rdbms/admin/userlock.sql SQL> @?/rdbms/admin/utlrp.sql	

Tarea	Descripción	Habilidades requeridas
Cree el usuario maestro.	Ya que la base de datos inicial se ha eliminado y la base de datos de destino se ha restaurado desde el origen mediante RMAN, deberá volver a crear el usuario principal. En este ejemplo, el usuario principal es `admin`. Para Oracle 12.1.0.2: `SQL> create user admin identified by <password>; SQL> grant dba to admin` Para Oracle 19c: `SQL> alter session set container=VIS;` `Session altered.` `SQL> create user admin identified by <password>;` `User created.` `SQL> grant dba to admin;` `Grant succeeded.`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cambie las contraseñas de los superusuarios.	1. Cambie las contraseñas del sistema usando la contraseña que obtuvo de Secrets Manager. Para Oracle 12.1.0.2: `SQL> alter user sys identified by xxxxxxxxxx; SQL> alter user system identified by xxxxxxxxxx;` Para Oracle 19c: `SQL> alter user sys identified by xxxxxxxxxx container =all; SQL> alter user system identified by xxxxxxxxxx container =all;` 1. Cambiar la contraseña `EBS_SYSTEM` . Para Oracle 12.1.0.2: `SQL> alter user ebs_system identified by xxxxxxxxxx;` Para Oracle 19c:	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	En esta versión, también debe conectarse a la base de datos del contenedor para actualizar allí la contraseña de `EBS_SYSTEM` . `SQL> alter session set container=vis;` `SQL> alter user ebs_system identified by xxxxxxxxxx;` `SQL> exit;` Si no cambia estas contraseñas, Amazon RDS Custom mostrará el mensaje de error: El usuario o las credenciales del usuario que supervisa la base de datos han cambiado.	

Cree directorios para Oracle E-Business Suite, instale ETCC y ejecute Autoconfig

Tarea	Descripción	Habilidades requeridas
Cree los directorios necesarios para Oracle E-Business Suite.	1. En la base de datos Oracle de Amazon RDS Custom, ejecute el siguiente script como usuario principal de Oracle para crear el directorio `9idata` en `$ORACLE_HOME/nls/data/9idata` . Estos directorios son necesarios para Oracle E-Business Suite.	

Tarea	Descripción	Habilidades requeridas
	`perl $ORACLE_HOME/nls/data/old/cr9idata.pl` Ignore el mensaje `ORA_NLS10` , ya que creará el entorno adaptado al contexto en pasos posteriores. 2. Copie el archivo `appsutil.tar` , que creó anteriormente desde el sistema de archivos compartido de Amazon EFS, y descomprímalo en el directorio principal de Oracle en Amazon RDS Custom. Cree el directorio de `appsutil` en el directorio `$ORACLE_HOME` . `$ cd /RMAN/appsutil` `$ cp sourceappsutil.tar $ORACLE_HOME` `$ cd $ORACLE_HOME` `$ tar xvf sourceappsutil.tar appsutil` 3. Copie el archivo `appsutil.zip` que guardó anteriormente en el sistema de archivos compartidos de Amazon EFS. Este es el archivo que creó en el nivel de la aplicación.	

Tarea	Descripción	Habilidades requeridas
	Como usuario `rdsdb` en la instancia de base de datos de Amazon RDS Custom: `$ cp /RMAN/appsutil/appsutil.zip $ORACLE_HOME` `$ cd $ORACLE_HOME` 4. Descomprima el archivo `appsutil.zip` para crear el directorio `appsutil` y los subdirectorios en el directorio principal de Oracle: `$ unzip -o appsutil.zip` La opción `-o` implica que algunos de los archivos se sobreescribirán.	

Tarea	Descripción	Habilidades requeridas
Configure los archivos tsanames.ora y sqlnet.ora.	Debe configurar el archivo `tnsnames.ora` para poder conectarse a la base de datos con la herramienta Autoconfig. En el siguiente ejemplo, puede ver que el archivo `tnsnames.ora` tiene un enlace simbólico, pero está vacío de forma predeterminada. `$ cd $ORACLE_HOME/network/admin` `$ ls -ltr` `-rw-r--r-- 1 rdsdb database 373 Oct 31 2013 shrept.lst` `lrwxrwxrwx 1 rdsdb database 30 Feb 9 17:17 listener.ora -> /rdsdbdata/config/listener.ora` `lrwxrwxrwx 1 rdsdb database 28 Feb 9 17:17 sqlnet.ora -> /rdsdbdata/config/sqlnet.ora` `lrwxrwxrwx 1 rdsdb database 30 Feb 9 17:17 tnsnames.ora -> /rdsdbdata/config/tnsnames.ora` 1. Cree la entrada `tnsnames.ora`. Debido a la forma en que la automatización de Amazon RDS analiza los archivos, deberá asegurarse	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	de que la entrada no contenga espacios en blanco, comentarios ni líneas adicionales. De lo contrario, es posible que tengas problemas al utilizar algunas de las API, como -replica. create-db-instance-read Utilice lo siguiente como ejemplo. 2. Sustituya el puerto, el host y la SID según sus necesidades: `$ vi tnsnames.ora` `VIS=(DESCRIPTION=` `(ADDRESS_LIST=(ADD` `RESS=(PROTOCOL=TCP` `)(PORT=1521)(HOST=` `xx.xx.xx.xx)))(CON` `NECT_DATA=(SID=VIS)` `(SERVER=DEDICATED)))` Nota: el archivo no debe contener líneas adicionales. Si no elimina las líneas, pueden surgir problemas al crear una réplica de lectura en el futuro. Es posible que se produzca un error al crear una réplica de lectura y aparezca el siguiente mensaje de error: La actividad arrojó una excepción : HostManagerException: No se pudo llamar correctam	

Tarea	Descripción	Habilidades requeridas
	ente a RestrictReplication en ningún host. 3. Confirme que se puede acceder a la base de datos: `$ tnsping vis` `OK (0 msec)` 4. Solo en Oracle 19c, actualice el archivo `sqlnet.ora` . De lo contrario , recibirá el error ORA-01017 : invalid username/password; logon denied cuando trate de conectarse a la base de datos. Edite `sqlnet.ora` en `$ORACLE_HOME/network/admin` para que coincida con lo siguiente: `NAMES.DIRECTORY_PATH=(TNSNAMES, ONAMES, HOSTNAME)` `SQLNET.EXPIRE_TIME= 10` `SQLNET.INBOUND_CONNECT_TIMEOUT =60` `SQLNET.ALLOWED_LOGON_VERSION_SERVER=10` `HTTPS_SSL_VERSION=undetermined` 5. Prueba de conectividad: `$ sqlplus apps/****@vis`	

Tarea	Descripción	Habilidades requeridas
Configuración de la base de datos.	Ahora que ha probado la conectividad con la base de datos, puede configurar la base de datos con la utilidad appsutil para crear un entorno adaptado al contexto. Para Oracle 12.1.0.2: 1. Ejecute los comandos siguientes: `$ cd $ORACLE_HOME/appsutil/bin` `$ perl adbldxml.pl appsuser=apps` `Enter Hostname of Database server: oebs-db01` `Enter Port of Database server: 1521` `Enter SID of Database server: VIS` `Enter Database Service Name: VIS` `Enter the value for Display Variable: :1` `The context file has been created at: /rdsdbbin/oracle/appsutil/VIS_oebs-db01.xml` 2. Cree `oraInst.loc` desde el usuario raíz: `$ vi /etc/oraInst.loc` `inventory_loc=/rdsdbbin/oracle.12.1.c`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`ustom.r1.EE.1/oraI nventory inst_group=database`	
	3. Clone el archivo de contexto para establecer el nombre de host lógico con el archivo de contexto que ha creado en el paso anterior. Como usuario `rdsdb`, ejecute: `$ cd $ORACLE_HOME/appsu til/clone/bin` `$ perl adclonectx.pl \` `contextfile=[ORA CLE_HOME]/appsutil/ [current context file] \` `template=[ORACLE _HOME]/appsutil/te mplate/adxdbctx.tmp`	
	`oebs-db01log` es el nombre de host lógico. Por ejemplo: `$ perl adclonectx.pl \` `contextfile=/rdsdbbin/ oracle.12.1.custom.r1 .EE.1/appsutil/VIS _oebs-db01.xml \` `template=/rdsdbbin/ oracle/appsutil/ template/adxdbctx.tmp` `Target System Hostname (virtual or normal) [oebs-db01] : oebs- db01log`	

Tarea	Descripción	Habilidades requeridas
	Target System Base Directory : /rdsdbbin/oracle Target Instance is RAC (y/n) [n] : n Target System Database SID : VIS Oracle OS User [rdsdb] : Oracle OS Group [rdsdb] : database Role separation is supported y/n [n] ? : n Target System utl_file_dir Directory List : /tmp Number of DATA_TOP's on the Target System [1] : Target System DATA_TOP Directory 1 [/rdsdbbin/oracle/data] : /rdsdbdata/db/VIS_A/datafile/ Target System RDBMS ORACLE_HOME Directory [/rdsdbbin/oracle/12.1.0] : /rdsdbbin/oracle Do you want to preserve the Display [:1] (y/n) : y Do you want the target system to have the same port values as	

Tarea	Descripción	Habilidades requeridas
	the source system (y/n) [y] ? : y The new database context file has been created : /rdsdbbin/oracle.12.1.custom.r1.EE.1/appsutil/clone/bin/VIS_oebs-db01log.xml contextfile=/rdsdbbin/oracle.12.1.custom.r1.EE.1/appsutil/clone/bin/VIS_oebs-db01log.xml	
	Para Oracle 19c: 1. Ejecute los comandos siguientes: $ cd $ORACLE_HOME/appsutil/bin $ perl adbldxml.pl appsuser=apps Enter Hostname of Database server: oebs-db01 Enter Port of Database server: 1521 Enter SID of Database server: VIS Enter the database listener name:L_VISCDB_001 Enter the value for Display Variable: :1 The context file has been created at: /rdsdbbin/oracle/appsutil/VIS_oebs-db01.xml	

Tarea	Descripción	Habilidades requeridas
	2. Cree `oraInst.loc` desde el usuario raíz: `$ vi /etc/oraInst.loc` `inventory_loc=/rdsdbbin/oracle/oraInventory` `inst_group=database` 3. Clone el archivo de contexto para establecer el nombre de host lógico con el archivo de contexto que ha creado en el paso anterior. Como usuario `rdsdb`, ejecute: `$ cd $ORACLE_HOME/appsutil/clone/bin` `$ perl adclonectx.pl \` `contextfile=[ORACLE_HOME]/appsutil/[current context file] \` `template=[ORACLE_HOME]/appsutil/template/adxdbctx.tmp` `oebs-db01log` es el nombre de host lógico. Por ejemplo: `$ perl adclonectx.pl \` `contextfile=/rdsdbbin/oracle/appsutil/VIS_oebs-db01.xml \` `template=/rdsdbbin/oracle/appsutil/template/adxdbctx.tmp`	

Tarea	Descripción	Habilidades requeridas
	Target System Hostname (virtual or normal) [oebs-db01] : oebs-db01log Target System Base Directory : /rdsdbbin/oracle Target Instance is RAC (y/n) [n] : n Target System CDB Name : VISCDB Target System PDB Name : VIS Oracle OS User [oracle] : rdsdb Oracle OS Group [dba] : database Role separation is supported y/n [n] ? : n Number of DATA_TOP's on the Target System [2] : Target System DATA_TOP Directory 1 [/d01/oracle/VISCDB] : /rdsdbdata/db/pdb/VISCDB_A Target System DATA_TOP Directory 2 [/d01/oracle/data] : /rdsdbdata/db/pdb/VISCDB_A/datafile Specify value for OSBACKUPDBA group [database] : Specify value for OSDGDBA group [database] : Specify value for OSKMDBA group [database] :	

Tarea	Descripción	Habilidades requeridas
	Specify value for OSRACDBA group [database] : Target System RDBMS ORACLE_HOME Directory [/d01/oracle/19.0.0] : /rdsdbbin/oracle Do you want to preserve the Display [:1] (y/n) : y Do you want the target system to have the same port values as the source system (y/n) [y] ? : y Validating if the source port numbers are available on the target system.. Complete port information available at /rdsdbbin/oracle/appsutil/clone/bin/out/VIS_oebs-db01log/portpool.lst New context path and file name [VIS_oebs-db01log.xml] : /rdsdbbin/oracle/appsutil/VIS_oebs-db01log.xml Do you want to overwrite it (y/n) [n] ? : y Replacing /rdsdbbin/oracle/appsutil/VIS_oebs-db01log.xml file. The new database context file has been created : contextfile=/rdsdbbin/oracle/appsutil/VIS_oebs-db01log.xml	

Tarea	Descripción	Habilidades requeridas
	`Check Clone Context logfile /rdsdbbin/oracle/appsutil/clone/bin/CloneContext_0609141428.log for details.`	

Tarea	Descripción	Habilidades requeridas
Instale ETCC y ejecute Autoconfig.	1. Instale Oracle E-Business Suite Technology Codelevel Checker (ETCC). Descargue el parche 17537119 de My Oracle Support y siga las instrucciones que se indican en `README.txt` . Cree un directorio llamado `etcc` en el directorio `$ORACLE_HOME` , descomprima el parche para crear un script llamado `checkMTpatch.sh` y, a continuación, ejecute el script para comprobar las versiones del parche. 2. Ejecute la utilidad Autoconfig y pase el nuevo archivo de contexto del nombre de host lógico. Para Oracle 12.1.0.2: `cd $ORACLE_HOME/appsutil/bin` `$ ./adconfig.sh contextfile=/rdsdbbin/oracle.12.1.customstom.r1.EE.1/appsutil/clone/bin/VIS_oebs-db01log.xml` Para Oracle 19c:	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Autoconfig espera que el nombre del oyente sea CDBNAME. Por lo tanto, el archivo de configuración del oyente original de la copia de seguridad usará L_<CDBNAME>_001 temporalmente. `$ lsnrctl stop L_VISCDB_001` `$ cp -rp /rdsdbdata/config/listener.ora /rdsdbdata/config/listener.ora_orig` `$ vi /rdsdbdata/config/listener.ora` `:%s/L_VISCDB_001/VISCDB/g` `$ lsnrctl start VISCDB` `$ cd /rdsdbbin/oracle/appsutil` `$ . ./txkSetCfgCDB.env dboraclehome=/rdsdbbin/oracle.19.custom.r1.EE-CDB.1` `Oracle Home being passed: /rdsdbbin/oracle` `$ echo $ORACLE_HOME` `/rdsdbbin/oracle.19.custom.r1.EE-CDB.1` `$ export ORACLE_SID=VISCDB` `$ cd $ORACLE_HOME/appsutil/bin` `$ perl $ORACLE_HOME/appsutil/bin/t`	

Tarea	Descripción	Habilidades requeridas
	`xkPostPDBCreationTasks.pl -dboraclehome=$ORACLE_HOME -outdir=$ORACLE_HOME/appsutil/log -cdbsid=VISCDB -pdbsid=VIS -appsuser=apps -dbport=1521 -servicetype=onpremise` `Enter the APPS Password: <apps password>` `Enter the CDB SYSTEM Password:<password from secrets manager>` Nota: si los directorios de su base de datos han cambiado, siga las instrucciones de la nota de soporte de Oracle 2525754.1.	

Configure las entradas de TNS para Amazon RDS Custom y Oracle E-Business Suite

Tarea	Descripción	Habilidades requeridas
Configure las entradas de TNS para Amazon RDS Custom y Oracle E-Business Suite.	Autoconfig genera los ifiles de TNS en las ubicaciones predeterminadas. En Oracle 12.1.0.2 (sin CDB) y en Oracle19c PDB, la ubicación predeterminada es `$ORACLE_HOME/network/admin/$<CONTEXT_NAME>` . El CDB de Oracle	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	19c usa el valor predeterm inado `$ORACLE_HOME/network/admin/` , tal como define `$TNS_ADMIN` en los archivos de entorno que se generan al ejecutar Autoconfig en los pasos anteriores. En Oracle 12.1.0.2 y 19c CDB no los usará, ya que los archivos `tnsnames.ora` y `listener.ora` generados por Autoconfig no cumplen con los requisitos de Amazon RDS, como no incluir espacios en blanco ni comentarios. En su lugar, usará los archivos genéricos proporcionados con la base de datos de Amazon RDS Custom para garantizar el cumplimiento de las expectativas del sistema y reducir el margen de error. Por ejemplo, Amazon RDS Custom espera el siguiente formato de nomenclatura: `L_<INSTANCE_NAME>_001` En el caso de Oracle 12.1.0.2, sería: `L_VIS_001`	

Tarea	Descripción	Habilidades requeridas
	En el caso de Oracle 19c, sería: `L_VISCDB_001` Este es un ejemplo del archivo `listener.ora` que va a utilizar. Se ha generado al crear la base de datos de Amazon RDS Custom. Aún no ha realizado ningún cambio en este archivo, y lo dejará como predeterminado. Para Oracle 12.1.0.2: `$ cd $ORACLE_HOME/network/admin` `$ cat listener.ora` `ADR_BASE_L_VIS_001=/rdsdbdata/log/` `SID_LIST_L_VIS_001=(SID_LIST =` `(SID_DESC = (SID_NAME = VIS)(GLOBAL_DBNAME = VIS) (ORACLE_HOME = /rdsdbbin/oracle)))` `L_VIS_001=(DESCRIPTION_LIST =` `(DESCRIPTION =` `(ADDRESS = (PROTOCOL = TCP)(PORT = 1521)(HOST = xx.xx.xx.xx))) (DESCRIPTION =` `(ADDRESS = (PROTOCOL = TCP)(PORT = 1521)(HOST = 127.0.0.1))))`	

Tarea	Descripción	Habilidades requeridas
	`SUBSCRIBE_FOR_NODE_DOW N_EVENT_L_VIS_001=OFF` En Oracle 19c: restaure el archivo `listener.ora` original con el nombre de oyente `L_<INSTAN CE_NAME>_001` . `$ cd $ORACLE_HOME/netwo rk/admin` `$ cp -rp /rdsdbdata/ config/listener.ora / rdsdbdata/config/ listener.ora_autoc onfig` `$ cp -rp /rdsdbdat a/config/listener. ora_orig /rdsdbdata/ config/listener.ora` `$ cat listener.ora SUBSCRIBE_FOR_ NODE_DOWN_EVENT_L_ VISCDB_001=OFF ADR_BASE_L_VISCDB_001 =/rdsdbdata/log/ USE_SID_AS_SERVICE_ L_VISCDB_001=ON L_VISCDB_001=(DESCRI PTION_LIST = (DESCRIPT ION = (ADDRESS = (PROTOCOL = TCP)(PORT = 1521)(HOST = xx.xx.xx. xx))) (DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(PORT = 1521)(HOST = 127.0.0.1))))`	

Tarea	Descripción	Habilidades requeridas
	`SID_LIST_L_VISCDB_001= (SID_LIST = (SID_DESC = (SID_NAME = VISCDB)(GLOBAL_DBNAME = VISCDB) (ORACLE_HOME = /rdsdbbin/oracle)))` Inicie el oyente `L_<INSTANCE_NAME>_001` para las operaciones estándar de Amazon RDS: `$ lsnrctl stop` `$ lsnrctl start L_VISCDB_001` Para Oracle 12.1.0.2: Edite el archivo de entorno de Oracle E-Business Suite para cambiar la ruta `$TNS_ADMIN` y usar los ifiles TNS genéricos de Amazon RDS Custom. El archivo de entorno se ha creado al ejecutar Autoconfig anteriormente. Edite la variable `TNS_ADMIN` eliminando el sufijo `<CONTEXT_NAME>` . Nota: debe editar el archivo de entorno únicamente en Oracle 12.1.0.2, ya que el directorio predeterminado de 19c es `$ORACLE_HOME/network/admin` , igual al	

Tarea	Descripción	Habilidades requeridas
	predeterminado de Amazon RDS Custom. Por ejemplo, en Oracle 12.1.0.2, edite el archivo: `$ vi $ORACLE_HOME/VIS_oebs-db01log.env` Cambie la ruta de: `TNS_ADMIN=”/rdsdbbin/oracle/network/admin/VIS_oebs-db01log”` `export TNS_ADMIN` a: `TNS_ADMIN=”/rdsdbbin/oracle/network/admin”` `export TNS_ADMIN` Nota: cada vez que ejecute Autoconfig, deberá repetir este paso para asegurarse de que se usan los ifiles TNS correctos (solo en 12.1.0.2). Para Oracle 19c: 1. Cambie el valor de la variable de contexto del nivel de la base de datos `s_cdb_tnsadmin` a `<ORACLE_HOME>/network/admin` en lugar de `<ORACLE_HOME>/netw`	

Tarea	Descripción	Habilidades requeridas
	ork/admin/<CONTEXT_NAME> . Nota: no actualice la variable de contexto s_db_tnsadmin . Guárdelo como <ORACLE_HOME>/network/admin/<CONTEXT_NAME> . `$ . $ORACLE_HOME/VIS_oebs-db01log.env` `$ vi $CONTEXT_FILE` 2. Guarde los cambios realizados en el valor de s_cdb_tnsadmin . Los valores de s_db_tnsadmin y s_cdb_tnsadmin deberían ser similares a los siguientes, con el nombre de PDB VIS y el nombre lógico del nodo de la base de datos oebs-db01log . `$ grep -i tns_admin $CONTEXT_FILE` `<TNS_ADMIN oa_var="s_db_tnsadmin">/rdsdbbin/oracle/network/admin/VIS_oebs-db01log</TNS_ADMIN>` `<CDB_TNS_ADMIN oa_var="s_cdb_tnsadmin">/rdsdbbin/or`	

Tarea	Descripción	Habilidades requeridas
	acle/network/admin</ CDB_TNS_ADMIN> 3. Ejecute Autoconfig en el nivel de base de datos: $. $ORACLE_HOME/VISCD B_oebs-db01log.env $ export ORACLE_PD B_SID=VIS $ sqlplus "/ as sysdba" @$ORACLE_HOME/apps util/admin/adgrant s.sql APPS $ sqlplus "/ as sysdba" @$ORACLE_HOME/rdbms/ admin/utlrp.sql $. $ORACLE_HOME/VIS_o ebs-db01log.env $ echo $ORACLE_SID VIS $ cd $ORACLE_HOME/appsu til/scripts/$CONTE XT_NAME $ ./adautocfg.sh	

Tarea	Descripción	Habilidades requeridas
Configure el entorno para el usuario rdsdb.	Omita este paso en el caso de Oracle 19c. Para Oracle 12.1.0.2: Ahora que ha completado las entradas de Autoconfig y TNS, debe cargar el archivo de entorno configurándolo en el perfil del usuario `rdsdb`. Actualice `.bash_profile` para llamar al archivo de base de datos `.env` de Oracle E-Business Suite. Debe actualizar el perfil para asegurarse de que el entorno esté cargado. El archivo de entorno se ha creado al ejecutar Autoconfig anteriorm ente. Al ejecutar Autoconfig, se crea el siguiente archivo de entorno de ejemplo: `. /rdsdbbin/oracle/V IS_oebs-db01log.env` Como usuario `rdsdb`: `cd $HOME vi .bash_profile export LD_LIBRARY_PATH= ${ORACLE_HOME}/lib:$ {ORACLE_HOME}/ctx/lib`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`export SHLIB_PATH= ${ORACLE_HOME}/lib export PATH=$PATH: ${ORACLE_HOME}/bin alias sql='rlwrap -c sqlplus / as sysdba' . ${ORACLE_HOME}/VIS _oebs-db01log.env` Nota: en el caso de Oracle 19c, no es necesario cargar el entorno CDB en `.bash_profile` . Esto se debe a que el valor predeterminado `ORACLE_HOME` es la ruta predeterminada `$ORACLE_HOME/network/admin` , igual al directorio raíz predeterminado del usuario `rdsdb` (principal de Oracle).	

Tarea	Descripción	Habilidades requeridas
Configure la aplicación y la base de datos para Amazon RDS Custom.	Complete los dos primeros pasos en Oracle 12.1.0.2 y 19c. Los siguientes pasos difieren según la versión. 1. En el nivel de aplicación, edite `/etc/hosts` y cambie la dirección IP de la base de datos por la dirección IP de Amazon RDS Custom: `xx.xx.xx.xx OEBS-db01 .localdomain OEBS-db01 OEBS-db01log.local domain OEBS-db01log` Al usar nombres de host lógicos, puede reemplazar el nodo de la base de datos con total fluidez. 2. En la instancia de base de datos de Amazon RDS Custom, añada o modifique el grupo de seguridad asignado a la instancia de EC2 de origen para reflejar la instancia de base de datos de Amazon RDS Custom y garantizar que la aplicación pueda acceder al nodo. Para Oracle 12.1.0.2: 3. Ejecute Autoconfig. Como propietario de la aplicació	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	n (por ejemplo, `applmgr`), ejecute: `$ cd $INST_TOP/admin/scripts` `$ ./adautocfg.sh` `AutoConfig completed successfully.` 4. Compruebe las entradas de `fnd_nodes` : `SQL> select node_name from apps.fnd_nodes` `NODE_NAME` `----------` `AUTHENTICATION` `OEBS-APP01LOG` `OEBS-DB01LOG` 5. Confirme que puede iniciar sesión e iniciar la aplicación: `$ ./adstrtal.sh` Para Oracle 19c: 1. Compruebe si la PDB está abierta y ábrala si es necesario: `SQL> show pdbs`	

Tarea	Descripción	Habilidades requeridas
	<pre>CON_ID CON_NAME OPEN MODE RESTRICTED ---------- --------- ---------- ---------- ---------- 2 PDB$SEED READ ONLY NO 3 VIS MOUNTED SQL> alter session set container=vis; SQL> alter database open; SQL> alter database save state;</pre> 2. Prueba de conectividad como `apps`: <pre>SQL> sqlplus apps/**** @vis</pre> 3. Ejecute Autoconfig en el nivel de base de datos: <pre>$. $ORACLE_HOME/VIS_o ebs-db01log.env $ echo $ORACLE_SID VIS $ cd $ORACLE_HOME/appsu til/scripts/$CONTE XT_NAME $ ./adautocfg.sh</pre>	

Tarea	Descripción	Habilidades requeridas
	4. Ejecute Autoconfig en el nivel de aplicación como propietario de la aplicación (por ejemplo, `applmgr`): `$ cd $INST_TOP/admin/scripts` `$ ./adautocfg.sh` `AutoConfig completed successfully.` 5. Compruebe las entradas de `fnd_nodes` : `SQL> select node_name from apps.fnd_nodes` `NODE_NAME` `----------` `AUTHENTICATION` `OEBS-APP01LOG` `OEBS-DB01LOG` 6. Iniciar la aplicación: `$ ./adstrtal.sh`	

Realice los pasos posteriores a la migración

Tarea	Descripción	Habilidades requeridas
Reanude la automatización para confirmar que funciona.	Reanude la automatización ejecutando el siguiente comando en la CLI de AWS: `aws rds modify-db-instance \ --db-instance-identifier vis \ --automation-mode full \` Amazon RDS Custom administra ahora la base de datos. Por ejemplo, si el oyente o la base de datos dejan de funcionar, el agente de Amazon RDS Custom los reiniciará. Para ello, ejecute los siguientes comandos. Ejemplo de detención de oyente: `-bash-4.2$ lsnrctl stop vis` Ejemplo de cierre de base de datos: `SQL> shutdown immediate ;`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Valide el esquema, las conexiones y las tareas de mantenimiento.	Para finalizar la migración debe realizar, como mínimo, las siguientes tareas. • Ejecute `FS_CLONE` para sincronizar el sistema de archivos de parches. • Recopile las estadísticas del esquema. • Asegúrese de que las interfaces y los sistemas externos se puedan conectar a la nueva base de datos de Amazon RDS Custom. • Configure las copias de seguridad y la programación de mantenimiento. • Compruebe que los parches en línea de AD (ADOP) funcionan según lo previsto ordenando una transición para cambiar los sistemas de archivos.	Administrador de base de datos

Solución de problemas

Problema	Solución
Aparece un error ORA-01624 al intentar eliminar los archivos de registro.	Si aparece un error ORA-01624 al intentar eliminar los archivos de registro, siga los siguientes pasos.

Problema	Solución
	Ejecute el siguiente comando y espere hasta que el estado de los archivos de registro que desea eliminar sea `INACTIVE`. Para obtener más información acerca de los códigos de estado en `V$log`, consulte la documentación de Oracle. A continuación, se muestra un ejemplo de comando y su resultado: `SQL> select group#, status from v$log;` `GROUP# STATUS` `---------- ----------------` `1 ACTIVE` `2 CURRENT` `3 UNUSED` `4 UNUSED` `5 UNUSED` `6 UNUSED` `6 rows selected.` En este ejemplo, el archivo de registro 1 es `ACTIVE`, por lo que debe forzar el cambio de un archivo de registro tres veces para asegurarse de que el primer archivo de registro nuevo que agregó anteriormente tenga el estado `CURRENT`: `SQL> alter system switch logfile;` `System altered.` `SQL> alter system switch logfile;` `System altered.` `SQL> alter system switch logfile;` `System altered.` Espere a que todos los archivos de registro que desea eliminar tengan el estado `INACTIVE`,

Problema	Solución
	como en el ejemplo siguiente, y ejecute el comando `DROP LOGFILE`. `SQL> select group#, status from v$log;` `GROUP# STATUS` `---------- ----------------` `1 INACTIVE` `2 INACTIVE` `3 INACTIVE` `4 CURRENT` `5 UNUSED` `6 UNUSED` `6 rows selected.`
Aparece un error ORA-00392 al abrir la base de datos con `resetlogs` .	Si recibe el error ORA-00392: log xx of thread 1 is being cleared, operation not allowed, ejecute el siguiente comando (sustituya `xx` por el número de archivo de registro) y ejecute de nuevo el comando abierto `resetlogs` : `SQL> alter database clear logfile group xx;` `SQL> alter database open resetlogs;`

Problema	Solución
Tiene problemas para conectarse a la aplicación mediante Sysadmin o el usuario de la aplicación.	Para confirmar el problema, ejecute la siguiente consulta SQL: `SQL> select dbms_java.get_jdk_ version() from dual; select dbms_java.get_jdk_version() from dual ERROR at line 1: ORA-29548: Java system class reported: release of Java system classes in the database (19.0.0.0.220719 1.8) does not match that of the oracle executabl e (19.0.0.0.0 1.8)` Causa principal: la base de datos de origen se aplicó con múltiples parches, pero el `DB_HOME` de Amazon RDS Custom es una instalación nueva, o bien el CEV no incluyó todos los parches porque no usó los parches de RSU necesarios, como OJVM, al crear el CEV. Para validar este aspecto, compruebe si aparecen los detalles del parche de origen en `$ORACLE_HOME/sqlpath` , `$ORACLE_HOME/.patch_storage` y `opatch -lsinventory` . Referencia: datapatch -verbose Fails with Error :" Patch xxxxxx: Archived Patch Directory Is Empty" (Doc ID 2235541.1) Solución: copie los archivos relacionados con el parche que faltan en la fuente (`$ORACLE_HOME/sqlpatch/`) a Amazon RDS Custom (`$ORACLE_HOME/sqlpatch/`) y, a continuación, vuelva a ejecutar `./datapatch -verbose`.

Problema	Solución
	Por ejemplo: `-bash-4.2$ cp -rp 18793246 20204035 20887355 22098146 22731026 $ORACLE_HOME/sqlpatch/` Como solución alternativa, puede ejecutar el siguiente comando en CDB y PDB: `@?/javavm/install/update_javavm_db.sql` A continuación, ejecute el siguiente comando en PDB: `sql> alter session set container=vis; @?/javavm/install/update_javavm_db.sql` Ejecute de nuevo la prueba: `SQL> select dbms_java.get_jdk_version() from dual;`

Recursos relacionados

- Uso de Amazon RDS Custom (documentación de Amazon RDS)
- Amazon RDS Custom para Oracle: nuevas capacidades de control en el entorno de bases de datos (blog de AWS News)
- Integre Amazon RDS Custom para Oracle con Amazon EFS (blog de AWS Database)
- Migración de Oracle E-Business Suite a AWS (documento técnico de AWS)
- Arquitectura de Oracle E-Business Suite en AWS (documento técnico de AWS)
- Configure una arquitectura HA/DR para Oracle E-Business Suite en Amazon RDS Custom con una base de datos en espera activa (Recomendaciones de AWS)

Información adicional

Operaciones de mantenimiento

Parchear la base de datos de Oracle E-Business Suite con nuevos parches

Como el volumen bin (`/rdsdbbin`) es una out-of-place actualización, su contenido se elimina durante la actualización del CEV. Por lo tanto, debe crear una copia del directorio `appsutil` antes de realizar cualquier actualización mediante CEV.

En la instancia de Amazon RDS Custom de origen, antes de actualizar el CEV, realice una copia de seguridad de `$ORACLE_HOME/appsutil`.

Nota: en este ejemplo se usa un volumen NFS. Sin embargo, puede usar una copia de Amazon Simple Storage Service (Amazon S3) en su lugar.

1. Cree un directorio para almacenar appsutil en la instancia de Amazon RDS Custom de origen:

```
$ mkdir /RMAN/appsutil.preupgrade
```

2. Cree un tar y copie en el volumen de Amazon EFS:

```
$ tar cvf /RMAN/appsutil.preupgrade appsutil
```

3. Compruebe que el archivo tar existe:

```
$ bash-4.2$ ls -l /RMAN/appsutil.preupgrade
-rw-rw-r-- 1 rdsdb rdsdb 622981120 Feb  8 20:16 appsutil.tar
```

4. Actualice al CEV más reciente (ya se ha creado el CEV como requisito previo) siguiendo las instrucciones indicadas en la sección Actualizar una instancia de base de datos de RDS Custom de la documentación de Amazon RDS.

También puede aplicar los parches directamente mediante OPATCH. Consulte la sección Requisitos y consideraciones de actualizaciones de RDS Custom para Oracle de la documentación de Amazon RDS.

Nota: la dirección IP de la máquina host no cambia durante el proceso de aplicación de parches de CEV. Este proceso realiza una out-of-place actualización y, durante el inicio, se adjunta un nuevo volumen bin a la misma instancia.

Migre Oracle PeopleSoft a Amazon RDS Custom

Creado por Gaurav Gupta (AWS)

Entorno: producción	Origen: Amazon EC2	Destino: Amazon RDS Custom
Tipo R: redefinir la plataforma	Carga de trabajo: Oracle	Tecnologías: migración; infraestructura; bases de datos
Servicios de AWS: Amazon RDS; Amazon S3; AWS Secrets Manager; Amazon EFS		

Resumen

Oracle PeopleSoft es una solución de planificación de recursos empresariales (ERP) para procesos de toda la empresa. PeopleSoft tiene una arquitectura de tres niveles: cliente, aplicación y base de datos. PeopleSoft se puede ejecutar en Amazon Relational Database Service (Amazon RDS). Ahora, también puede ejecutar PeopleSoft en Amazon RDS Custom, que proporciona acceso al sistema operativo subyacente.

Amazon RDS Custom para Oracle es un servicio de base de datos administrado para aplicaciones heredadas, personalizadas y empaquetadas que requieren acceso al sistema operativo y al entorno de base de datos subyacentes. Al migrar la base de datos de Oracle a Amazon RDS Custom, Amazon Web Services (AWS) puede gestionar las tareas de backup y la alta disponibilidad, al tiempo que usted puede centrarse en el mantenimiento de la PeopleSoft aplicación y la funcionalidad. Para conocer los factores clave que se deben tener en cuenta para una migración, consulte las estrategias de migración de bases de datos de Oracle en Recomendaciones de AWS.

Este patrón se centra en los pasos para migrar una PeopleSoft base de datos de Amazon Elastic Compute Cloud (Amazon EC2) a Amazon RDS Custom mediante una copia de seguridad de Oracle Recovery Manager (RMAN). Utiliza un sistema de archivos compartido Amazon Elastic File System (Amazon EFS) entre la instancia EC2 y Amazon RDS Custom, aunque también puede utilizar

Amazon FSx o cualquier unidad compartida. El patrón utiliza una copia de seguridad completa en RMAN (a veces denominada copia de seguridad de nivel 0).

Requisitos previos y limitaciones

Requisitos previos

- Base de datos de origen Oracle versión 19C que se ejecuta en Amazon EC2 con Oracle Linux 7, Oracle Linux 8, Red Hat Enterprise Linux (RHEL) 7 o RHEL 8. En los ejemplos de este patrón, el nombre de la base de datos de origen es `FSDM092`, pero no es obligatorio.

  Nota: También puede utilizar este patrón con las bases de datos fuente de Oracle en las instalaciones. Debe tener la conectividad de red adecuada entre la red en las instalaciones y una nube privada virtual (VPC).
- Una instancia de demostración de PeopleSoft 9.2.
- Un único nivel PeopleSoft de aplicación. Sin embargo, puede adaptar este patrón para que funcione con varios niveles de aplicación.
- Amazon RDS Custom está configurado con al menos 8 GB de espacio de intercambio.

Limitaciones

Este patrón no admite las siguientes configuraciones:

- Establecer el parámetro `ARCHIVE_LAG_TARGET` de la base de datos en un valor fuera del rango de 60 a 7200
- Inhabilitar el modo de registro de la instancia de base de datos (`NOARCHIVELOG`)
- Desactivar el atributo optimizado Amazon Elastic Block Store (Amazon EBS) de la instancia EC2
- Modificar los volúmenes de EBS originales adjuntos a la instancia EC2
- Añadir nuevos volúmenes de EBS o cambiar el tipo de volumen de gp2 a gp3
- Cambiar el formato de extensión del parámetro `LOG_ARCHIVE_FORMAT` (requiere `*.arc`)
- Multiplexar o cambiar la ubicación y el nombre del archivo de control (tiene que ser `/rdsdbdata/db/*DBNAME*/controlfile/control-01.ctl`)

Para obtener información adicional sobre estas y otras configuraciones no compatibles, consulte la documentación de Amazon RDS.

Versiones de producto

Para ver las versiones de Oracle Database y clases de instancia compatibles con Amazon RDS Custom, consulte Requisitos y limitaciones de Amazon RDS Custom para Oracle.

Arquitectura

Pila de tecnología de destino

- Equilibrador de carga de aplicación
- Amazon EFS
- Amazon RDS Custom para Oracle
- AWS Secrets Manager
- Amazon Simple Storage Service (Amazon S3)

Arquitectura de destino

El siguiente diagrama de arquitectura representa un PeopleSoft sistema que se ejecuta en una única zona de disponibilidad en AWS. Se accede al nivel de aplicación a través de un Equilibrador de carga de aplicación. Tanto la aplicación como las bases de datos se encuentran en subredes privadas, y las instancias de base de datos Amazon RDS Custom y Amazon EC2 utilizan un sistema de archivos compartidos Amazon EFS para almacenar y acceder a los archivos de respaldo de RMAN. Amazon S3 se utiliza para crear el motor RDS Oracle personalizado y para almacenar los metadatos de redo logs.

Herramientas

Herramientas

Servicios de AWS

- Amazon RDS Custom para Oracle es un servicio de base de datos administrado para aplicaciones heredadas, personalizadas y empaquetadas que requieren acceso al sistema operativo y al entorno de base de datos subyacentes. Automatiza las tareas de administración de bases de datos, como las copias de seguridad y la alta disponibilidad.
- Amazon Elastic File System (Amazon EFS) le ayuda a crear y a configurar sistemas de archivos compartidos en la nube de AWS. Este patrón emplea un sistema de archivos compartidos de Amazon EFS para almacenar y acceder a los archivos de copia de seguridad de RMAN.

- AWS Secrets Manager le permite reemplazar las credenciales codificadas en el código, incluidas las contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación. En este patrón, se recuperan las contraseñas de usuario de la base de datos de Secrets Manager para crear los usuarios `RDSADMIN` y `ADMIN` y cambiar las contraseñas `sys` y `system`.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Elastic Load Balancing (ELB) distribuye el tráfico entrante de aplicaciones o redes entre varios destinos. Así, por ejemplo, puede distribuir el tráfico a través de instancias de Amazon Elastic Compute Cloud (Amazon EC2), contenedores y direcciones IP de una o varias zonas de disponibilidad. Este patrón utiliza un equilibrador de carga de aplicación.

Otras herramientas

- Oracle Recovery Manager (RMAN) proporciona soporte de copia de seguridad y recuperación para bases de datos Oracle. Este patrón utiliza RMAN para realizar una copia de seguridad activa de la base de datos Oracle de origen en Amazon EC2 que se restaura en Amazon RDS Custom.

Prácticas recomendadas

- Para los parámetros de inicialización de la base de datos, personalice el perfil estándar que proporciona la instancia de base de datos personalizada de Amazon RDS PeopleSoft en lugar de utilizar el archivo spfile de la base de datos de origen de Oracle. El motivo de esto es que los espacios en blanco y los comentarios causan problemas al crear réplicas de lectura en Amazon RDS Custom. Para obtener más información sobre los parámetros de inicialización de la base de datos, consulte la nota de soporte de Oracle 1100831.1 (requiere una cuenta de Oracle Support).
- Amazon RDS Custom utiliza la administración automática de memoria de Oracle de forma predeterminada. Si desea utilizar el núcleo de Hugemem, puede configurar Amazon RDS Custom para que utilice en su lugar la gestión automática de la memoria compartida.
- Mantenga el parámetro `memory_max_target` habilitado de forma predeterminada. El marco lo utiliza en segundo plano para crear réplicas de lectura.
- Habilite la base de datos Oracle Flashback. Esta característica resulta útil para restablecer el modo de espera en escenarios de pruebas de conmutación por error (no de transición).

Epics

Configure la instancia de base de datos y el sistema de archivos

Tarea	Descripción	Habilidades requeridas
Crear la instancia de base de datos.	En la consola de Amazon RDS, cree una instancia de base de datos Amazon RDS Custom for Oracle con un nombre de base de datos denominado FSDMO92 (o el nombre de la base de datos de origen). Para obtener más instrucci ones, consulte Trabajar con Amazon RDS Custom en la documentación de AWS, y la publicación del blog Amazon RDS Custom para Oracle: nuevas capacidades de control en entornos de base de datos. Este paso garantiza que la base de datos tenga el mismo nombre que la base de datos de origen. (Si se deja en blanco, la instancia de EC2 y el nombre de la base de datos se definirán como `ORCL`).	Administrador de base de datos

Realice una copia de seguridad completa de RMAN de la base de datos Amazon EC2 de origen

Tarea	Descripción	Habilidades requeridas
Cree un script de copia de seguridad.	Cree un script de respaldo de RMAN para hacer una	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	copia de seguridad de la base de datos en el sistema de archivos Amazon EFS que montó (`/efs` en el siguiente ejemplo). Puede usar el código de ejemplo o ejecutar uno de sus scripts de RMAN existentes. `#!/bin/bash` `Dt=`date +'%Y%m%d-%H` `%M'` `BACKUP_LOG="rman-${O` `RACLE_SID}-$Dt"` `export TAGDATE=`date +` `%Y%m%d%H%M`;` `LOGPATH=/u01/scripts/l` `ogs` `rman target / >>` ` $LOGPATH/rman-${OR` `ACLE_SID}-$Dt << EOF` `SQL "ALTER SYSTEM SWITCH` ` LOGFILE";` `SQL "ALTER SESSION SET` ` NLS_DATE_FORMAT="D` `D.MM.YYYY HH24:MI:S` `S"";` `RUN` `{` ` ALLOCATE CHANNEL ch11` ` TYPE DISK MAXPIECESIZE` ` 5G;` ` ALLOCATE CHANNEL ch12` ` TYPE DISK MAXPIECESIZE` ` 5G;` ` BACKUP AS COMPRESSED` ` BACKUPSET FULL DATABASE` ` FORMAT '/efs/rma` `n_backup/FSCM/%d_%T_` `%s_%p_FULL' ;`	

Tarea	Descripción	Habilidades requeridas
	<pre> SQL "ALTER SYSTEM ARCHIVE LOG CURRENT"; BACKUP FORMAT '/efs/ rman_backup/FSCM/%d_ %T_%s_%p_ARCHIVE' ARCHIVELOG ALL DELETE ALL INPUT ; BACKUP CURRENT CONTROLFILE FORMAT '/ efs/rman_backup/FSCM/ %d_%T_%s_%p_CONTROL'; } EXIT; EOF</pre>	
Ejecute el script de copia de seguridad.	Para ejecutar el script de respaldo de RMAN, inicie sesión como Oracle Home User y ejecute el script. <pre>$ chmod a+x rman_back up.sh $ ./rman_backup.sh &</pre>	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Compruebe que no haya errores y anote el nombre del archivo de copia de seguridad.	Compruebe si hay errores en el archivo de registro RMAN. Si todo parece correcto, publique la copia de seguridad del archivo de control ejecutando el siguiente comando. `RMAN> list backup of controlfile;` `using target database control file instead of recovery catalog` Anote el nombre del archivo de salida. `List of Backup Sets ==================` `BS Key Type LV Size Device Type Elapsed Time Completion Time ------- ---- -- ---------- --------- -- ------------ ---------- 12 Full 21.58M DISK 00:00:01 13-JUL-22 BP Key: 12 Status: AVAILABLE Compressed: NO Tag: TAG20220713T150155 Piece Name: /efs/rman_backup/FSCM/FSDMO92_20220713_12_1_CONTROL`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`Control File Included: Ckp SCN: 165591599 85898 Ckp time: 13-JUL-22` Utilizará el archivo de control de la copia de seguridad `/efs/rman_backup/FSCM/FSDM092_20220713_12_1_CONTROL` cuando restaure la base de datos en Amazon RDS Custom.	

Apague el nivel de aplicación de origen

Tarea	Descripción	Habilidades requeridas
Cierre la aplicación.	Para cerrar el nivel de la aplicación de origen, utilice la utilidad `psadmin` o la utilidad de línea de comandos `psadmin`. 1. Para cerrar el servidor web, ejecute el siguiente comando. `psadmin -w shutdown -d "webserver domain name"` 2. Para cerrar el servidor de la aplicación, ejecute el siguiente comando.	DBA, administrador PeopleSoft

Tarea	Descripción	Habilidades requeridas
	`psadmin -c shutdown -d "application server domain name"` 3. Para cerrar el programador de procesos, ejecute el siguiente comando. `psadmin -p stop -d "process scheduler domain name"`	

Configure la base de datos Amazon RDS Custom de destino

Tarea	Descripción	Habilidades requeridas
Instale el paquete nfs-utils rpm.	Para instalar el paquete `nfs-utils rpm`, ejecute el comando siguiente. `$ yum install -y nfs-utils`	Administrador de base de datos
Monte el almacenamiento EFS.	Obtenga el comando de montaje de Amazon EFS en la página de la consola de Amazon EFS. Monte el sistema de archivos EFS en la instancia de Amazon RDS mediante un cliente de Network File System (NFS). `sudo mount -t nfs4 -o nfsvers=4.1,rsize=1048576,wsize=1048`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	576,hard,timeo=600 ,retrans=2,noresvp ort fs-xxxxxxxxxx.efs. eu-west-1.amazonaw s.com:/ /efs sudo mount -t nfs4 -o nfsvers=4.1,rsize= 1048576,wsize=1048 576,hard,timeo=600 ,retrans=2,noresvp ort fs-xxxxxxxxxx.efs. eu-west-1.amazonaw s.com:/ /efs	

Elimine la base de datos inicial y cree los directorios para almacenar los archivos de la base de datos

Tarea	Descripción	Habilidades requeridas
Pause el modo de automatización.	Debe pausar el modo de automatización en su instancia de base de datos de Amazon RDS Custom antes de continuar con los siguientes pasos, para asegurarse de que la automatización no interfiera con la actividad de restauración de RMAN. Puede pausar la automatización mediante la consola de AWS o el comando Interfaz de la línea de comandos de AWS (AWS CLI) (asegúrese de haber configurado AWS CLI primero).	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`aws rds modify-db-instance \ --db-instance-id entifier peoplesoft-fscm-92 \ --automation-mode all-paused \ --resume-full-au tomation-mode-minute 360 \ --region eu-west-1` Cuando especifique la duración de la pausa, asegúrese de dejar tiempo suficiente para la restauración de RMAN. Este tiempo dependerá del tamaño de la base de datos de origen, por lo que deberá modificar el valor 360 en consecuencia. Además, asegúrese de que el tiempo total de la automatización pausada no se superponga con la ventana de copia de seguridad o mantenimiento de la base de datos.	

Tarea	Descripción	Habilidades requeridas
Cree y modifique el archivo de parámetros para PeopleSoft	Para crear y modificar el perfil PeopleSoft, utilice el perfil estándar creado con la instancia de base de datos personalizada de Amazon RDS. Añada los parámetros que necesite. PeopleSoft 1. Cambie a `rds user rdsdb` ejecutando el siguiente comando. `$ sudo su - rdsdb` 2. Inicie sesión en SQL*Plus en la base de datos inicial y cree el pfile ejecutando el siguiente comando. `SQL> create pfile from spfile;` Esto crea el archivo en `$ORACLE_HOME/dbs` . 3. Haga una copia de seguridad de este perfil. 4. Edite el perfil para añadir o actualizar PeopleSoft los parámetros. `*._gby_hash_aggregation_enabled=false` `*._unnest_subquery=false`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`*.nls_language='AMERICAN'` `*.nls_length_semantics='CHAR'` `*.nls_territory='AMERICA'` `*.open_cursors=1000` `*.db_files=1200` `*.undo_tablespace='UNDOTBS1'` PeopleSoft Los parámetros relacionados se encuentran en la nota de soporte de Oracle 1100831.1. 5. Elimine la referencia al spfile del perfil. `*.spfile='/rdsdbbin/oracle/dbs/spfileFSDM092.ora'`	

Tarea	Descripción	Habilidades requeridas
Elimine la base de datos inicial.	Para eliminar la base de datos Amazon RDS Custom existente, utilice el siguiente código. `$ sqlplus / as sysdba` `SQL> shutdown immediate ;` `SQL> startup mount exclusive restrict;` `SQL> drop database;` `SQL> exit`	

Tarea	Descripción	Habilidades requeridas
Restaure la base de datos Amazon RDS Custom a partir de la copia de seguridad.	Restaure la base de datos mediante el siguiente script. El script restaurará primero el archivo de control y, a continuación, restaurará toda la base de datos a partir de las piezas de respaldo almacenadas en el soporte EFS. `#!/bin/bash` `Dt=`date +'%Y%m%d-%H%M'`` `BACKUP_LOG="rman-${ORACLE_SID}-$Dt"` `export TAGDATE=`date +%Y%m%d%H%M`;` `LOGPATH=/rdsdbdata/scripts/logs` `rman target / >> $LOGPATH/rman-${ORACLE_SID}-$Dt << EOF` `restore controlfile from "/efs/rman_backup/FSCM/FSDMO92_20220713_12_1_CONTROL";` `alter database mount;` `run` `{` `set newname for database to '/rdsdbdata/db/FSDMO92_A/datafile/%f_%b';` `SET NEWNAME FOR TEMPFILE 1 TO '/rdsdbdata/db/FSDMO92_A/datafile/%f_%b';` `RESTORE DATABASE;` `SWITCH DATAFILE ALL;` `SWITCH TEMPFILE ALL;`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	RECOVER DATABASE; } EOF sqlplus / as sysdba >> $LOGPATH/rman-${OR ACLE_SID}-$Dt<<-EOF ALTER DATABASE RENAME FILE '/u01/psoft/db/ oradata/FSDMO92/redo0 1.log' TO '/rdsdbda ta/db/FSDMO92_A/on linelog/redo01.log'; ALTER DATABASE RENAME FILE '/u01/psoft/db/ oradata/FSDMO92/redo0 2.log' TO '/rdsdbda ta/db/FSDMO92_A/on linelog/redo02.log'; ALTER DATABASE RENAME FILE '/u01/psoft/db/ oradata/FSDMO92/redo0 3.log' TO '/rdsdbda ta/db/FSDMO92_A/on linelog/redo03.log'; alter database clear unarchived logfile group 1; alter database clear unarchived logfile group 2; alter database clear unarchived logfile group 3; alter database open resetlogs; EXIT EOF	

Recupere contraseñas de Secrets Manager, cree usuarios y cambie contraseñas

Tarea	Descripción	Habilidades requeridas
Recupere la contraseña de Secrets Manager.	Puede ejecutar este paso mediante la consola de AWS o la AWS CLI. Los siguientes pasos muestran instrucciones para la consola. 1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon RDS. 2. En el panel de navegación, elija Bases de datos y, luego, la base de datos Amazon RDS. 3. Seleccione la pestaña Configuración y anote el ID del recurso de la instancia. Tendrá el formato `db-<ID>` (por ejemplo, `db-73GJNHLGDNZNDOXNWXSECUW6LE`). 4. Abra la consola de Secrets Manager. 5. Elija el secreto que tenga el mismo nombre que `do-not-delete-custom-<resource_id>` , donde `resource-id` se refiere al Identificador de recurso que anotó en el paso 3.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	6. Seleccione Retrieve secret value (Recuperar valor secreto). Esta contraseña será la misma para los usuarios `sys`, `system`, `rdsadmin` y `admin`.	

Tarea	Descripción	Habilidades requeridas
Cree el usuario RDSADMIN.	`RDSADMIN` es el usuario de la base de datos para monitorear y orquestar la instancia de base de datos de Amazon RDS Custom. Ya que la base de datos inicial se ha eliminado y la base de datos de destino se ha restaurado desde el origen mediante RMAN, deberá volver a crear este usuario tras la operación de restauración para asegurarse de que la supervisión de Amazon RDS Custom funciona según lo previsto. También debe crear un perfil y un espacio de tabla independientes para el usuario de `RDSADMIN`. 1. Ingrese los siguientes comandos en la pregunta de SQL. `SQL> set echo on` `feedback on serverout` `on` `SQL> @?/rdbms/admin/` `utlpwdmg.sql` `SQL> ALTER PROFILE` `DEFAULT` `LIMIT` `FAILED_LOGIN_` `ATTEMPTS UNLIMITED` `PASSWORD_LIFE_TIME` `UNLIMITED`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	PASSWORD_VERIFY_F UNCTION NULL; 2. Crear el perfil RDSADMIN. SQL> set echo on feedback on serverout on SQL> alter session set "_oracle_script"=t rue; SQL> CREATE PROFILE RDSADMIN LIMIT COMPOSITE_LIMIT UNLIMITED SESSIONS_PER_USER UNLIMITED CPU_PER_SESSION UNLIMITED CPU_PER_CALL UNLIMITED LOGICAL_READS_PER _SESSION UNLIMITED LOGICAL_READS_PER _CALL UNLIMITED IDLE_TIME UNLIMITED CONNECT_TIME UNLIMITED PRIVATE_SGA UNLIMITED FAILED_LOGIN_ATTE MPTS 10 PASSWORD_LIFE_TIME UNLIMITED PASSWORD_REUSE_TIME UNLIMITED PASSWORD_REUSE_MAX UNLIMITED PASSWORD_VERIFY_F UNCTION NULL	

Tarea	Descripción	Habilidades requeridas
	PASSWORD_LOCK_TIME 86400/86400 PASSWORD_GRACE_TIME 604800/86400; 3. Cree el espacio de tabla RDSADMIN. SQL> CREATE BIGFILE TABLESPACE rdsadmin '/rdsdbdata/db/FSDMO92_A/datafile/rdsadmin.dbf' DATAFILE SIZE 7M AUTOEXTEND ON NEXT 1m LOGGING ONLINE PERMANENT BLOCKSIZE 8192 EXTENT MANAGEMENT LOCAL AUTOALLOCATE DEFAULT NOCOMPRESS SEGMENT SPACE MANAGEMENT AUTO; 4. Crear el usuario RDSADMIN. Sustituya la contraseña RDSADMIN por la contraseña que obtuvo anteriormente de Secrets Manager. SQL> CREATE USER rdsadmin IDENTIFIED BY xxxxxxxxxx DEFAULT TABLESPACE rdsadmin TEMPORARY TABLESPACE TEMP profile rdsadmin ; 5. Otorgue privilegios a RDSADMIN.	

Tarea	Descripción	Habilidades requeridas
	`` SQL> GRANT "CONNECT" TO RDSADMIN WITH ADMIN OPTION; SQL> GRANT "RESOURCE " TO RDSADMIN WITH ADMIN OPTION; SQL> GRANT "DBA" TO RDSADMIN; SQL> GRANT "SELECT_C ATALOG_ROLE" TO RDSADMIN WITH ADMIN OPTION; SQL> GRANT ALTER SYSTEM TO RDSADMIN; SQL> GRANT UNLIMITED TABLESPACE TO RDSADMIN; SQL> GRANT SELECT ANY TABLE TO RDSADMIN; SQL> GRANT ALTER DATABASE TO RDSADMIN; SQL> GRANT ADMINISTER DATABASE TRIGGER TO RDSADMIN; SQL> GRANT ANY OBJECT PRIVILEGE TO RDSADMIN WITH ADMIN OPTION; SQL> GRANT INHERIT ANY PRIVILEGES TO RDSADMIN; SQL> ALTER USER RDSADMIN DEFAULT ROLE ALL; ``` 6. Set the SYS, SYSTEM, and DBSNMP user profiles to RDSADMIN.	

Tarea	Descripción	Habilidades requeridas
	`SQL> set echo on feedback on serverout on` `SQL> alter user SYS profile RDSADMIN;` `SQL> alter user SYSTEM profile RDSADMIN;` `SQL> alter user DBSNMP profile RDSADMIN;`	
Cree el usuario maestro.	Ya que la base de datos inicial se ha eliminado y la base de datos de destino se ha restaurado desde el origen mediante RMAN, deberá volver a crear el usuario principal. En este ejemplo, el nombre del usuario principal es `admin`. `SQL> create user admin identified by <password>;` `SQL> grant dba to admin`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cambiar las contraseñas del sistema.	Cambie las contraseñas del sistema usando la contraseña que obtuvo de Secrets Manager. `SQL> alter user sys identified by xxxxxxxxxx;` `SQL> alter user system identified by xxxxxxxxxx;` Si no cambia estas contraseñas, Amazon RDS Custom mostrará el mensaje de error “El usuario o las credenciales de usuario que supervisa la base de datos han cambiado”.	Administrador de base de datos

Configure las entradas de TNS para Amazon RDS Custom y PeopleSoft

Tarea	Descripción	Habilidades requeridas
Configure el archivo tnsnames.	Para conectarse a la base de datos desde el nivel de aplicación, configure el archivo `tnsnames.ora` de forma que pueda conectarse a la base de datos desde el nivel de aplicación. En el siguiente ejemplo, puede ver que hay un enlace temporal al archivo `tnsnames.ora`, pero el archivo está vacío de forma predeterminada.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`` $ cd /rdsdbbin/oracle/n etwork/admin $ ls -ltr -rw-r--r-- 1 rdsdb database 1536 Feb 14 2018 shrept.lst lrwxrwxrwx 1 rdsdb database 30 Apr 5 13:19 listener.ora - > /rdsdbdata/config/ listener.ora lrwxrwxrwx 1 rdsdb database 28 Apr 5 13:19 sqlnet.ora - > /rdsdbdata/config/ sqlnet.ora lrwxrwxrwx 1 rdsdb database 30 Apr 5 13:19 tnsnames.ora - > /rdsdbdata/config/ tnsnames.ora ``` 1. Cree la entrada `tsnames.ora` . Debido a la forma en que la automatización de Amazon RDS analiza los archivos, deberá asegurarse de que la entrada no contenga espacios en blanco, comentarios ni líneas adicionales. De lo contrario , podría tener problemas al utilizar algunas de las API, como create-db-instance-read -replica.	

Tarea	Descripción	Habilidades requeridas
	2. Sustituya el puerto, el host y el SID de acuerdo con los requisitos de la PeopleSoft base de datos. Utilice el siguiente código como ejemplo. `$ vi tnsnames.ora` `FSDMO92=(DESCRIP TION = (ADDRESS_ LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = x.x.x.x)(PORT = 1521))) (CONNECT_ DATA = (SERVER = DEDICATED) (SID = FSDMO92)))` 3. Para confirmar que se puede acceder a la PeopleSoft base de datos, ejecute el siguiente comando. `$ tnsping FSDMO92` `TNS Ping Utility for Linux: Version 19.0.0.0.0 - Production on 14-JUL-2022 10:16:45` `Copyright (c) 1997, 2021, Oracle. All rights reserved.` `Used parameter files:`	

Tarea	Descripción	Habilidades requeridas
	`/rdsdbbin/oracle/network/admin/sqlnet.ora` `Used TNSNAMES adapter to resolve the alias` `Attempting to contact (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = x.x.x.x)(PORT = 1521))) (CONNECT_DATA = (SERVER = DEDICATED) (SID = FSDMO92)))` `OK (0 msec)`	

Cree el enlace temporal de spfile

Tarea	Descripción	Habilidades requeridas
Cree el enlace temporal de spfile.	1. Para crear spfile en la ubicación `/rdsdbdata/admin/FSDMO92/pfile` , ejecute el siguiente comando. `SQL> create spfile='/rdsdbdata/admin/FSDMO92/pfile/spfileFSDMO92.ora' from pfile;` 2. Navegue hasta `$ORACLE_HOME/dbs` y cree un enlace temporal para spfile.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`ln -s '/rdsdbdata/admin/FSDMO92/pfile/spfileFSDMO92.ora' spfileFSDMO92.ora` 3. Una vez creado este archivo, puede cerrar e iniciar la base de datos mediante el spfile.	

Realice los pasos posteriores a la migración

Tarea	Descripción	Habilidades requeridas
Valide el esquema, las conexiones y las tareas de mantenimiento.	Para finalizar la migración, realice las siguientes tareas. • Recopile las estadísticas del esquema. • Asegúrese de que el nivel de PeopleSoft aplicación se pueda conectar a la nueva base de datos Amazon RDS Custom. • Configure sus programas de respaldo y mantenimiento.	Administrador de base de datos

Recursos relacionados

- Trabajar con Amazon RDS Custom
- Amazon RDS Custom para Oracle: nuevas capacidades de control en el entorno de bases de datos (entrada del blog)
- Integre Amazon RDS Custom para Oracle con Amazon EFS (entrada del blog)

- Configuración de Amazon RDS como una PeopleSoft base de datos de Oracle (documento técnico de AWS)

Migre la funcionalidad ROWIdentificador de Oracle a PostgreSQL en AWS

Creado por Rakesh Raghav (AWS) y Ramesh Pathuri (AWS)

Entorno: PoC o piloto	Origen: base de datos de Oracle	Destino: base de datos PostgreSQL en AWS
Tipo R: redefinir la plataforma	Carga de trabajo: Oracle	Tecnologías: migración; bases de datos
Servicios de AWS: Amazon Aurora; Amazon RDS; AWS SCT; AWS CLI		

Resumen

Este patrón describe las opciones para migrar la funcionalidad de pseudocolumnas `ROWID` de Oracle Database a una base de datos PostgreSQL en Amazon Relational Database Service (Amazon RDS) para PostgreSQL, Amazon Aurora PostgreSQL Compatible Edition o Amazon Elastic Compute Cloud (Amazon EC2).

En una base de datos de Oracle, la pseudocolumna `ROWID` es la dirección física de una fila de una tabla. Esta pseudocolumna se utiliza para identificar de forma exclusiva una fila, incluso si la clave principal no está presente en la tabla. PostgreSQL tiene una pseudocolumna similar llamada `ctid`, pero no se puede usar como `ROWID`. Como se explica en la documentación de PostgreSQL, `ctid` puede cambiar si se actualiza o después de cada proceso `VACUUM`.

Hay tres maneras de crear la funcionalidad de pseudocolumnas `ROWID` en PostgreSQL:

- Utilice una columna de clave principal en lugar de `ROWID` para identificar una fila de una tabla.
- Utilice una clave principal o única lógica (que puede ser una clave compuesta) en la tabla.
- Agregue una columna con valores generados automáticamente y conviértala en una clave principal/única para imitar a `ROWID`.

Este patrón le guía por las tres implementaciones y describe las ventajas y desventajas de cada opción.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Experiencia en codificación en lenguaje procedimental/PostgreSQL (PL/pgSQL)
- Base de datos de origen de Oracle
- Un clúster de Amazon RDS para PostgreSQL o Aurora compatible con PostgreSQL, o una instancia EC2 para alojar la base de datos de PostgreSQL

Limitaciones

- Este patrón proporciona soluciones alternativas para la funcionalidad de `ROWID`. PostgreSQL no proporciona un equivalente a `ROWID` en Oracle Database.

Versiones de producto

- PostgreSQL 11.9 o posterior

Arquitectura

Pila de tecnología de origen

- Base de datos de Oracle

Pila de tecnología de destino

- Aurora compatible con PostgreSQL, Amazon RDS para PostgreSQL o una instancia EC2 con una base de datos PostgreSQL

Opciones de implementación

Existen tres opciones para solucionar la falta de compatibilidad de `ROWID` con PostgreSQL, en función de si la tabla tiene una clave principal o un índice único, una clave principal lógica o un

atributo de identidad. La elección depende de los plazos del proyecto, de la fase de migración actual y de las dependencias del código de la aplicación y de la base de datos.

Opción	Descripción	Ventajas	Desventajas
Clave principal o índice único	Si la tabla de Oracle tiene una clave principal, puede utilizar los atributos de esta clave para identificar de forma exclusiva una fila.	• No depende de las funciones de la base de datos patentada. • El impacto en el rendimiento es mínimo, ya que los campos de clave principal están indexados.	• Requiere cambios en el código de la aplicación y la base de datos en el que se basa en `ROWID` para cambiar a los campos de clave principal.
Clave lógica primaria/ única	Si la tabla de Oracle tiene una clave principal lógica, puede utilizar los atributos de esta clave para identificar de forma exclusiva una fila. Una clave principal lógica consta de un atributo o un conjunto de atributos que pueden identificar de forma única una fila, pero no se aplica a la base de datos mediante una restricción.	• No depende de las funciones de la base de datos patentada.	• Requiere cambios en el código de la aplicación y la base de datos en el que se basa en `ROWID` para cambiar a los campos de clave principal. • Si los atributos de la clave principal lógica no están indexados, se produce un impacto significativo en el rendimiento. No obstante, puede añadir un índice único para evitar problemas de rendimiento.

Atributo de identidad	si la tabla de Oracle no tiene una clave principal, puede crear un campo adicional como `GENERATED ALWAYS AS IDENTITY`. Este atributo genera un valor único cada vez que se insertan datos en la tabla, por lo que se puede utilizar para identificar de forma única una fila para las operaciones del lenguaje de manipulación de datos (DML).	• No depende de las funciones de la base de datos patentada. • La base de datos PostgreSQL rellena el atributo y mantiene su exclusividad.	• Requiere cambios en el código de la aplicación y la base de datos en el que se basa en `ROWID` para cambiar el atributo de identidad. • Si el campo adicional no está indexado, tiene un impacto significativo en el rendimiento. No obstante, puede añadir un índice para evitar problemas de rendimiento.

Herramientas

- Amazon Relational Database Service (Amazon RDS) para PostgreSQL le ayuda a configurar, utilizar y escalar una base de datos relacional de PostgreSQL en la nube de AWS.
- Amazon Aurora compatible con PostgreSQL es un motor de base de datos relacional compatible con ACID y completamente administrado que le permite configurar, administrar y escalar implementaciones de PostgreSQL.
- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos. En este patrón, puede usar la AWS CLI para ejecutar comandos SQL a través de pgAdmin.
- pgAdmin es una herramienta de gestión de código abierto para PostgreSQL. Proporciona una interfaz gráfica que permite crear, mantener y utilizar objetos de bases de datos.
- La Herramienta de conversión de esquemas de AWS (AWS SCT) simplifica las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de

origen y la mayor parte del código personalizado, lo que incluye las vistas, los procedimientos almacenados y las funciones, a un formato compatible con la base de datos de destino.

Epics

Identificar las tablas de origen

Tarea	Descripción	Habilidades requeridas
Identifique las tablas de Oracle que utilizan el `ROWID` atributo.	Utilice la herramienta de conversión de esquemas de AWS (AWS SCT) para identificar las tablas de Oracle que tienen funcionalidad de `ROWID`. Para obtener más información, consulte la documentación de AWS SCT. —o— En Oracle, utilice la vista de `DBA_TAB_COLUMNS` para identificar las tablas que tienen un atributo `ROWID`. Estos campos se pueden utilizar para almacenar caracteres alfanuméricos de 10 bytes. Determine el uso y conviértalos en un campo `VARCHAR`, si procede.	Administrador de base de datos o desarrollador
Identifique el código que hace referencia a estas tablas.	Utilice AWS SCT para generar un informe de evaluación de la migración a fin de identificar los procedimientos afectados por `ROWID`. Para obtener más información, consulte la documentación de AWS SCT.	Administrador de base de datos o desarrollador

Tarea	Descripción	Habilidades requeridas
	—o— En la base de datos Oracle de origen, utilice el campo de texto de la tabla `dba_source` para identificar los objetos que utilizan la funcionalidad de `ROWID`.	

Determine el uso de clave principal

Tarea	Descripción	Habilidades requeridas
Identifica las tablas que no tienen claves principales.	En la base de datos Oracle de origen, utilice `DBA_CONSTRAINTS` para identificar las tablas que no tienen claves principales. Esta información le ayudará a determinar la estrategia de cada tabla. Por ejemplo: `select dt.* from dba_tables dt where not exists (select 1 from all_constraints ct where ct.owner = Dt.owner and ct.table_name = Dt.table_name and ct.constraint_type = 'P' )`	Administrador de base de datos o desarrollador

Tarea	Descripción	Habilidades requeridas
	`and dt.owner = '{schema}'`	

Identifique y aplique la solución

Tarea	Descripción	Habilidades requeridas
Aplique cambios a las tablas que tengan una clave principal lógica o definida.	Realice los cambios en el código de la aplicación y la base de datos que se muestran en la sección Información adicional para utilizar una clave principal única o una clave principal lógica para identificar una fila de la tabla.	Administrador de base de datos o desarrollador
Agregue un campo adicional a las tablas que no tengan una clave principal lógica o definida.	Añada un atributo de tipo `GENERATED ALWAYS AS IDENTITY`. Realice los cambios en el código de la aplicación y la base de datos que se muestran en la sección Información adicional.	Administrador de base de datos o desarrollador
Añada un índice si es necesario.	Agregue un índice al campo adicional o a la clave principal lógica para mejorar el rendimiento de SQL.	Administrador de base de datos o desarrollador

Recursos relacionados

- CTID de PostgreSQL (documentación de PostgreSQL)
- Columnas generadas (documentación de PostgreSQL)

- Pseudocolumna ROWID (documentación de Oracle)

Información adicional

En las siguientes secciones se proporcionan ejemplos de código de Oracle y PostgreSQL para ilustrar los tres enfoques.

Escenario 1: Uso de una clave única principal

En los siguientes ejemplos, se crea la tabla `testrowid_s1` con `emp_id` la clave principal.

Código de Oracle:

```
create table testrowid_s1 (emp_id integer, name varchar2(10), CONSTRAINT testrowid_pk
 PRIMARY KEY (emp_id));
INSERT INTO testrowid_s1(emp_id,name) values (1,'empname1');
INSERT INTO testrowid_s1(emp_id,name) values (2,'empname2');
INSERT INTO testrowid_s1(emp_id,name) values (3,'empname3');
INSERT INTO testrowid_s1(emp_id,name) values (4,'empname4');
commit;

SELECT rowid,emp_id,name FROM testrowid_s1;
ROWID                  EMP_ID NAME
------------------ ---------- ----------
AAAF3pAAAAAAAMOAAA          1 empname1
AAAF3pAAAAAAAMOAAB          2 empname2
AAAF3pAAAAAAAMOAAC          3 empname3
AAAF3pAAAAAAAMOAAD          4 empname4

UPDATE testrowid_s1 SET name = 'Ramesh' WHERE rowid = 'AAAF3pAAAAAAAMOAAB' ;
commit;

SELECT rowid,emp_id,name FROM testrowid_s1;
ROWID                  EMP_ID NAME
------------------ ---------- ----------
AAAF3pAAAAAAAMOAAA          1 empname1
AAAF3pAAAAAAAMOAAB          2 Ramesh
AAAF3pAAAAAAAMOAAC          3 empname3
AAAF3pAAAAAAAMOAAD          4 empname4
```

Código PostgreSQL:

```
CREATE TABLE public.testrowid_s1
```

```
(
    emp_id integer,
    name character varying,
    primary key (emp_id)
);

insert into public.testrowid_s1 (emp_id,name) values
(1,'empname1'),(2,'empname2'),(3,'empname3'),(4,'empname4');

select emp_id,name from testrowid_s1;
 emp_id |   name
--------+----------
      1 | empname1
      2 | empname2
      3 | empname3
      4 | empname4

update testrowid_s1 set name = 'Ramesh' where emp_id = 2 ;

select emp_id,name from testrowid_s1;
 emp_id |   name
--------+----------
      1 | empname1
      3 | empname3
      4 | empname4
      2 | Ramesh
```

Escenario 2: uso de una clave principal lógica

En los ejemplos siguientes, se crea la tabla `testrowid_s2` con `emp_id` la clave principal lógica.

Código de Oracle:

```
create table testrowid_s2 (emp_id integer, name varchar2(10) );
INSERT INTO testrowid_s2(emp_id,name) values (1,'empname1');
INSERT INTO testrowid_s2(emp_id,name) values (2,'empname2');
INSERT INTO testrowid_s2(emp_id,name) values (3,'empname3');
INSERT INTO testrowid_s2(emp_id,name) values (4,'empname4');
commit;

SELECT rowid,emp_id,name FROM testrowid_s2;
ROWID                  EMP_ID NAME
------------------ ---------- ----------
AAAF3rAAAAAAAMeAAA          1 empname1
```

```
AAAF3rAAAAAAAMeAAB          2 empname2
AAAF3rAAAAAAAMeAAC          3 empname3
AAAF3rAAAAAAAMeAAD          4 empname4

UPDATE testrowid_s2 SET name = 'Ramesh' WHERE rowid = 'AAAF3rAAAAAAAMeAAB' ;
commit;

SELECT rowid,emp_id,name FROM testrowid_s2;
ROWID                  EMP_ID NAME
------------------ ---------- ----------
AAAF3rAAAAAAAMeAAA          1 empname1
AAAF3rAAAAAAAMeAAB          2 Ramesh
AAAF3rAAAAAAAMeAAC          3 empname3
AAAF3rAAAAAAAMeAAD          4 empname4
```

Código PostgreSQL:

```
CREATE TABLE public.testrowid_s2
(
    emp_id integer,
    name character varying
);

insert into public.testrowid_s2 (emp_id,name) values
(1,'empname1'),(2,'empname2'),(3,'empname3'),(4,'empname4');

select emp_id,name from testrowid_s2;
 emp_id |   name
--------+----------
      1 | empname1
      2 | empname2
      3 | empname3
      4 | empname4

update testrowid_s2 set name = 'Ramesh' where emp_id = 2 ;

select emp_id,name from testrowid_s2;
 emp_id |   name
--------+----------
      1 | empname1
      3 | empname3
      4 | empname4
      2 | Ramesh
```

Escenario 3: Uso de un atributo de identidad

En los ejemplos siguientes, se crea la tabla `testrowid_s3` sin clave principal y mediante un atributo de identidad.

Código de Oracle:

```
create table testrowid_s3 (name varchar2(10));
INSERT INTO testrowid_s3(name) values ('empname1');
INSERT INTO testrowid_s3(name) values ('empname2');
INSERT INTO testrowid_s3(name) values ('empname3');
INSERT INTO testrowid_s3(name) values ('empname4');
commit;

SELECT rowid,name FROM testrowid_s3;
ROWID              NAME
------------------ ----------
AAAF3sAAAAAAAMmAAA empname1
AAAF3sAAAAAAAMmAAB empname2
AAAF3sAAAAAAAMmAAC empname3
AAAF3sAAAAAAAMmAAD empname4

UPDATE testrowid_s3 SET name = 'Ramesh' WHERE rowid = 'AAAF3sAAAAAAAMmAAB' ;
commit;

SELECT rowid,name FROM testrowid_s3;
ROWID              NAME
------------------ ----------
AAAF3sAAAAAAAMmAAA empname1
AAAF3sAAAAAAAMmAAB Ramesh
AAAF3sAAAAAAAMmAAC empname3
AAAF3sAAAAAAAMmAAD empname4
```

Código PostgreSQL:

```
CREATE TABLE public.testrowid_s3
(
    rowid_seq bigint generated always as identity,
    name character varying
);

insert into public.testrowid_s3 (name) values
('empname1'),('empname2'),('empname3'),('empname4');
```

```
select rowid_seq,name from testrowid_s3;
 rowid_seq |   name
-----------+----------
         1 | empname1
         2 | empname2
         3 | empname3
         4 | empname4

update testrowid_s3 set name = 'Ramesh' where rowid_seq = 2 ;

select rowid_seq,name from testrowid_s3;
 rowid_seq |   name
-----------+----------
         1 | empname1
         3 | empname3
         4 | empname4
         2 | Ramesh
```

Migre los códigos de error de Oracle Database a una base de datos Amazon Aurora compatible con PostgreSQL

Creado por Sai Parthasaradhi (AWS) y Veeranjaneyulu Grandhi (AWS)

Entorno: PoC o piloto	Origen: Oracle	Destino: PostgreSQL
Tipo R: redefinir la plataforma	Carga de trabajo: Oracle	Tecnologías: Migración; bases de datos
Servicios de AWS: Amazon Aurora		

Resumen

Este patrón muestra cómo migrar los códigos de error de Oracle Database a una base de datos de Amazon Aurora compatible con PostgreSQL mediante una tabla de metadatos predefinida.

Los códigos de error de Oracle Database no siempre tienen un código de error de PostgreSQL correspondiente. Esta diferencia en los códigos de error puede dificultar la configuración de la lógica de procesamiento de los procedimientos o funciones en la arquitectura PostgreSQL de destino.

Puede simplificar el proceso almacenando los códigos de error de la base de datos de origen y destino significativos para su programa PL/pgSQL en una tabla de metadatos. Configure la tabla para marcar los códigos de error válidos de Oracle Database y asignarlos a sus equivalentes de PostgreSQL antes de continuar con el resto de la lógica del proceso. Si el código de error de Oracle Database no está en la tabla de metadatos, el proceso finaliza con una excepción. Podrá revisar manualmente los detalles del error y añadir el nuevo código de error a la tabla si su programa lo requiere.

Al usar esta configuración, su base de datos Amazon Aurora compatible con PostgreSQL puede gestionar los errores de la misma manera que lo hace su base de datos Oracle de origen.

Nota: la configuración de una base de datos PostgreSQL para gestionar correctamente los códigos de error de Oracle Database suele requerir cambios en el código de la base de datos y de la aplicación.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos Oracle de origen con servicios de instancia y oyente en ejecución
- Un clúster de Amazon Aurora compatible con PostgreSQL en ejecución
- Familiaridad con Oracle Database
- Familiaridad con bases de datos PostgreSQL

Arquitectura

El siguiente diagrama muestra un ejemplo de flujo de trabajo de base de datos Amazon Aurora compatible con PostgreSQL para la validación y gestión de códigos de error de datos:

En el diagrama, se muestra el siguiente flujo de trabajo:

1. La tabla contiene los códigos de error y clasificaciones de Oracle Database, así como los códigos de error y clasificaciones de PostgreSQL equivalentes. La tabla incluye una columna valid_error que clasifica si los códigos de error específicos y predefinidos son válidos o no.
2. Cuando una función PL/pgSQL (func_processdata) arroja una excepción, invoca una segunda función PL/pgSQL (error_validation).
3. La función error_validation acepta el código de error de la base de datos Oracle como argumento de entrada. A continuación, la función compara el código de error entrante con la tabla para comprobar si el error está incluido en la tabla.
4. Si el código de error de la base de datos Oracle está incluido en la tabla, la función error_validation devuelve un valor TRUE y la lógica del proceso continúa. Si el código de error no está incluido en la tabla, la función devuelve un valor FALSE y la lógica del proceso se cierra con una excepción.
5. Cuando la función devuelve un valor FALSE, el responsable funcional de la aplicación revisa manualmente los detalles del error para determinar su validez.
6. A continuación, el nuevo código de error se añade manualmente a la tabla o no. Si el código de error es válido y se añade a la tabla, la función error_validation devolverá un valor TRUE la

próxima vez que se produzca la excepción. Si el código de error no es válido y el proceso debe fallar cuando se produzca la excepción, el código de error no se agregará a la tabla.

Pila de tecnología

- PostgreSQL de Amazon Aurora
- pgAdmin
- Oracle SQL Developer

Herramientas

- La edición de Amazon Aurora compatible con PostgreSQL es un motor de base de datos relacional, compatible con ACID completamente administrado que le permite configurar, administrar y escalar implementaciones de PostgreSQL.
- pgAdmin es una plataforma de administración y desarrollo de código abierto para PostgreSQL. Proporciona una interfaz gráfica que ayuda a crear, mantener y usar objetos de base de datos.
- Oracle SQL Developer es un entorno de desarrollo integrado que simplifica el desarrollo y la administración de bases de datos de Oracle, tanto en implementaciones tradicionales como en implementaciones basadas en la nube.

Epics

Migre los códigos de error de Oracle Database a una base de datos Amazon Aurora compatible con PostgreSQL

Tarea	Descripción	Habilidades requeridas
Cree una tabla en la base de datos de Amazon Aurora compatible con PostgreSQL.	Ejecute el comando de PostgreSQL CREATE TABLE: `( source_error_code numeric NOT NULL,`	Desarrollador de PostgreSQL, Oracle, RDS/Aurora para PostgreSQL

Tarea	Descripción	Habilidades requeridas
	<pre> target_error_code character varying NOT NULL, valid_error character varying(1) NOT NULL);</pre>	

Tarea	Descripción	Habilidades requeridas
Añada los códigos de error de PostgreSQL y sus correspondientes códigos de error de Oracle Database a la tabla.	Ejecute el comando de PostgreSQL INSERT para añadir los valores de código de error necesarios a la tabla error_codes. Los códigos de error de PostgreSQL deben usar un tipo de datos que varíe en caracteres (valor SQLSTATE). Los códigos de error de Oracle deben usar un tipo de datos numéricos (valor SQLCODE). Ejemplo de instrucciones de inserción: `insert into error_codes values (-1817,'22007','Y');` `insert into error_codes values (-1816,'22007','Y');` `insert into error_codes values (-3114,'08006','N');` Nota: si detecta excepciones de conectividad de bases de datos Java (JDBC) específicas de Oracle, debe sustituirlas por excepciones genéricas entre bases de datos o cambiar a excepciones específicas de PostgreSQL.	Desarrollador de PostgreSQL, Oracle, RDS/Aurora para PostgreSQL

Tarea	Descripción	Habilidades requeridas
Cree una función PL/pgSQL para validar los códigos de error.	Cree una función PL/pgSQL ejecutando el comando de PostgreSQL CREATE FUNCTION. Asegúrese de que la función haga lo siguiente: • Aceptar los códigos de error de Oracle generados por un programa. • Comprobar si hay códigos de error en la tabla error_codes. • Devolver un valor TRUE o FALSE, en función de si el código de error está presente en la tabla de metadatos o no.	Desarrollador de PostgreSQL, Oracle, RDS/Aurora para PostgreSQL

Tarea	Descripción	Habilidades requeridas
Revise manualmente los nuevos códigos de error a medida que los registra la función PL/pgSQL.	Revise manualmente los nuevos códigos de error. Si un nuevo código de error es válido para su caso de uso, agréguelo a la tabla error_codes ejecutando el comando de PostgreSQL INSERT. -o bien- Si un código de error nuevo no es válido para su caso de uso, no lo añada a la tabla. La lógica del proceso seguirá fallando y se cerrará con una excepción cuando se produzca el error.	Desarrollador de PostgreSQL, Oracle, RDS/Aurora para PostgreSQL

Recursos relacionados

Apéndice A. Códigos de error de PostgreSQL (documentación de PostgreSQL)

Mensajes de error de base de datos (documentación de Oracle Database)

Migración de las cargas de trabajo de Redis a Redis Enterprise Cloud en AWS

Creado por Antony Prasad Thevaraj (AWS) y Srinivas Pendyala (Redis)

Entorno: producción	Origen: base de datos local (Redis u otra)	Destino: Redis Enterprise Cloud en AWS
Tipo R: redefinir la plataforma	Carga de trabajo: código abierto	Tecnologías: migración; bases de datos
Servicios de AWS: AWS DMS; Amazon S3		

Resumen

Este patrón analiza el proceso de alto nivel para migrar las cargas de trabajo de Redis a Redis Enterprise Cloud en Amazon Web Services (AWS). Describe los pasos de la migración, proporciona información sobre la selección de herramientas disponibles y analiza las ventajas, desventajas y pasos para usar cada herramienta. Si lo desea, si necesita ayuda adicional para migrar cargas de trabajo desde Redis, puede contratar los servicios profesionales de Redis.

Si utiliza Redis OSS o Redis Enterprise Software de forma en las instalaciones, estará familiarizado con los importantes gastos administrativos y la complejidad operativa que supone mantener las bases de datos de Redis en el centro de datos. Al migrar sus cargas de trabajo a la nube, puede reducir considerablemente esta carga operativa y aprovechar Redis Enterprise Cloud, que es una oferta de base de datos como servicio (DBaaS) totalmente alojada de Redis. Esta migración ayuda a aumentar la agilidad empresarial, mejora la fiabilidad de las aplicaciones y reduce los costos generales, al tiempo que obtiene acceso a las funciones más recientes de Redis Enterprise Cloud en AWS, como la disponibilidad del 99,999 %, la simplicidad de la arquitectura y la escalabilidad.

Redis Enterprise Cloud tiene posibles aplicaciones en los sectores de los servicios financieros, el comercio minorista, la sanidad y los juegos, así como en casos de uso que requieren soluciones para la detección del fraude, el inventario en tiempo real, el procesamiento de reclamaciones y la gestión de sesiones. Puede usar Redis Enterprise Cloud para conectarse a sus recursos de AWS, por ejemplo, a un servidor de aplicaciones que se ejecute en instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a un microservicio que se implemente como un servicio AWS Lambda.

Requisitos previos y limitaciones

Supuestos

- Actualmente utiliza un sistema de base de datos en las instalaciones que desea migrar a la nube.
- Ha identificado los requisitos de migración para sus cargas de trabajo, entre los que se incluyen:
  - Requisitos de consistencia de datos
  - Requisitos del entorno de infraestructura y sistema
  - Requisitos de mapeo y transformación de datos
  - Requisitos de pruebas funcionales
  - Requisitos de pruebas de rendimiento
  - Requisitos de validación
  - Estrategia de transición definida
- Ha evaluado los plazos y las estimaciones de costos necesarios para la migración.
- Sus requisitos tienen en cuenta el alcance del trabajo y los sistemas y bases de datos que haya identificado como parte de la migración.
- Ha identificado a las partes interesadas junto con sus funciones y responsabilidades en una matriz responsable, consultada e informada (RACI).
- Ha recibido el acuerdo y las aprobaciones necesarios de todas las partes interesadas.

Costo

En función de las especificaciones técnicas de la base de datos fuente existente (por ejemplo, el tamaño de la memoria, el rendimiento y el tamaño total de los datos), un arquitecto de soluciones de Redis puede dimensionar el sistema de destino en Redis Enterprise Cloud. Para obtener información general sobre los precios, consulte los Precios de Redis en el sitio web de Redis.

Personas y habilidades

El proceso de migración implica las siguientes funciones y responsabilidades.

Rol	Descripción	Habilidades requeridas
Arquitecto de soluciones de migración	Arquitecto técnico con experiencia en la definición,	Comprensión técnica y a nivel de aplicación de los sistemas de origen y destino; experienc

	planificación e implementación de estrategias de migración	ia en la migración de cargas de trabajo a la nube
Arquitecto de datos	Arquitecto técnico con amplia experiencia en la definición, implementación y entrega de soluciones de datos para una amplia variedad de bases de datos	Modelado de datos para datos estructurados y no estructur ados, con amplios conocimie ntos y experiencia en la implementación de bases de datos para una empresa
Arquitecto de soluciones de Redis	Un arquitecto técnico que puede ayudar a diseñar un clúster Redis de tamaño óptimo para el caso de uso adecuado	Experiencia en el diseño e implementación de solucione s de Redis para una amplia variedad de casos de uso
Arquitecto de soluciones en la nube	Un arquitecto técnico con un conocimiento más profundo de las soluciones en la nube, especialmente en AWS	Experiencia en la creación de soluciones para la nube; experiencia en migración de cargas de trabajo y moderniza ción de aplicaciones
Arquitecto empresarial	Un arquitecto técnico que tenga un conocimiento completo del panorama técnico de su organizac ión, que tenga una visión compartida de la hoja de ruta del futuro y que practique y establezca las prácticas recomendadas de arquitectura estandarizadas en todos los equipos de su organización	Certificaciones de arquitectura de software, como el TOGAF, conocimientos básicos de ingeniería de software y experiencia en arquitectura de soluciones y arquitectura empresarial

Informática o DevOps ingeniero	Un ingeniero responsable de crear y mantener la infraestructura, incluida la supervisión de la infraestructura para detectar problemas, realizar tareas de mantenimiento y realizar las actualizaciones necesarias.	Amplio conocimiento de diversas tecnologías, incluidos los sistemas operativos, las redes y la computación en la nube; familiaridad con lenguajes de programación como Python, Bash y Ruby, así como con herramientas como Docker, Kubernetes y Ansible

Arquitectura

Opciones de migración

En el siguiente diagrama, se muestran las opciones para migrar los orígenes de datos en las instalaciones (basadas en Redis u otras) a AWS. Muestra varias herramientas de migración entre las que puede elegir, como la exportación de archivos de Redis Database (RDB) a Amazon Simple Storage Service (Amazon S3), el uso de la característica de replicación de Redis o el uso de AWS DMS.

1. Orígenes de datos en las instalaciones: bases de datos que no están basadas en Redis, como MySQL, PostgreSQL, Oracle, SQL Server o MariaDB.
2. Orígenes de datos en las instalaciones: bases de datos basadas en el protocolo de Redis, como Redis OSS y Redis Enterprise Software.
3. La forma más sencilla de migrar datos de bases de datos basadas en Redis es exportar archivos RDB e importarlos a la nube empresarial de Redis de destino en AWS.
4. Como alternativa, puede migrar los datos del origen al destino mediante la función de replicación (`ReplicaOf`) de Redis.
5. Si sus requisitos de migración de datos incluyen la transformación de los datos, puede utilizar las herramientas de entrada y salida de Redis (RIOT) para migrar los datos.
6. Como alternativa, puede utilizar AWS Data Migration Service (AWS DMS) para migrar los datos desde bases de datos basadas en SQL.

7. Debe utilizar la interconexión de nube privada virtual (VPC) para AWS DMS a fin de migrar los datos correctamente a la nube empresarial de Redis de destino en AWS.

Arquitectura de destino

El siguiente diagrama muestra una arquitectura de implementación típica de Redis Enterprise Cloud en AWS e ilustra cómo se puede usar con los principales servicios de AWS.

1. Puede conectarse a las aplicaciones empresariales respaldadas por Redis Enterprise Cloud en AWS.
2. Puede ejecutar aplicaciones empresariales en su propia cuenta de AWS, en una VPC dentro de esa cuenta.
3. Puede utilizar los puntos de conexión de la base de datos de Redis Enterprise Cloud para conectarse a sus aplicaciones. Algunos ejemplos incluyen un servidor de aplicaciones que se ejecuta en instancias de EC2, un microservicio implementado como un servicio de AWS Lambda, una aplicación de Amazon Elastic Container Service (Amazon ECS) o una aplicación Amazon Elastic Kubernetes Service (Amazon EKS).
4. Las aplicaciones empresariales que se ejecutan en su VPC requieren una conexión de emparejamiento de VPC a la VPC de Redis Enterprise Cloud. Esto permite que las aplicaciones empresariales se conecten de forma segura a través de puntos de conexión privados.
5. Redis Enterprise Cloud en AWS es una plataforma de base de datos NoSQL en memoria que se implementa como DBaaS en AWS y está totalmente gestionada por Redis.
6. Redis Enterprise Cloud se implementa dentro de una VPC en una cuenta de AWS estándar creada por Redis.
7. Por motivos de seguridad, Redis Enterprise Cloud se implementa en una subred privada a la que se puede acceder desde puntos de conexión públicos y privados. Le recomendamos que conecte las aplicaciones de cliente a Redis en puntos de conexión privados. Si planea utilizar un punto de conexión público, le recomendamos encarecidamente que habilite TLS para cifrar los datos entre sus aplicaciones cliente y Redis Enterprise Cloud.

La metodología de migración de Redis se alinea con la metodología de migración de AWS, que se ilustra en Movilice su organización para acelerar las migraciones a gran escala en el sitio web AWS Prescriptive Guidance.

Automatizar y escalar

Las tareas de configuración del entorno para la migración se pueden automatizar mediante AWS Landing Zone y plantillas de infraestructura como código (IaC) para la automatización y la escalabilidad. Estas cuestiones se analizan en la sección Epics de este patrón.

Herramientas

En función de sus requisitos de migración de datos, puede elegir entre una selección de opciones tecnológicas para migrar sus datos a Redis Enterprise Cloud en AWS. En la tabla siguiente se describen estos parámetros.

Herramienta	Descripción	Ventajas	Desventajas
Exportación e importación de RDB	Los datos de la base de datos de origen (por ejemplo, Redis OSS o Redis Enterprise Software) se exportan en forma de archivos RDB. Si la base de datos se proporciona a través de un clúster de OSS de Redis, exporta cada partición maestro a una RDB. A continuación, importe todos los archivos RDB en un solo paso. Si la base de datos de origen se basa en un clúster de OSS, pero la base de datos de destino no utiliza la API de clúster de OSS, debe	• Sencillo. • Funciona con cualquier solución basada en Redis que pueda exportar datos en formato RDB como fuente (incluido s Redis OSS y Redis Enterprise Software). • Logra la coherenci a de datos con un proceso sencillo.	• No responde a los requisitos de transformación de datos ni admite las fusiones lógicas de bases de datos. • Consume mucho tiempo para conjuntos de datos más grandes. • La falta de soporte para la migración delta puede provocar un tiempo de inactividad más prolongado.

	cambiar el código fuente de la aplicación para utilizar una biblioteca cliente de Redis estándar.
	Los requisitos de transformación de datos o las fusiones de bases de datos lógicas requieren un proceso más complejo, que se explica en Fusión lógica de bases de datos más adelante en esta tabla.

Función de replicación de Redis (activa-pasiva)	Puede replicar continuamente los datos de una base de datos de Redis OSS, Enterprise Software o Enterprise Cloud a una base de datos de Redis Enterprise Cloud. Tras la sincronización inicial, la función de replicación de Redis (`ReplicaOf `) realiza una migración delta, lo que significa que prácticamente no se observa ningún tiempo de inactividad de las aplicaciones. La característica de replicación de Redis está diseñada para usarse de forma activa y pasiva. Se supone que el objetivo es pasivo y se vuelve a sincronizar por completo (se vacía y sincroniza desde la base de datos de origen). Por lo tanto, cambiar entre el origen y el destino es algo más complicado.	• Admite la replicación continua (carga de datos inicial seguida de deltas). • Prácticamente no hay tiempo de inactividad (depende del retraso de la replicación). • Logra la coherencia de datos.	• Se prevé que solo un sitio esté activo, por lo que cambiar de un sitio a otro es más complicado. • Admite un máximo de 32 particiones maestras al migrar desde un clúster de OSS.

	Es posible replicar desde un clúster de OSS de Redis a una base de datos estándar de Redis Enterprise Cloud agrupada en clústeres especificando todas las particion es maestras del clúster de OSS como fuentes. Sin embargo, la función de replicaci ón de Redis permite un máximo de 32 bases de datos de origen.		
AWS DMS	Puede usar AWS DMS para migrar datos de cualquier base de datos de origen compatible a un almacén de datos de Redis de destino con un tiempo de inactividad mínimo. Para obtener más información, consulte Uso de Redis como objetivo para AWS DMS en la documenta ción de AWS DMS.	• Soporta la migración de orígenes de datos NoSQL y SQL. • Funciona bien con otros servicios de AWS. • Admite casos de uso de la captura de datos de cambio y migración en tiempo real (CDC, change data capture).	• Los valores clave de Redis no pueden contener caracteres especiales como%. • No admite la migración de datos que contengan caracteres especiales en las filas o en los nombres de los campos. • No es compatibl e con el modo de objetos binarios completamente grandes (LOB).

Combinación lógica de bases de datos	Los requisitos especiales de combinación de bases de datos pueden requerir una solución de migración de datos personalizada. Por ejemplo, es posible que tenga cuatro bases de datos lógicas (`SELECT 0..3`) en Redis OSS, pero tal vez desee utilizar un único punto de conexión de base de datos en lugar de mover los datos a varias bases de datos de Redis Enterprise Cloud. Redis Enterprise no admite bases de datos lógicas seleccionables, por lo que tendría que transformar el modelo de datos físicos de la base de datos de origen. Por ejemplo, puede asignar cada índice de base de datos a un prefijo (`0` a `usr`, `1` a `cmp`, etc.) y, a continuación, utilizar un script de migración o una herramienta de extracción, transform	• Control detallado de la configuración de los datos durante la migración al sistema de destino mediante scripts personalizados.	• Si decide no completar la migración, la reversión puede ser muy difícil, especialmente si los datos más recientes deben devolverse a los sistemas de origen. • El costo de creación puede ser elevado si el objetivo es crear una solución única para una migración única. • Los costos de mantenimiento del código, la infraestructura, el tiempo de desarrollo y otras áreas pueden ser altos si los requisitos de migración cambian con frecuencia.

	ación y carga (ETL) para generar un archivo RDB que, a continuación, podrá importar a la base de datos de destino.

Además, puede utilizar las siguientes herramientas y servicios de AWS.

Herramientas de evaluación y descubrimiento:

- AWS Application Discovery Service
- Evaluador de migración

Herramientas de migración de aplicaciones y servidores:

- AWS Application Migration Service

Herramientas de migración de bases de datos:

- Herramienta de conversión de esquemas de AWS (AWS SCT)
- AWS Database Migration Service (AWS DMS)

Herramientas de migración de datos:

- AWS Storage Gateway
- AWS DataSync
- AWS Direct Connect
- AWS Snowball
- Amazon Data Firehose

Gestión de la migración:

- AWS Migration Hub

Soluciones de socios de AWS:

- Socios con competencias en migración de AWS

Epics

Complete las tareas de descubrimiento y evaluación

Tarea	Descripción	Habilidades requeridas
Identifique cargas de trabajo.	Identifique las cargas de trabajo candidatas adecuadas que desea migrar. Tenga en cuenta lo siguiente antes de elegir una carga de trabajo para la migración: • ¿Cuál es el valor empresarial de migrar o no migrar esta carga de trabajo? • ¿Existe un plan de contingencia si esta carga de trabajo no se migra correctamente al sistema de destino? Lo ideal es elegir una carga de trabajo que tenga el máximo impacto empresarial con el mínimo de riesgos involucrados. Mantenga el proceso general iterativo y migre en pequeños incrementos.	Arquitecto de datos, promotor empresarial y patrocinador de proyectos de migración
Identifique los orígenes y los requisitos de datos; diseñe un modelo de datos.	Redis organiza un taller para acelerar el descubrimiento y definir la planificación de la	Arquitecto de soluciones de Redis

Tarea	Descripción	Habilidades requeridas
	migración para el proyecto. Como parte de este taller, los equipos de Redis identifican los orígenes de datos y los requisitos del modelo de datos fuente, y analizan cómo se pueden remodelar en Redis Enterprise Cloud. El equipo de migración de Redis (servicios profesionales) realiza un ejercicio detallado de diseño del modelo de datos con su organización. Como parte de este ejercicio, el equipo de Redis: • Identifica las estructuras de datos de Redis objetivo. • Define la estrategia de mapeo de datos. • Documenta el enfoque y las recomendaciones de migración. • Revisa y finaliza el modelo de datos con las partes interesadas.	

Tarea	Descripción	Habilidades requeridas
Identificar las características de la base de datos de origen.	Identifique el producto de Redis que se utiliza en los entornos de origen y destino. Por ejemplo: • ¿La base de datos de origen es una base de datos de clúster de OSS, una base de datos de Redis independiente o una base de datos de Redis Enterprise? • ¿La base de datos de destino será una base de datos estándar de Redis Enterprise o una base de datos compatible con OSS Cluster? • ¿Cuáles son las implicaciones relacionadas con el código fuente de la aplicación?	Arquitecto de datos
Recopile el SLA actual del sistema y otras métricas de tamaño.	Determine los acuerdos de nivel de servicio (SLA) actuales expresados en términos de rendimiento (operaciones por segundo), latencia, tamaño total de memoria por base de datos y requisitos de alta disponibilidad (HA).	Arquitecto de datos

Tarea	Descripción	Habilidades requeridas
Identifique las características del sistema de destino.	Determine las respuestas a estas preguntas: • ¿Cuántos datos se deben migrar? • ¿Cuánto tiempo demora migrar la cantidad de datos dada? • ¿Cuáles son los requisitos de tiempo de inactividad para la migración? ¿Es aceptable que su servicio o aplicación no estén disponibles durante un período específico? Si es así, ¿durante cuánto tiempo? • ¿Qué grado de coherencia deben tener los datos migrados? ¿Puede la base de datos de destino estar en un estado ligeramente incoherente (desactualizada)? • ¿Es necesario transformar los datos antes de cargarlos en la base de datos de destino? (Por ejemplo, es posible que desee convertir índices de base de datos seleccionables en prefijos antes de la migración). • ¿Se puede acceder a la base de datos de origen	Arquitecto de datos, arquitecto de soluciones de Redis (opcional)

Tarea	Descripción	Habilidades requeridas
	desde el host de la base de datos de destino (por ejemplo, desde una VPC homóloga o desde un punto de conexión público mediante cifrado)? • Realice un ejercicio de dimensionamiento de datos y tamaño de clústeres de Redis con un arquitecto técnico de Redis. • Identifique los requisito s de red, los requisito s de infraestructura, las versiones de software y las licencias de software, y adquiera cualquier componente antes de la migración. • ¿Hay algún problema de seguridad relacionado con la transferencia de estos datos?	

Tarea	Descripción	Habilidades requeridas
Identifique las dependencias.	Identifique las dependencias ascendentes y descendentes del sistema actual que se va a migrar. Asegúrese de que el trabajo de migración esté alineado con otras migracion es de sistemas dependientes. Por ejemplo, si planea migrar otras aplicaciones empresari ales de las instalaciones a la nube de AWS, identifique estas aplicaciones y alinéelas en función de los objetivos, los plazos y las partes interesad as del proyecto.	Arquitecto de datos, arquitecto empresarial

Tarea	Descripción	Habilidades requeridas
Identifique las herramientas de migración.	En función de sus requisitos de migración de datos (como los datos de origen o los requisitos de tiempo de inactividad), puede utilizar cualquiera de las herramientas descritas anteriormente en la sección Herramientas. Además, puede utilizar: • Replicación bidireccional (activa-activa) mediante la implementación de CRDB. • Secuencias de comandos de exportación/importación personalizadas (por ejemplo, mediante comandos `DUMP/RESTORE`). • Herramientas adicionales de exportación/importación y herramientas de ayuda, como RIOT, ECStats2 o ETL. • Herramientas de IaC como Terraform o plantillas de AWS CloudFormation .	Arquitecto de soluciones de migración, arquitecto de soluciones de Redis
Cree un plan de contingencia.	Establezca un plan de contingencia para dar marcha atrás en caso de que surjan problemas durante la migración.	Gestión de proyectos, equipos técnicos, incluido el arquitecto

Complete las tareas de seguridad y cumplimiento

Tarea	Descripción	Habilidades requeridas
Proteja la consola de administración de Redis.	Para proteger la consola de administración, siga las instrucciones de la documentación de Redis.	Administrador de la infraestructura de TI
Proteja la base de datos de Redis.	Consulte las siguientes páginas de la documentación de Redis para: • Definir control de acceso basado en roles • Defina la seguridad de la red. • Habilite TLS.	
Proteja las API de Redis Cloud.	Al habilitar la API, puede administrar las claves de API de todos los propietarios de su cuenta de Redis Cloud. Para obtener una descripción general de las funciones de seguridad de la API, consulte la documentación de autenticación de la API en el sitio web de Redis.	Administrador de la infraestructura de TI

Configurar el nuevo entorno de

Tarea	Descripción	Habilidades requeridas
Configure un nuevo entorno en AWS.	Esta tarea incluye:	¿Informático o ingeniero DevOps

Tarea	Descripción	Habilidades requeridas
	• Actividades de configuración de AWS Landing Zone. La zona de aterrizaje admite: • Implementaciones con varias cuentas • Base de seguridad mínima • Una forma automatizada de aprovisionar nuevas cuentas con una base de seguridad y requisitos previos de ISV (redes, configuración de seguridad, etc.) • Notificaciones, registro centralizado y supervisión • Actividades de configuración del software ISV. Esto incluye las configuraciones que deben incluirse en la migración, como la configuración y los cambios de los productos y las cargas de trabajo. • Actividades de IaC, como configurar o personalizar las plantillas de AWS CloudFormation o Terraform.	

Tarea	Descripción	Habilidades requeridas
Implemente la arquitectura de migración.	1. Configure Redis Enterprise Cloud en AWS. 2. Instale herramientas de migración como RIOT o AWS DMS. Consulte la sección Herramientas para ver una lista de las herramientas disponibles. 3. Establezca la conectividad entre las capas de aplicación, migración y base de datos. 4. Cree una carga de trabajo de muestra que pueda fluir por cada capa y migrar un conjunto pequeño de datos de muestra. Ahora está preparado para ejecutar los procesos de migración de datos reales y probarlos.	¿Informático o DevOps ingeniero

Configurar redes

Tarea	Descripción	Habilidades requeridas
Establezca la conectividad.	Establezca la conectividad entre la infraestructura en las instalaciones y los recursos de la nube de AWS. Utilice los grupos de seguridad, AWS Direct Connect y otros	¿Informático o DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	recursos para lograr esta funcionalidad. Para obtener más información, consulte Conectar su centro de datos a AWS en el sitio web de AWS.	
Configure las interconexiones con VPC.	Establezca la interconexión de VPC entre las VPC que ejecutan aplicaciones empresariales (o las instancias EC2 que ejecutan herramientas de migración o el servidor de replicación de AWS DMS) y la VPC que ejecuta Redis Enterprise Cloud. Para obtener instrucciones, consulte Comenzar con Amazon VPC en la documentación de Amazon VPC y Habilitar el emparejamiento de VPC en la documentación de Redis.	¿Informático o DevOps ingeniero

Migración de datos

Tarea	Descripción	Habilidades requeridas
Elija una herramienta de migración de datos.	Consulte la tabla de la sección Herramientas para ver las descripciones, ventajas y desventajas de estas herramientas: • Exportación e importación de RDS	Arquitecto de soluciones de migración

Tarea	Descripción	Habilidades requeridas
	• Función de replicación de Redis (`ReplicaOf `) • AWS DMS • Combinación lógica de bases de datos Las filas siguientes describen las tareas de migración de datos asociadas a cada herramienta.	

Tarea	Descripción	Habilidades requeridas
Opción 1: utilice la exportación e importación de RDB.	1. Desconectar la fuente: detenga el tráfico en la base de datos de origen (por ejemplo, desconect ando las aplicaciones empresariales). 2. Exportar: exporte los datos de la base de datos de origen como un archivo RDB. 3. Etapa: cargue los datos en una ubicación a la que puedan acceder las instancias de Redis Enterprise Cloud en AWS (por ejemplo, puede cargarlos en un bucket de S3 o en un servidor FTP). 4. Importación: importe los archivos RDB (enumerán dolos todos en un solo paso de importación) a su base de datos de destino de Redis Enterprise Cloud. 5. Transición: vaya a la base de datos de destino (por ejemplo, conectando su aplicación, conéctese a ella). Para obtener más información, consulte la documentación de Redsis.	Arquitecto de soluciones de migración, arquitecto de soluciones de Redis

Tarea	Descripción	Habilidades requeridas
Opción 2: utilice la caracterí stica de replicación de Redis (activa-pasiva).	1. Conectar base de datos: establezca un enlace de `ReplicaOf` entre las bases de datos de origen y destino. 2. Ejecute una sincronización inicial: espere hasta que se complete la sincronización inicial entre las bases de datos de origen y destino. 3. Desconectar la fuente: detenga el tráfico en la base de datos de origen (por ejemplo, desconect ando la aplicación). 4. Ejecute la replicación delta: espere hasta que la replicación delta se replique en la base de datos de destino. 5. Transición: vaya a la base de datos de destino (por ejemplo, conectando su aplicación a ella). 6. Eliminar: elimine el enlace de `ReplicaOf` entre las bases de datos de origen y destino. Para obtener más información, consulte la documentación de Redsis.	Arquitecto de soluciones de migración, arquitecto de soluciones de Redis

Tarea	Descripción	Habilidades requeridas
Opción 3: utilice AWS DMS.	1. Configurar una instancia de replicación de AWS DMS: esta instancia realiza todos los procesos de migración. Para obtener instrucciones: Trabajar con una instancia de replicación de AWS DMS en la documentación de AWS DMS. 2. Defina la base de datos de origen: defina el punto de conexión de origen. Pruebe la conectividad entre el punto de conexión de origen y el servidor de replicación de AWS DMS. Para obtener instrucciones: Cómo crear puntos de enlace de origen y destino en la documentación de AWS DMS. 3. Configurar la base de datos de destino: configure Redis Enterprise Cloud en AWS y configure la base de datos a la que se va a migrar. 4. Defina la base de datos de destino: defina el punto de conexión de destino. Asegúrese de que la Interconexión de VPC esté establecida entre la VPC en la que se ejecuta AWS DMS y la VPC que aloja	Arquitecto de soluciones de migración, arquitecto de soluciones de Redis

Tarea	Descripción	Habilidades requeridas
	Redis Enterprise Cloud en AWS. Pruebe la conectividad entre el servidor de replicación de AWS DMS y la base de datos de destino. 5. Cree una tarea de AWS DMS: cree una tarea o un conjunto de tareas para definir las tablas y los procesos de replicación que desee utilizar para migrar los datos. Para obtener instrucciones: Trabajar con las tareas de AWS DMS en la documentación de AWS DMS. 6. Migrar: migre los datos ejecutando la tarea de AWS DMS. 7. Transición: vaya a la base de datos de destino (por ejemplo, conectando su aplicación a ella).	
Opción 4: utilice la combinación lógica de bases de datos.	Esta opción implica el uso de un script de migración o una herramienta ETL que pueda transformar el modelo de datos físicos de la base de datos de origen y generar un archivo RDB. Los servicios profesionales de Redis pueden ayudar con este paso, si es necesario.	Arquitecto de soluciones de migración, arquitecto de soluciones de Redis

Migración de la aplicación

Tarea	Descripción	Habilidades requeridas
Alinee los plazos y los objetivos de la gestión de proyectos.	Alinee los objetivos, hitos y plazos del proyecto de migración de la capa de aplicación con los del proyecto de migración de datos de Redis.	Administración de proyectos
Alinee las actividades de prueba.	Después de migrar y modernizar la capa de aplicaciones en la nube de AWS, dirija la capa de aplicaciones a la recién migrada Redis Enterprise Cloud en AWS para realizar pruebas.	Pruebas

Prueba

Tarea	Descripción	Habilidades requeridas
Implemente planes de pruebas.	Ejecute las rutinas de migración de datos y los scripts que se desarrollaron durante la fase de implement ación en un entorno de pruebas, según los requisitos de las pruebas, en su sitio.	Pruebas
Prueba de calidad de datos de prueba.	Prueba de la calidad de los datos después de migrarlos.	Pruebas
Pruebe la funcionalidad.	Pruebe las consultas de datos y la capa de aplicación para	Pruebas

Tarea	Descripción	Habilidades requeridas
	asegurarse de que la aplicación funciona al mismo nivel que en el sistema de origen.	

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Tome la decisión de transición.	Una vez finalizadas todas las pruebas a nivel de aplicación y base de datos, el equipo de liderazgo ejecutivo y las partes interesadas toman la decisión final sobre si pasarán al nuevo entorno de AWS en función de los resultados finales confirmados por los equipos de pruebas.	La gestión de proyectos, campeona del mundo empresarial
Transición a la nube de AWS.	Cuando haya confirmado que todo está en su lugar, dirija la capa de aplicación a los datos recién migrados y dirija los clientes a la nueva capa de aplicaciones que se está ejecutando en función del nuevo sistema Redis Enterprise Cloud en AWS.	DevOps Ingeniero o informático, arquitecto de datos, arquitecto de soluciones de migración, arquitecto de soluciones de Redis

Recursos relacionados

Recursos de Redis

- Documentación de Redis Enterprise Cloud

- Herramienta RIOT (GitHub repositorio)
- Terraform Provider (descargar)

Recursos de AWS

- Migraciones de demostración
- Soluciones de socios de AWS
- Documentación
- Publicaciones de blog
- Libros blancos
- Tutoriales y videos
- Migración de datos a la nube de AWS
- Recomendaciones de AWS

Información adicional

Para conocer los requisitos de seguridad estándar para la migración de cargas de trabajo de Redis a la nube de AWS, consulte las prácticas recomendadas en materia de seguridad, identidad y conformidad en el sitio web de AWS y el Centro de confianza de Redis en el sitio web de Redis.

Migre SAP ASE de Amazon EC2 a Amazon Aurora compatible con PostgreSQL mediante AWS SCT y AWS DMS

Creado por Amit Kumar (AWS) y Ankit Gupta

Entorno: PoC o piloto	Origen: SAP ASE	Destino: Aurora compatible con PostgreSQL
Tipo R: redefinir la plataforma	Carga de trabajo: SAP	Tecnologías: migración; bases de datos
Servicios de AWS: AWS DMS; AWS SCT		

Resumen

Este patrón describe cómo migrar una base de datos de SAP Adaptive Server Enterprise (SAP ASE) alojada en una instancia de Amazon Elastic Compute Cloud (Amazon EC2) a una edición compatible con PostgreSQL de Amazon Aurora mediante la herramienta de conversión de esquemas de AWS (AWS SCT) y el AWS Database Migration Service (AWS DMS). El patrón se centra tanto en la conversión del lenguaje de definición de datos (DDL) para los objetos almacenados como en la migración de datos.

Compatible con Aurora PostgreSQL, admite las cargas de trabajo de procesamiento de transacciones online (OLTP). Este servicio gestionado proporciona configuraciones que se escalan automáticamente según la demanda. Puede iniciar, cerrar, ampliar o reducir automáticamente la base de datos en función de las necesidades de la aplicación. Puede ejecutar su base de datos en la nube sin administrar ninguna instancia de base de datos. Compatible con Aurora PostgreSQL ofrece una opción rentable para las cargas de trabajo poco frecuentes, intermitentes o impredecibles.

El proceso de migración consta de dos fases principales:

- Conversión de esquemas de bases de datos con AWS SCT
- Migración de los datos mediante AWS DMS

En la sección Epics se proporcionan instrucciones detalladas para ambas fases. Para obtener información sobre la solución de problemas específicos del uso de AWS DMS con bases de datos de SAP ASE, consulte Solución de problemas con SAP ASE en la documentación de AWS DMS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos SAP ASE de origen en una instancia EC2 con servicios de servidor, base de datos y oyente en funcionamiento
- Una base de datos de destino Aurora compatible con PostgreSQL

Limitaciones

- El número de puerto para las conexiones puede ser 5432.
- La función huge_pages está activada de forma predeterminada, pero se puede modificar.
- La granularidad oint-in-time de la recuperación de P (PITR) es de 5 minutos.
- La replicación entre regiones no está disponible actualmente.
- El tamaño máximo de almacenamiento para una base de datos Aurora es de 128 TiB.
- Puede crear un máximo de 15 réplicas de lectura.
- El límite de tamaño de la tabla está limitado únicamente por el tamaño del volumen del clúster de Aurora, por lo que el tamaño máximo de la tabla para un clúster de base de datos compatible con Aurora PostgreSQL es de 32 TiB. Le recomendamos que siga estas prácticas recomendadas de diseño de tabla, como la partición de tablas grandes.

Versiones de producto

- Base de datos de origen: AWS DMS actualmente es compatible con SAP ASE 15, 15.5, 15.7 y 16.x. Consulte la Guía del usuario de AWS DMS para obtener la información más reciente sobre el soporte de versiones de SAP ASE.
- Base de datos de destino: PostgreSQL 9.4 y versiones posteriores (para la versión 9.x), 10.x, 11.x, 12.x, 13.x y 14.x. Consulte la Guía del usuario de AWS DMS para ver las últimas versiones compatibles de PostgreSQL.
- Amazon Aurora 1.x o posteriores. Para obtener la información más reciente, consulte las versiones compatibles con Aurora PostgreSQL y las versiones del motor en la documentación de Aurora.

Arquitectura

Pila de tecnología de origen

- Base de datos SAP ASE que se ejecuta en Amazon EC2

Pila de tecnología de destino

- Base de datos Aurora compatible con PostgreSQL

Arquitectura de migración

Herramientas

- Edición de Amazon Aurora compatible con PostgreSQL es un motor de base de datos relacional compatible con ACID, completamente administrado, que le permite configurar, administrar y escalar implementaciones de PostgreSQL.
- La herramienta de conversión de esquemas de AWS (AWS SCT) admite migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado a un formato compatible con la base de datos de destino.
- AWS DMS admite varias bases de datos de origen y destino diferentes. Para obtener más información, consulte Fuentes de migración de datos y Objetivos de migración de datos en la documentación de AWS DMS. Para obtener el soporte más completo de versiones y funciones, recomendamos que utilice la última versión de AWS DMS.

Epics

Configurar el entorno

Tarea	Descripción	Habilidades requeridas
Configure el acceso a la red en la instancia EC2 de origen.	Configure grupos de seguridad en la instancia EC2 que aloja la base de datos SAP ASE de origen.	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	Para obtener instrucciones, consulte Grupos de seguridad de Amazon EC2 para instancias de Linux en la documentación de Amazon EC2.	
Cree su clúster de base de datos Aurora compatible con PostgreSQL de destino.	Instale, configure y lance un clúster compatible con Aurora PostgreSQL para la base de datos de destino. Para obtener más información, consulte Creación de un clúster de base de datos de Amazon Aurora, en la documentación de Aurora.	Administrador de base de datos
Configure la autorización para el clúster de base de datos de destino.	Configure grupos de seguridad y firewalls para la base de datos de destino. Para obtener instrucciones, consulte Creación de un clúster de base de datos de Amazon Aurora en la documentación de Aurora.	Administrador de base de datos, administrador de sistemas

Convierta el esquema de su base de datos con AWS SCT

Tarea	Descripción	Habilidades requeridas
Iniciar AWS SCT.	Para iniciar AWS SCT, siga las instrucciones de la documentación de AWS SCT.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	AWS SCT proporciona una interfaz de usuario basada en el proyecto para convertir automáticamente el esquema de la base de datos de su base de datos SAP ASE de origen en un formato compatible con su instancia de base de datos de Aurora compatible con PostgreSQL de destino.	
Cree puntos de enlace SCT de AWS.	Cree puntos de conexión para las bases de datos de origen SAP ASE, y las bases de datos de desino PostgreSQL. Para obtener instrucciones, consulte la documentación de AWS SCT.	Administrador de base de datos
Generar un informe de evaluación.	Cree un informe de evaluació n de la migración de la base de datos para evaluar la migración y detectar cualquier objeto o función incompatible. Para obtener instrucciones, consulte la documentación de AWS SCT.	Administrador de base de datos
Convierta el esquema.	Convierta el esquema de la base de datos siguiendo las instrucciones de la documenta ción de AWS SCT.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Valide los objetos de la base de datos.	Si AWS SCT no puede convertir un objeto de base de datos, identificará su nombre y otros detalles. Debe convertir estos objetos manualmente. Para identificar estas discrepancias, siga las instrucciones de la entrada del blog de AWS sobre cómo Validar los objetos de la base de datos después de migrar de SAP ASE a Amazon RDS para PostgreSQL o Amazon Aurora PostgreSQL.	Administrador de base de datos

Analice la migración a AWS DMS

Tarea	Descripción	Habilidades requeridas
Valide las versiones de las bases de datos de origen y de destino.	Compruebe la compatibilidad de las versiones de las bases de datos SAP ASE con AWS DMS. Para obtener más informaci ón, consulte Origens de AWS DMS y Objetivos de AWS DMS en la documentación de AWS DMS.	Administrador de base de datos
Identifique los requisitos de almacenamiento (como el tipo y la capacidad de almacenam	Elija la capacidad de almacenamiento adecuada para la base de datos de	Administrador de base de datos, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
iento) de la base de datos de destino.	destino en función del tamaño de la base de datos de origen.	
Elija el tipo de instancia, la capacidad y otras caracterí sticas de la instancia de replicación.	Elija el tipo de instancia, la capacidad, las funciones de almacenamiento y las funciones de red que mejor se adapten a sus necesidades. Para obtener orientación, consulte Elegir la instancia de replicación de AWS DMS correcta para la migración en la documentación de AWS DMS.	Administrador de base de datos, administrador de sistemas
Identifique los requisitos de seguridad de acceso a la red.	Identifique requisitos de seguridad para acceder a la red de las bases de datos de origen y destino. Siga las instrucciones de Configuración de una red para una instancia de replicación en la documentación de AWS DMS.	Administrador de base de datos, administrador de sistemas

Migrar datos

Tarea	Descripción	Habilidades requeridas
Migre los datos mediante la creación de una tarea de migración en AWS DMS.	Para migrar datos, cree una tarea y siga las instrucciones en la documentación de AWS DMS.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Le recomendamos utilizar la versión más reciente de AWS DMS para obtener el soporte más completo de versiones y características.	
Valide los datos.	Para validar que los datos se migraron con precisión de la base de datos de origen a la base de datos de destino, siga las pautas de validación de datos que se proporcionan en la documentación de AWS DMS.	Administrador de base de datos

Migrar la aplicación

Tarea	Descripción	Habilidades requeridas
Identificar la estrategia de migración de aplicaciones.	Elija una de las siete estrategias (7R) para migrar aplicaciones a la nube.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas
Seguir la estrategia de migración de aplicaciones.	Complete las tareas de la base de datos identificadas por el equipo de la aplicación, incluida la actualización de los detalles de la conexión DNS de la base de datos de destino y la actualización de las consultas dinámicas.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Realizar la transición a la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Cambiar los clientes de la aplicación a la nueva infraestructura.	Cambie la conexión de la base de datos de origen a la base de datos de destino. Para obtener más información, consulte la sección de Transición de la Estrategia de migración para bases de datos relacionales.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cerrar los recursos temporales de AWS.	Finalice todas las tareas de migración, las instancias de replicación, los puntos de enlace y otros recursos de AWS SCT y AWS DMS. Para obtener más información, consulte la documentación de AWS DMS.	Administrador de base de datos, administrador de sistemas
Revise y valide los documentos del proyecto.	Valide todos los pasos de la documentación del proyecto para asegurarse de que todas las tareas se hayan completado correctamente.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas
Cierre el proyecto.	Cierre el proyecto de migración y envíe sus comentarios.	Administrador de base de datos, propietario de la

Tarea	Descripción	Habilidades requeridas
		aplicación, administrador de sistemas

Recursos relacionados

Referencias

- Habilite las conexiones cifradas para las instancias de base de datos de PostgreSQL en Amazon RDS (Recomendaciones de AWS)
- Transporte bases de datos PostgreSQL entre dos instancias de base de datos de Amazon RDS mediante pg_transport (Recomendaciones de AWS)
- Precios de Amazon Aurora
- Prácticas recomendadas con Edición compatible con Amazon Aurora PostgreSQL (documentación de Amazon Aurora)
- Documentación de AWS SCT
- Documentación de AWS DMS
- Uso de una base de datos SAP ASE como origen para AWS DMS

Tutoriales y vídeos

- Introducción a AWS Database Migration Service (AWS DMS)
- AWS Database Migration Service (AWS DMS) (vídeo)

Migración de los certificados SSL de Windows a un equilibrador de carga de aplicación mediante ACM

Creado por Chandra Sekhar Yaratha (AWS) e Igor Kovalchuk (AWS)

Entorno: producción	Origen: aplicación web de Windows	Destino: equilibrador de carga de aplicación en AWS
Tipo R: redefinir la plataforma	Carga de trabajo: Microsoft	Tecnologías: migración; gestión y gobierno; aplicaciones web y móviles
Servicios de AWS: Elastic Load Balancing (ELB); AWS Certificate Manager (ACM)		

Resumen

Este patrón proporciona orientación sobre el uso de AWS Certificate Manager (ACM) para migrar los certificados Secure Sockets Layer (SSL) existentes desde sitios web alojados en servidores en las instalaciones o instancias de Amazon Elastic Compute Cloud (Amazon EC2) en Microsoft Internet Information Services (IIS). Después, los certificados SSL se pueden usar con Elastic Load Balancing en AWS.

SSL protege sus datos, afirma su identidad, proporciona una mejor clasificación en los motores de búsqueda, ayuda a cumplir los requisitos de la norma de seguridad de datos del sector de las tarjetas de pago (PCI DSS) y mejora la confianza de los clientes. Los desarrolladores y los equipos de TI que administran estas cargas de trabajo desean que sus aplicaciones e infraestructuras web, incluidos el servidor IIS y Windows Server, sigan cumpliendo con sus políticas básicas.

Este patrón incluye la exportación manual de los certificados SSL existentes desde Microsoft IIS, su conversión del formato de intercambio de información personal (PFX) al formato de correo privado mejorado (PEM) compatible con ACM y, a continuación, su importación a ACM en la cuenta de AWS. También se describe cómo crear un equilibrador de carga de aplicación para la aplicación y cómo configurar el equilibrador de carga de aplicación para que utilice los certificados importados. A continuación, las conexiones HTTPS finalizan en el equilibrador de carga de aplicación y no

se necesita más sobrecarga de configuración en el servidor web. Para obtener más información, consulte Create an HTTPS listener for your Application Load Balancer (Crear un oyente HTTPS para el equilibrador de carga de aplicación).

Los servidores Windows utilizan archivos .pfx o .p12 para contener el archivo de clave pública (certificado SSL) y el archivo de clave privada exclusivo. La autoridad de certificación (CA) le proporciona su archivo de clave pública. El servidor se utiliza para generar el archivo de clave privada asociado en el que se creó la solicitud de firma de certificados (CSR).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una nube privada virtual (VPC) en AWS con al menos una subred privada y una pública en cada zona de disponibilidad utilizada por los destinos
- La versión 8.0 o posterior de IIS se ejecuta en Windows Server 2012 o posterior
- Una aplicación web que se ejecute en IIS
- Acceso de administrador al servidor IIS

Arquitectura

Pila de tecnología de origen

- Implementación de un servidor web IIS con SSL para garantizar que los datos se transmitan de forma segura en una conexión cifrada (HTTPS)

Arquitectura de origen

Pila de tecnología de destino

- Certificados ACM en su cuenta de AWS
- Un equilibrador de carga de aplicación configurado para usar certificados importados
- Instancias de Windows Server en las subredes privadas

Arquitectura de destino

Herramientas

- AWS Certificate Manager (ACM) le ayuda a crear, almacenar y renovar certificados y claves SSL/TLS X.509 públicos y privados que protegen sus sitios web y aplicaciones de AWS.
- Elastic Load Balancing (ELB) distribuye el tráfico entrante de aplicaciones o redes entre varios destinos. Así, por ejemplo, puede distribuir el tráfico entre instancias de EC2, contenedores y direcciones IP de una o varias zonas de disponibilidad.

Prácticas recomendadas

- Imponga redireccionamientos de tráfico de HTTP a HTTPS.
- Configure correctamente los grupos de seguridad para su equilibrador de carga de aplicación para permitir el tráfico entrante solo a puertos específicos.
- Implemente las instancias de EC2 en diferentes zonas de disponibilidad para garantizar una alta disponibilidad.
- Configure el dominio de la aplicación para que apunte al nombre DNS del equilibrador de carga de aplicación en lugar de a su dirección IP.
- Asegúrese de que el equilibrador de carga de aplicación tenga configuradas las comprobaciones de estado de la capa de aplicación.
- Configure el umbral para las comprobaciones de estado.
- Usa Amazon CloudWatch para monitorear el Application Load Balancer.

Epics

Exportar un archivo .pfx

Tarea	Descripción	Habilidades requeridas
Exporte el archivo .pfx desde Windows Server.	Para exportar el certificado SSL como un archivo .pfx desde el administrador de IIS en las instalaciones de Windows Server:	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	1. Seleccione Start (iniciar) , Administrative (Admin), Internet Information Services (IIS) Manager. 2. Seleccione el nombre del servidor y, en Security (Seguridad), haga doble clic en Server Certificates (Certificados de servidor). 3. Seleccione el certificado que desea exportar y, a continuación, Export. 4. En el cuadro Export Certificate (Exportar certificado) seleccione una ubicación, una ruta y un nombre para el archivo .pfx. 5. Especifique y confirme una contraseña para el archivo .pfx. Nota: Necesitará esta contraseña al instalar el archivo .pfx. 6. Seleccione Aceptar. El archivo .pfx ahora debería guardarse en la ubicación y la ruta que especificó.	

Convertir el certificado codificado en PFX al formato PEM

Tarea	Descripción	Habilidades requeridas
Descargue e instale el kit de herramientas de OpenSSL.	1. Descargue e instale Win32/Win64 OpenSSL desde el sitio web de Shining Light Productions. 2. Agregue la ubicación de los archivos binarios de OpenSSL a la variable `PATH` de sistema para que estén disponibles para su uso en la línea de comandos.	Administrador de sistemas
Convertir el certificado codificado en PFX al formato PEM.	Los pasos siguientes convierten el archivo de certificado firmado y codificado en PFX en tres archivos en formato PEM: • `cert-file.pem` contiene el certificado SSL/TLS del recurso. • `privatekey.pem` contiene la clave privada del certificado sin protección por contraseña. • `ca-chain.pem` contiene el certificado raíz de la CA. Para convertir el certificado codificado en PFX: 1. Ejecute Windows PowerShell.	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	2. Utilice el comando siguiente para extraer la clave pública del certificado del archivo PFX. Escriba la contraseña del certificado cuando se le pida. `openssl pkcs12 -in <filename>.pfx -nocerts -out withpw-privatekey.pem` El comando genera un archivo de clave privada codificado en PEM denominado `privatekey.pem` . Escriba una contraseña para proteger el archivo de clave privada cuando se le solicite. 3. Ejecute el comando siguiente para eliminar la contraseña. Cuando se le pida, proporcione la contraseña que creó en el paso 2. `openssl rsa -in withpw-privatekey.pem -out privatekey.pem` Si el comando se ejecuta correctamente, se muestra el mensaje «writing RSA	

Tarea	Descripción	Habilidades requeridas
	key» (escribiendo clave RSA). 4. Utilice el comando siguiente para transferir el certificado del archivo PFX al archivo PEM. `openssl pkcs12 -in <file_name>.pfx -clcerts -nokeys -out cert-file.pem` Esto crea un archivo de certificado codificado para PEM denominado `cert-file.pem` . Si el comando se ejecuta correctamente, se muestra el mensaje «MAC verified OK» (MAC verificado correctamente). 5. Cree un archivo de cadena CA a partir del archivo PFX. Ejecute el comando siguiente para crear un archivo de cadena CA llamado `ca-chain.pem` . `openssl pkcs12 -in <file_name>.pfx -cacerts -nokeys -chain -out ca-chain.pem` Si el comando se ejecuta correctamente, se muestra el mensaje «MAC verified	

Tarea	Descripción	Habilidades requeridas
	OK» (MAC verificado correctamente).	

Importar un certificado a ACM

Tarea	Descripción	Habilidades requeridas
Prepárese para importar el certificado.	En la consola ACM, seleccione Import a certificate (Importar un certificado).	Administrador de la nube
Proporcione el cuerpo del certificado.	En el Certificate body, pegue el certificado codificado en PEM para importar. Para obtener más información sobre los comandos y los pasos descritos en esta y otras tareas de esta Epic, consulte Import a certificate (Importar un certificado) en la documentación de ACM.	Administrador de la nube
Proporcione la clave privada del certificado.	En Certificate private key, pegue la clave privada codificada en PEM y sin cifrar que coincida con la clave pública del certificado.	Administrador de la nube
Proporcione la cadena del certificado.	En Certificate chain (Cadena del certificado), pegue la cadena del certificado codificada en PEM, que se almacena en el archivo `CertificateChain.pem` .	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Importe el certificado.	Seleccione Review and import. Confirme que la información sobre su certificado es correcta y, a continuación, seleccione Import.	Administrador de la nube

Creación de un equilibrador de carga de aplicación

Tarea	Descripción	Habilidades requeridas
Cree y configure el equilibrador de carga y los oyentes.	Siga las instrucciones de la documentación de Elastic Load Balancing para configurar un grupo objetivo, registrar los objetivos y crear un equilibrador de carga de aplicación y un oyente. Agregue un segundo oyente (HTTPS) para el puerto 443.	Administrador de la nube

Solución de problemas

Problema	Solución
Windows PowerShell no reconoce el comando OpenSSL incluso después de agregarlo a la ruta del sistema.	Compruebe que `$env:path` incluya la ubicación de los binarios de OpenSSL. Si no es así, ejecute el siguiente comando en: PowerShell `$env:path = $env:path + ";C:\OpenSSL-Win64\bin"`

Recursos relacionados

Importing a certificate into ACM (Importar un certificado a ACM)

- Consola de ACM
- Certificate and key format for importing (Formato de certificado y de clave para importación)
- Importing a certificate (Importar un certificado)
- AWS Certificate Manager User Guide (Guía del usuario de AWS Certificate Manager)

Creating an Application Load Balancer (Crear un equilibrador de carga de aplicación)

- Creación de un equilibrador de carga de aplicación
- Application Load Balancer User Guide (Guía del usuario del equilibrador de carga de aplicación)

Migración de una cola de mensajes de Microsoft Azure Service Bus a Amazon SQS

Tipo R: redefinir la plataforma	Origen: Aplicaciones que utilizan colas de Azure Service Bus	Destino: Amazon SQS
Creado por: AWS	Entorno: PoC o piloto	Tecnologías: aplicaciones web y móviles; migración
Carga de trabajo: Microsoft	Servicios de AWS: Amazon SQS	

Resumen

Este patrón describe cómo migrar una aplicación web o de consola .NET Framework o .NET Core desde la plataforma de mensajería en cola Service Bus de Microsoft Azure a Amazon Simple Queue Service (Amazon SQS).

Las aplicaciones utilizan los servicios de mensajería para enviar y recibir datos de otras aplicaciones. Estos servicios ayudan a compilar microservicios disociados y altamente escalables, sistemas distribuidos y aplicaciones sin servidor en la nube.

Las colas de Azure Service Bus forman parte de una infraestructura de mensajería de Azure más amplia que admite la creación de colas y la mensajería de publicación y suscripción.

Amazon SQS es un servicio de colas de mensajes completamente administrado que permite el desacople y el escalado de microservicios, sistemas distribuidos y aplicaciones sin servidor. Amazon SQS elimina la complejidad y la sobrecarga asociadas a la administración y el funcionamiento del middleware orientado a mensajes y permite a los desarrolladores centrarse en diferenciar el trabajo. Con Amazon SQS, puede enviar, almacenar y recibir mensajes entre componentes de software a cualquier volumen, sin perder mensajes ni requerir la disponibilidad de otros servicios.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa

- Una aplicación web o de consola .NET Framework o .NET Core que utiliza colas de Azure Service Bus (se adjunta un código de muestra)

Versiones de producto

- .NET Framework 3.5 o posterior, o .NET Core 1.0.1, 2.0.0 o posterior

Arquitectura

Pila de tecnología de origen

- Una aplicación web o de consola .NET (Core o Framework) que utiliza una cola de Azure Service Bus para enviar mensajes

Pila de tecnología de destino

- Amazon SQS

Herramientas

Herramientas

- Microsoft Visual Studio

Código

Para crear una política de AWS Identity and Access Management (IAM) para Amazon SQS:

1. Inicie sesión en la consola de administración de AWS y abra la consola de IAM en https://console.aws.amazon.com/iam/.

2. En el panel de navegación de la izquierda, elija Políticas y, a continuación, elija Crear política.

3. Elija la pestaña JSON y pegue el siguiente código:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
```

```
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "sqs:DeleteMessage",
            "sqs:GetQueueUrl",
            "sqs:ChangeMessageVisibility",
            "sqs:SendMessageBatch",
            "sqs:ReceiveMessage",
            "sqs:SendMessage",
            "sqs:GetQueueAttributes",
            "sqs:ListQueueTags",
            "sqs:ListDeadLetterSourceQueues",
            "sqs:DeleteMessageBatch",
            "sqs:PurgeQueue",
            "sqs:DeleteQueue",
            "sqs:CreateQueue",
            "sqs:ChangeMessageVisibilityBatch",
            "sqs:SetQueueAttributes"
         ],
         "Resource": "arn:aws:sqs:*:<AccountId>:*"
      },
      {
         "Sid": "VisualEditor1",
         "Effect": "Allow",
         "Action": "sqs:ListQueues",
         "Resource": "*"
      }
   ]
}
```

4. Elija Revisar política, escriba un nombre y seleccione Crear política.

5. Adjunte la política recién creada a su rol de IAM existente o cree un rol nuevo.

Epics

Configuración de Amazon SQS en AWS

Tarea	Descripción	Habilidades requeridas
Cree una política de IAM para Amazon SQS.	Cree la política de IAM que proporcionará acceso a Amazon SQS. Consulte la	Ingeniero de sistemas

Tarea	Descripción	Habilidades requeridas
	sección Código para ver una muestra de política.	
Crear un perfil de AWS.	Cree un perfil nuevo ejecutando las herramientas de AWS para PowerShell el comando Set-AWSCredential. Este comando almacena la clave de acceso y la clave secreta en el archivo de credenciales predeterminado bajo el nombre de perfil que especifique. Vincule la política de Amazon SQS que creó anteriormente con esta cuenta. Conserve el ID de clave de acceso y la clave de acceso secreta de AWS. Estos serán necesarios en los pasos siguientes.	Ingeniero de sistemas
Crear una cola de SQS.	Puede crear una cola estándar o una cola con el primero en entrar, primero en salir (FIFO). Para obtener instrucciones, consulte el enlace de la sección Referencias.	Ingeniero de sistemas

Revisar el código de su aplicación .NET

Tarea	Descripción	Habilidades requeridas
Instalar AWS Toolkit for Visual Studio	Este kit de herramientas es una extensión para Microsoft Visual Studio y facilita la	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	creación e implementación de aplicaciones .NET en AWS. Para obtener instrucciones de instalación y uso, consulte el enlace de la sección Referenci as.	
Instale el paquete AWSSDK .SQS. NuGet	Puede instalar AWSSDK .SQS seleccionando «Administ rar NuGet paquete» en Visual Studio o ejecutando el comando « AWSSDKInstall-Package .SQS».	Desarrollador de aplicaciones
Cree un objeto en su AWSCredentials aplicació n.NET.	La aplicación de ejemplo del archivo adjunto muestra cómo crear un AWSCredentials objeto básico, que hereda de AWSCredentials. Puede utilizar el identificador de clave de acceso y la clave de acceso secreta de antes, o dejar que el objeto los elija de la carpeta .aws como parte del perfil de usuario en tiempo de ejecución.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Cree un objeto de cliente de SQS.	Cree un objeto de cliente de SQS (AmazonSQSClient) para .NET Framework. Esto forma parte del espacio de nombres Amazon.SQS. Este objeto es obligatorio en lugar del IQueueClient, que forma parte de Microsoft .Azure. ServiceBus espacio de nombres.	Desarrollador de aplicaciones
Llame al SendMessageAsync método para enviar mensajes a la cola de SQS.	Cambie el código que envía el mensaje a la cola para usar el. amazonSqsClient SendMessageAsync método. Para obtener más información, consulte el código de muestra adjunto.	Desarrollador de aplicaciones
Llame al ReceiveMessageAsync método para recibir mensajes de la cola de SQS.	Cambie el código que recibe el mensaje para usar el. amazonSqsClient ReceiveMessageAsync método. Para obtener más información, consulte el código de muestra adjunto.	Desarrollador de aplicaciones
Llame al DeleteMessageAsync método para eliminar los mensajes de la cola de SQS.	Para eliminar mensajes, cambie el código del QueueClient. CompleteAsync método para. amazonSqsClient DeleteMessageAsync método. Para obtener más información, consulte el código de muestra adjunto.	Desarrollador de aplicaciones

Recursos relacionados

- Guía para desarrolladores de AWS SDK para .NET
- Mensajería mediante Amazon SQS
- Creación y uso de una cola de Amazon SQS con AWS SDK para .NET
- Enviar un mensaje de Amazon SQS
- Recibir un mensaje de una cola de Amazon SQS
- Eliminar un mensaje de una cola de Amazon SQS
- AWS Toolkit for Visual Studio

Información adicional

Este patrón incluye dos aplicaciones de muestra (consulte la sección de adjuntos):

- AzureSbTestAppincluye código que usa la cola del bus de servicio de Azure.
- AmazonSqsTestApputiliza Amazon SQS. Se trata de una aplicación de consola que utiliza .NET Core 2.2 e incluye ejemplos para enviar y recibir mensajes.

Notas:

- QueueClient es un objeto de IQueueClient, que forma parte de Microsoft.Azure. ServiceBus espacio de nombres (incluido en Microsoft.Azure). ServiceBus NuGet paquete).
- amazonSqsClient es un objeto de AmazonSQSClient, que forma parte del espacio de nombres Amazon.sqs (incluido en el paquete.SQS). AWSSDK NuGet
- Dependiendo de dónde se ejecute el código, por ejemplo, si se ejecuta en EC2, el rol debe tener permiso para escribir en la cola de SQS.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Migre una EnterpriseOne base de datos de Oracle JD Edwards a AWS mediante Oracle Data Pump y AWS DMS

Creado por Thanigaivel Thirumalai (AWS)

Entorno: producción	Fuente: Oracle JD Edwards EnterpriseOne	Destino: Amazon RDS para Oracle
Tipo R: redefinir la plataforma	Carga de trabajo: Oracle	Tecnologías: Migración; bases de datos
Servicios de AWS: Amazon RDS; AWS DMS		

Resumen

Puede migrar y ejecutar la EnterpriseOne base de datos de JD Edwards en Amazon Relational Database Service (Amazon RDS). Al migrar la base de datos a Amazon RDS, AWS puede encargarse de las tareas de backup y de la configuración de alta disponibilidad, para que pueda concentrarse en el mantenimiento de EnterpriseOne la aplicación y su funcionalidad. Para obtener una lista completa de los factores clave a tener en cuenta durante el proceso de migración, consulte Estrategias de migración de bases de datos de Oracle en Recomendaciones de AWS.

Existen varias formas de migrar una EnterpriseOne base de datos, entre las que se incluyen las siguientes:

- Uso de Oracle Universal Batch Engine (UBE) R98403 para la creación de esquemas y tablas, y uso de AWS Database Migration Service (AWS DMS) para la migración
- Uso de herramientas nativas de bases de datos para la creación de esquemas y tablas y uso de AWS DMS para la migración
- Uso de herramientas nativas de bases de datos para la migración de datos existentes (carga completa) y uso de AWS DMS para tareas de captura de datos de cambios (CDC)

Este patrón cubre la tercera opción. En él se explica cómo migrar las EnterpriseOne bases de datos locales a Amazon RDS for Oracle mediante Oracle Data Pump con AWS DMS y su función CDC.

Oracle JD Edwards EnterpriseOne es una solución de planificación de recursos empresariales (ERP) para organizaciones que fabrican, construyen, distribuyen, dan servicio o gestionan productos o activos físicos. JD Edwards EnterpriseOne es compatible con varios hardware, sistemas operativos y plataformas de bases de datos.

Al migrar aplicaciones ERP fundamentales, como JD Edwards EnterpriseOne, es fundamental minimizar el tiempo de inactividad. AWS DMS minimiza el tiempo de inactividad gracias a su replicación, tanto continua como de carga completa, desde la base de datos de origen a la base de datos de destino. AWS DMS también proporciona supervisión y registro de la migración en tiempo real, lo que le ayudará a identificar y resolver cualquier problema que pueda provocar un tiempo de inactividad.

Cuando replique cambios con AWS DMS, debe especificar una hora o un número de cambio del sistema (SCN) como punto de partida para leer los cambios de los registros de la base de datos. Es crucial mantener estos registros accesibles en el servidor durante un periodo de tiempo determinado (recomendamos 15 días) para garantizar que AWS DMS tenga acceso a estos cambios.

Requisitos previos y limitaciones

Requisitos previos

- Una base de datos de Amazon RDS para Oracle aprovisionada en su entorno de la nube de AWS como base de datos de destino. Para obtener instrucciones, consulte la Documentación de Amazon RDS.
- Una EnterpriseOne base de datos que se ejecuta localmente o en una instancia de Amazon Elastic Compute Cloud (Amazon EC2) en AWS.

  Nota: Este patrón está diseñado para migrar de las instalaciones a AWS, pero se probó con una EnterpriseOne base de datos en una instancia de EC2. Si planea migrar desde su entorno en las instalaciones, debe configurar la conectividad de red adecuada.
- Detalles del esquema. Identifique el esquema de base de datos de Oracle (por ejemplo, el DV920) para el que planea migrar. EnterpriseOne Antes de iniciar el proceso de migración, recopile los siguientes detalles sobre el esquema:
  - Tamaño del esquema
  - La cantidad de objetos por tipo de objeto
  - La cantidad de objetos no válidos

Limitaciones

- Debe crear los esquemas que desee en la base de datos de Amazon RDS para Oracle de destino; AWS DMS no los crea por usted. (La sección Epics describe cómo usar Data Pump para exportar e importar esquemas). El nombre del esquema debe existir ya para la base de datos Oracle de destino. Las tablas del esquema de origen se importan al usuario o al esquema, y AWS DMS utiliza la cuenta del administrador o del sistema para conectarse a la instancia de destino. Para migrar varios esquemas, puede crear varias tareas de replicación. También puede migrar datos a diferentes esquemas en una instancia de destino. Para ello, utilice las reglas de transformación de esquemas en las asignaciones de tablas de AWS DMS.
- Este patrón se probó con un conjunto de datos de demostración. Le recomendamos que valide la compatibilidad y la personalización de su conjunto de datos.
- Este patrón usa una EnterpriseOne base de datos que se ejecuta en Microsoft Windows. Sin embargo, puede utilizar el mismo proceso con otros sistemas operativos compatibles con AWS DMS.

Arquitectura

El siguiente diagrama muestra un sistema que se ejecuta EnterpriseOne en una base de datos Oracle como base de datos de origen y una base de datos Amazon RDS for Oracle como base de datos de destino. Los datos se exportan desde la base de datos Oracle de origen y se importan a la base de datos Amazon RDS para Oracle de destino mediante Oracle Data Pump, y se replican para las actualizaciones de CDC mediante AWS DMS.

1. Oracle Data Pump extrae los datos de la base de datos de origen y los envía al destino de la base de datos de Amazon RDS para Oracle.
2. Los datos de CDC se envían desde la base de datos de origen a un punto de conexión de origen en AWS DMS.
3. Desde el punto de conexión de origen, los datos se envían a la instancia de replicación de AWS DMS, donde se realiza la tarea de replicación.
4. Una vez completada la tarea de replicación, los datos se envían al punto de conexión de destino en AWS DMS.
5. Desde el punto de conexión de destino, los datos se envían a la instancia de base de datos Amazon RDS para Oracle.

Herramientas

Servicios de AWS

- AWS Database Migration Service (AWS DMS) le permite migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones.
- Amazon Relational Database Service (Amazon RDS) para Oracle ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS.

Otros servicios

- Oracle Data Pump le ayuda a trasladar datos y metadatos entre una base de datos y otra a alta velocidad.

Prácticas recomendadas

Migración de LOBs

Si la base de datos de origen contiene objetos binarios de gran tamaño (LOB) que deben migrarse a la base de datos de destino, AWS DMS ofrece las siguientes opciones:

- Full LOB mode: AWS DMS migra todos los LOB (objetos grandes) de la base de datos de origen a la de destino sin importar el tamaño. Aunque la migración es más lenta que en los otros modos, la ventaja es que los datos no se truncan. Para obtener un mayor rendimiento, puede crear una tarea independiente en la nueva instancia de replicación para migrar las tablas que contienen LOB de más de unos pocos megabytes.
- Modo LOB limitado: usted especifica el tamaño máximo de los datos de la columna LOB, lo que permite a AWS DMS preasignar los recursos y aplicar los LOB en lotes. Si el tamaño de las columnas LOB supera el tamaño especificado en la tarea, AWS DMS trunca los datos y envía advertencias al archivo de registro de AWS DMS. Puede mejorar el rendimiento usando el modo LOB limitado si el tamaño de los datos de LOB se encuentra dentro del tamaño de LOB limitado.
- Modo LOB en línea: puede migrar los LOB sin truncar los datos ni ralentizar el rendimiento de la tarea replicando los LOB pequeños y grandes. En primer lugar, especifique un valor para el parámetro `InlineLobMaxSize`, que sólo está disponible cuando el modo LOB completo está establecido en `true`. La tarea de AWS DMS transfiere los pequeños LOB en línea, lo que resulta más eficiente. A continuación, AWS DMS migra los LOB grandes realizando una búsqueda en

la tabla de origen. Sin embargo, el modo LOB en línea funciona únicamente en la fase de carga completa.

Generación de valores de secuencia

Durante el proceso de AWS DMS CDC, los números de secuencia incrementales no se replican desde la base de datos de origen. Para evitar discrepancias en los valores de secuencia, debe generar el valor de secuencia más reciente del origen para todas las secuencias y aplicarlo a la base de datos Amazon RDS para Oracle de destino.

AWS Secrets Manager

Para ayudarle a gestionar sus credenciales, le recomendamos que siga las instrucciones de la entrada del blog Gestionar sus credenciales de punto de conexión de AWS DMS con AWS Secrets Manager.

Rendimiento

- Instancias de replicación: para obtener orientación sobre cómo elegir el mejor tamaño de instancia, consulte Selección del mejor tamaño para una instancia de replicación en la documentación de AWS DMS.
- Opciones de conectividad: para evitar problemas de latencia, le recomendamos que elija la opción de conectividad adecuada. AWS Direct Connect proporciona el camino más corto a los recursos de AWS, ya que es una conexión dedicada entre los centros de datos corporativos y AWS. Mientras se encuentra en tránsito, el tráfico de red permanece en la red global de AWS y nunca pasa por Internet. Esto reduce la posibilidad de que se produzcan cuellos de botella o aumentos inesperados de la latencia en comparación con el uso de una VPN o de la Internet pública.
- Ancho de banda de la red: para optimizar el rendimiento, compruebe que el rendimiento de la red sea rápido. Si utiliza un túnel VPN entre la base de datos de origen en las instalaciones y AWS DMS, asegúrese de que el ancho de banda sea suficiente para su carga de trabajo.
- Paralelismo de tareas: puede acelerar la replicación de datos cargando varias tablas en paralelo durante la carga completa. Este patrón utiliza puntos de conexión del RDBMS, por lo que esta opción solo se aplica al proceso de carga completa. El paralelismo de las tareas se controla mediante el parámetro `MaxFullLoadSubTasks`, que determina cuántas subtareas a plena carga se ejecutan en paralelo. De forma predeterminada, este parámetro está establecido en 8, lo que significa que ocho tablas (si se seleccionan en el mapeo de tablas) se cargan juntas durante el modo completo. Puede ajustar este parámetro en la sección de configuración de tareas de carga completa del script JSON de la tarea.

- Paralelismo de tablas: AWS DMS también le permite cargar una sola tabla grande mediante varios subprocesos paralelos. Esto resulta especialmente útil para las tablas fuente de Oracle que tienen miles de millones de registros, así como varias particiones y subparticiones. Si la tabla de origen no está particionada, puede usar límites de columna para cargas paralelas.
- Dividir las cargas: al dividir las cargas en varias tareas o instancias de AWS DMS, recuerde los límites de las transacciones al capturar los cambios.

Epics

Utilice Oracle Data Pump para exportar el esquema EnterpriseOne

Tarea	Descripción	Habilidades requeridas
Genere el SCN.	Cuando la base de datos de origen esté activa y la EnterpriseOne aplicación la utilice, inicie la exportación de datos con Oracle Data Pump. En primer lugar, debe generar un número de cambio del sistema (SCN) a partir de la base de datos de origen, tanto para la coherencia de datos durante la exportación con Oracle Data Pump como punto de partida para el CDC en AWS DMS. Para generar el SCN actual a partir de su base de datos de origen, utilice la siguiente instrucción SQL: `SQL> select current_scn` `from v$database;` `CURRENT_SCN` `----------`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`30009727` Guarde el SCN generado. Utilizará el SCN cuando exporte los datos y para crear la tarea de replicación de AWS DMS.	

Tarea	Descripción	Habilidades requeridas
Cree el archivo de parámetros.	Para crear un archivo de parámetros para exportar el esquema, puede usar el siguiente código. `directory=DMS_DATA_PUMP_DIR logfile=export_dms.log dumpfile=export_dms_data.dmp schemas=<schema name> flashback_scn=<SCN from previous command>` Nota: también puede definir su propio DATA_PUMP_DIR mediante los siguientes comandos, en función de sus necesidades. `SQL> CREATE OR REPLACE DIRECTORY DMS_DATA_PUMP_DIR AS '<Directory for dump>'; Directory created.` `SQL> GRANT READ, WRITE ON DIRECTORY DMS_DATA_PUMP_DIR TO SYSTEM; Grant succeeded.`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Exporte el esquema.	Para realizar la exportación, utilice la utilidad expdp como se indica a continuación: C:\Users\Administrator>expdp system/********@<DB Name> PARFILE='<Path to PAR file create above>' Export: Release 19.0.0.0.0 - Production on *** *** ** **:**:** **** Version 19.3.0.0.0 Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved. Connected to: Oracle Database 19c Standard Edition 2 Release 19.0.0.0.0 - Production Starting "SYSTEM"."SYS_EXPORT_SCHEMA_02": system/**********@<DB Name>PARFILE='E:\exp_dms_datapump.par' Processing object type SCHEMA_EXPORT/TABLE/TABLE_DATA Processing object type SCHEMA_EXPORT/TABLE/INDEX/STATISTICS/INDEX_STATISTICS Processing object type SCHEMA_EXPORT/TABL	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	E/STATISTICS/TABLE _STATISTICS Processing object type SCHEMA_EXPORT/STAT ISTICS/MARKER Processing object type SCHEMA_EXPORT/USER Processing object type SCHEMA_EXPORT/ROLE _GRANT Processing object type SCHEMA_EXPORT/DEFA ULT_ROLE Processing object type SCHEMA_EXPORT/TABL ESPACE_QUOTA Processing object type SCHEMA_EXPORT/PRE_ SCHEMA/PROCACT_SCHEMA Processing object type SCHEMA_EXPORT/TABLE/ TABLE Processing object type SCHEMA_EXPORT/TABL E/GRANT/OWNER_GRANT/ OBJECT_GRANT Processing object type SCHEMA_EXPORT/TABLE/ INDEX/INDEX Processing object type SCHEMA_EXPORT/TABLE/ CONSTRAINT/CONSTRAINT . . exported "<Schema Name>"."<Table Name>" 228.9 MB 496397 rows Master table "SYSTEM". "SYS_EXPORT_SCHEMA _02" successfully loaded/unloaded	

Tarea	Descripción	Habilidades requeridas
	`` ********** ********** ********** ********** **** Dump file set for SYSTEM.SYS_EXPORT_ SCHEMA_02 is: E:\DMSDUMP\EXPORT_ DMS_DATA.DMP Job "SYSTEM"."SYS_EXPO RT_SCHEMA_02" successfully completed at *** *** ** **:**:** **** elapsed 0 00:01:57 ```	

Utilice Oracle Data Pump para importar el EnterpriseOne esquema

Tarea	Descripción	Habilidades requeridas
Transfiera el archivo de volcado a la instancia de destino.	Para transferir sus archivos mediante la utilidad `DBMS_FILE_TRANSFER`, necesita crear un enlace de base de datos desde la base de datos de origen a la instancia de Amazon RDS para Oracle. Una vez establecido el enlace, la utilidad le permitirá transferir los archivos de Data Pump directamente a la instancia de Amazon RDS. Como alternativa, puede transferir los archivos de Data Pump a Amazon Simple Storage Service (Amazon S3)	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	y, a continuación, importarl os a la instancia de Amazon RDS para Oracle. Para más información sobre esta opción, consulte la sección Informaci ón adicional. Para crear un enlace de base de datos ORARDSDB que conecte con el usuario principal de Amazon RDS en la instancia de base de datos de destino, ejecute los siguientes comandos en la base de datos de origen: `sqlplus / as sysdba` `SQL*Plus: Release 19.0.0.0.0 on *** *** ** **:**:** **** Version 19.3.0.0.0` `Copyright (c) 1982, 2019, Oracle. All rights reserved.` `Connected to: Oracle Database 19c Standard Edition 2 Release 19.0.0.0.0 Version 19.3.0.0.0` `SQL> create database link orardsdb connect to admin identifie d by "******" using '(DESCRIPTION = (ADDRESS = (PROTOCOL =`	

Tarea	Descripción	Habilidades requeridas
	TCP)(HOST = orcl.**** **.us-east-1.rds.a mazonaws.com)(PORT = 1521))(CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = orcl)))'; Database link created. SQL>	
Pruebe el enlace de la base de datos.	Pruebe el enlace a la base de datos para asegurarse de que puede conectarse a la base de datos de destino de Amazon RDS para Oracle usando `sqlplus`. SQL> select name from v $database@orardsdb; NAME --------- ORCL	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Transfiera el archivo de volcado a la base de datos de destino.	Para copiar el archivo de volcado en la base de datos de Amazon RDS para Oracle, puede utilizar el directorio `DATA_PUMP_DIR` predeterminado o crear su propio directorio mediante el código siguiente, que debe ejecutar en la instancia de Amazon RDS de destino: `exec rdsadmin.rdsadmin_util.create_directory(p_directory_name => 'DMS_TARGET_PUMP_DIR');` `PL/SQL procedure successfully completed.` El siguiente script copia un archivo de volcado denominado `EXPORT_DMS_DATA.DMP` desde la instancia de origen a una base de datos de Amazon RDS para Oracle usando el enlace de la base de datos denominado `orardsdb`. Debe ejecutar el script en la instancia de la base de datos de origen. `BEGIN DBMS_FILE_TRANSFER.PUT_FILE(`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`source_directory_object => 'DMS_DATA_PUMP_DIR', source_file_name => 'EXPORT_DMS_DATA.DMP', destination_directory_object => 'DMS_TARGET_PUMP_DIR', destination_file_name => 'EXPORT_DMS_DATA.DMP', destination_database => 'orardsdb'); END;` `PL/SQL procedure successfully completed.`	
Incluya el archivo de volcado en la base de datos de destino.	Una vez completado el procedimiento PL/SQL, puede incluir el archivo de volcado de datos en la base de datos de Amazon RDS para Oracle mediante el siguiente código: `select * from table (rdsadmin.rds_file_util.listdir(p_directory => 'DMS_TARGET_PUMP_DIR'));`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree usuarios específicos de JDE en la instancia de destino.	Cree un perfil y un rol de JD Edwards mediante estos comandos en la instancia de destino: `SQL> CREATE PROFILE "JDEPROFILE" LIMIT IDLE_TIME 15;` `Profile created.` `SQL> CREATE ROLE "JDE_ROLE";` `Role created.` `SQL> CREATE ROLE "JDEADMIN";` `CREATE ROLE "JDEUSER";` `Role created.` `Role created.` Conceda los permisos necesarios al rol: `SQL> GRANT CREATE ANY SEQUENCE TO JDE_ROLE;` `GRANT DROP ANY SEQUENCE TO JDE_ROLE;` `GRANT CREATE ANY TRIGGER TO JDE_ROLE;` `GRANT DROP ANY TRIGGER TO JDE_ROLE;`	Administrador de base de datos, JDE CNC

Tarea	Descripción	Habilidades requeridas
Cree espacios de tabla en la instancia de destino.	Cree los espacios de tabla necesarios en la instancia de destino mediante los siguientes comandos para los esquemas que intervienen en esta migración: `SQL> CREATE TABLESPACE <Tablespace Name for Tables>;` `Tablespace created.` `SQL> CREATE TABLESPACE <Tablespace Name for Indexes>;` `Tablespace created.`	Administrador de base de datos, JDE CNC

Tarea	Descripción	Habilidades requeridas
Inicie la importación en la base de datos de destino.	Antes de iniciar el proceso de importación, configure los roles, esquemas y espacios de tabla en la base de datos de destino Amazon RDS para Oracle mediante el archivo de volcado de datos. Para realizar la importación, acceda a la base de datos de destino con la cuenta de usuario principal de Amazon RDS y use el nombre de la cadena de conexión del archivo `tnsnames.ora` , que incluye el `tns-entry` de la base de datos Amazon RDS para Oracle. Si es necesario , puede incluir una opción de reasignación para importar el archivo de volcado de datos a un espacio de tabla diferente o con un nombre de esquema diferente. Para iniciar la importación, utilice el siguiente código: `impdp admin@orardsdb directory=DMS_TARGET_PUMP_DIR logfile=import.log dumpfile=EXPORT_DMS_DATA.DMP` Para garantizar una importación correcta, compruebe	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	la ausencia de errores en el archivo de registro de importación y revise detalles como el número de objetos, el número de filas y los objetos no válidos. Si hay algún objeto no válido, repita la compilación. Compare también los objetos de la base de datos de origen y destino para confirmar que coinciden.	

Aprovisione una instancia de replicación de AWS DMS con los puntos de conexión de origen y destino

Tarea	Descripción	Habilidades requeridas
Descargue la plantilla de .	Descargue la plantilla AWS CloudFormation DMS_Instance.yaml para aprovisionar la instancia de replicación de AWS DMS y sus puntos de enlace de origen y destino.	Administrador de la nube, administrador de bases de datos
Inicie la creación de la pila.	1. Inicie sesión en la consola de administración de AWS y abra la CloudFormation consola de AWS en https://console.aws.amazon.com/cloudformation. 2. Seleccione Crear pila. 3. En Specify template (Especificar plantilla), elija Upload a template	Administrador de la nube, Administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	file (Cargar un archivo de plantilla). 4. Seleccione Elegir archivo. 5. Seleccione el archivo `DMS_instance.yaml` . 6. Elija Siguiente.	

Tarea	Descripción	Habilidades requeridas
Especifique los parámetros.	1. En Stack name (Nombre de la pila), ingrese el nombre de la pila. 2. En Parámetros de instancia de AWS DMS, introduzca los siguientes parámetros: • DMS InstanceType: elija la instancia requerida para la instancia de replicación de AWS DMS en función de las necesidades de su empresa. • DMS StorageSize: introduzca el tamaño de almacenamiento de la instancia de AWS DMS, en función del tamaño de la migración. 3. En Configuración de la base de datos Oracle de origen, introduzca los siguientes parámetros: • SourceOracleEndpointID: el nombre del servidor de base de datos Oracle de origen • SourceOracleDatabaseName— El nombre del servicio de base de datos de origen o el ID de sesión (SID), según proceda	Administrador de la nube, Administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	• SourceOracleUserName— El nombre de usuario de la base de datos de origen (el predeterminado `essystem`) • SourceOracledbPassword: la contraseña del nombre de usuario de la base de datos fuente • SourceOracledBPort: el puerto de la base de datos de origen 4. Para Configuración de RDS para bases de datos Oracle, introduzca los siguientes parámetros: • OracleEndpointID de TargetRDS: el punto final de la base de datos RDS de destino • TargetRDS: el nombre de la base de datos de RDS de destino OracleDatabaseName • TargetRS OracleUserName: el nombre de usuario del RDS de destino • TargetRDSOracleDBPassword: la contraseña de RDS de destino	

Tarea	Descripción	Habilidades requeridas
	• TargetOracledBPort: el puerto de la base de datos RDS de destino 5. En Configuración de VPC, subred y grupo de seguridad, introduzca los siguientes parámetros: • VPCID: la VPC de la instancia de replicación • VPC SecurityGroupId: el grupo de seguridad de VPC para la instancia de replicación • DMSSubnet1: la subred de la zona de disponibilidad 1 • DMSSubnet1: la subred de la zona de disponibilidad 2 6. Elija Siguiente.	

Tarea	Descripción	Habilidades requeridas
Cree la pila.	1. En la página Configura r opciones de pila, para Etiquetas, introduzca cualquier valor opcional. 2. Elija Siguiente. 3. En la página Revisar, verifique los detalles y, a continuación, seleccione Enviar. El aprovisionamiento debería completarse en un plazo aproximado de 5 a 10 minutos. Se completa cuando la página de AWS CloudFormation Stacks muestra CREATE_CO MPLETE.	Administrador de la nube, administrador de bases de datos
Configure los puntos de conexión.	1. Abra la consola de AWS DMS en https://console.a ws.amazon.com/dms/v2/. 2. En Administración de recursos, elija Instancias de replicación y, a continuac ión, revise las instancias de replicación. 3. En Administración de recursos, elija Puntos de conexión y, a continuac ión, revise los puntos de conexión.	Administrador de la nube, Administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
Probar la conectividad.	Cuando los puntos de conexión de origen y destino muestren el estado Activo, pruebe la conectividad. Seleccione Ejecutar prueba en cada punto de conexión (origen y destino) para asegurarse de que el estado sea correcto.	Administrador de la nube, Administrador de bases de datos

Crear una tarea de replicación de AWS DMS para la replicación en vivo

Tarea	Descripción	Habilidades requeridas
Crear una tarea de replicación.	Cree la tarea de replicación de AWS DMS siguiendo estos pasos: 1. Abra la consola de AWS DMS en https://console.aws.amazon.com/dms/v2/. 2. En el panel de navegación, en Migrar datos, elija Tarea de migración de bases de datos. 3. En el cuadro Configuración de tareas, para Identificador de tareas, introduzca el identificador de su tarea. 4. En Instancia de replicación, elija la instancia de replicación DMS que creó.	Administrador de la nube, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	5. En Punto de conexión de base de datos de origen, seleccione el punto de conexión de origen. 6. En Punto de conexión de base de datos de destino, seleccione la base de datos de destino Amazon RDS para Oracle. 7. En Tipo de migración, seleccione Replicar solo cambios de datos. Si recibe un mensaje que le indica que debe activar el registro suplementario, siga las instrucciones de la sección Solución de problemas. 8. En el cuadro Configuración de la tarea, seleccione Especificar el número de secuencia de registro. 9. En Número de cambio del sistema, introduzca el SCN de la base de datos Oracle que generó en la base de datos Oracle de origen. 10. Seleccione Activar validación. 11. Elija Habilitar registros. CloudWatch Al activar esta función, puede validar los datos y los registros de Amazon	

Tarea	Descripción	Habilidades requeridas
	para revisar CloudWatch los registros de las instancias de replicación de AWS DMS. 12. En Reglas de selección, complete lo siguiente: • Para Esquema, elija Introducir un esquema. • En Nombre del esquema, introduzca el nombre del esquema JDE (por ejemplo: DV920). • En Nombre de la tabla, introduzca %. • En Acción, elija Incluir. 13. Seleccione Crear tarea. Tras crear la tarea, AWS DMS migra los cambios en curso a la instancia de base de datos de Amazon RDS para Oracle desde el SCN que proporcionó en el modo de inicio de CDC. También puede verificar la migración revisando los CloudWatch registros.	
Repita la tarea de replicación.	Repita los pasos anteriores para crear tareas de replicación para otros esquemas de JD Edwards que formen parte de la migración.	Administrador de la nube, Administrador de bases de datos, administrador de JDE CNC

Valide el esquema de la base de datos de Amazon RDS para Oracle

Tarea	Descripción	Habilidades requeridas
Valide la transferencia de datos.	Una vez iniciada la tarea de AWS DMS, puede consultar la pestaña Estadísticas de tabla en la página Tareas para ver los cambios realizados en los datos. Puede supervisar el estado de la replicación en curso desde la consola, en la página Tareas de migración de bases de datos. Para más información, consulte Validación de datos de AWS DMS	Administrador de la nube, administrador de bases de datos

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Detención de la replicación.	Interrumpa el procedimiento de replicación y detenga los servicios de la aplicación de origen.	Administrador de la nube, Administrador de bases de datos
Inicie la aplicación JD Edwards.	Inicie la aplicación de nivel lógico y de presentación JD Edwards de destino en AWS y diríjala a la base de datos Amazon RDS para Oracle.	Administrador de base de datos, administrador de JDE CNC

Tarea	Descripción	Habilidades requeridas
	Cuando acceda a la aplicación, verá que todas las conexiones se establecen ahora con la base de datos Amazon RDS para Oracle.	
Desactive la base de datos de origen.	Después de confirmar que no hay más conexiones, puede desactivar la base de datos de origen.	Administrador de base de datos

Solución de problemas

Problema	Solución
Recibe un mensaje de advertencia para habilitar el registro adicional en la base de datos de origen para una replicación continua	Introduzca estos comandos para habilitar el registro suplementario: `SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (ALL) COLUMNS;` `SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (PRIMARY KEY) COLUMNS;` `SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (UNIQUE) COLUMNS;` `SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (FOREIGN KEY) COLUMNS;` `SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (PRIMARY KEY) COLUMNS;` `SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (UNIQUE) COLUMNS;`
AWS DMS tiene desactivado el registro suplementario.	El registro suplementario se encuentra desactivado de forma predeterminada en AWS DMS. Para activarlo en un punto de conexión de Oracle de origen:

Problema	Solución
	1. Inicie sesión en la consola de administración de AWS y abra la consola de AWS DMS en https://console.aws.amazon.com/dms/v2/. 2. Elija Puntos de conexión. 3. Elija el punto de conexión de origen de Oracle al que desee agregar el registro . 4. Elija Modificar. 5. Elija Opciones avanzadas y agregue después el código siguiente en el cuadro de texto Atributos de conexión adicionales: `addSupplementalLogging=Y` 6. Elija Modificar.
El registro suplementario no está habilitado en el nivel de CDB.	1. Introduzca este comando: `SQL> alter session set container = CDB$ROOT;` `Session altered.` 2. Repita los pasos para activar el registro suplementario.
Aparece el siguiente mensaje de error: «Falló el punto final de prueba: estado de la aplicació n: 1020912, mensaje de la aplicación: no se admite en el entorno Oracle PDB, no LogMiner se pudo inicializar el punto final».	Si aparece este mensaje de error, puede utilizar Binary Reader en lugar de. LogMiner En Configuración de puntos de conexión, añada esta línea a los atributos de conexión adicionales de la base de datos de origen: `useLogMinerReader=N;useBfile=Y;`

Recursos relacionados

- Introducción a AWS Database Migration Service (AWS DMS)
- Buenas prácticas de AWS Database Migration Service (AWS DMS)
- Migración de bases de datos de Oracle a la nube de AWS
- Referencia de tipo de recurso de AWS Database Migration Service para AWS CloudFormation
- Administre sus credenciales de punto de conexión de AWS DMS con AWS Secrets Manager
- Solución de problemas de las tareas de migración en AWS Database Migration Service (AWS DMS)
- Buenas prácticas de AWS Database Migration Service (AWS DMS)

Información adicional

Transfiera archivos con Amazon S3

Para transferir los archivos a Amazon S3, puede utilizar la CLI de AWS o la consola de Amazon S3. Tras transferir los archivos a Amazon S3, puede usar la instancia de Amazon RDS para Oracle para importar los archivos de Data Pump desde Amazon S3.

Si prefiere transferir el archivo de volcado usando la integración de Amazon S3 como método alternativo, siga estos pasos:

1. Crear un bucket de S3.
2. Exporte los datos de la base de datos de origen utilizando Oracle Data Pump.
3. Suba los archivos de Data Pump al bucket S3.
4. Descargue los archivos de Data Pump desde el bucket de S3 en la base de datos de destino Amazon RDS para Oracle.
5. Realice la importación con los archivos de Data Pump.

Nota: para transferir archivos de datos de gran tamaño entre instancias S3 y RDS, le recomendamos que utilice la función de Aceleración de transferencias de Amazon S3.

Migre una PeopleSoft base de datos de Oracle a AWS mediante AWS DMS

Entorno: producción	Fuente: Oracle PeopleSoft	Destino: Amazon RDS para Oracle
Tipo R: redefinir la plataforma	Carga de trabajo: Oracle	Tecnologías: Migración; bases de datos
Servicios de AWS: AWS DMS; Amazon RDS		

Resumen

Oracle PeopleSoft es una solución de planificación de recursos empresariales (ERP) para procesos de toda la empresa. PeopleSoft tiene una arquitectura de tres niveles: cliente, aplicación y base de datos. PeopleSoft se puede ejecutar en Amazon Relational Database Service (Amazon RDS).

Si migra su base de datos de Oracle a Amazon RDS, Amazon Web Services (AWS) podrá encargarse de las tareas de backup y de la alta disponibilidad, lo que le permitirá concentrarse en el mantenimiento de PeopleSoft la aplicación y su funcionalidad. Para obtener una lista completa de los factores clave a tener en cuenta durante el proceso de migración, consulte Estrategias de migración de bases de datos de Oracle en Recomendaciones de AWS.

Este patrón proporciona una solución para migrar sus bases de datos de Oracle en las instalaciones a Amazon RDS para Oracle mediante Oracle Data Pump con AWS Database Migration Service (AWS DMS) y su característica de captura de datos de cambios (CDC).

Al migrar aplicaciones ERP críticas, como Oracle PeopleSoft, es fundamental minimizar el tiempo de inactividad. AWS DMS minimiza el tiempo de inactividad gracias a su replicación, tanto continua como de carga completa, desde la base de datos de origen a la base de datos de destino. AWS DMS también proporciona supervisión y registro de la migración en tiempo real, lo que le ayudará a identificar y resolver cualquier problema que pueda provocar un tiempo de inactividad.

Al replicar los cambios con AWS DMS, debe especificar una hora o número de cambio de sistema (SCN) como punto de partida para que AWS DMS lea los cambios de los registros de la base de datos. Es fundamental mantener estos registros accesibles en el servidor durante un determinado período de tiempo para asegurar que AWS DMS tenga acceso a estos cambios.

Requisitos previos y limitaciones

Requisitos previos

- Base de datos Amazon RDS para Oracle aprovisionada en su entorno de nube de AWS como base de datos de destino.
- Una PeopleSoft base de datos Oracle que se ejecuta localmente o en Amazon Elastic Compute Cloud (Amazon EC2) en la nube de AWS.

  Nota: Este patrón está diseñado para migrar de las instalaciones a AWS, pero se ha probado con Oracle Database en una instancia de Amazon EC2. Para migrar desde una ubicación en las instalaciones, necesitará configurar la conectividad de red adecuada.
- Detalles del esquema. Al migrar una PeopleSoft aplicación de Oracle a Amazon RDS for Oracle, es necesario identificar qué esquema de base de datos de Oracle (por ejemplo`SYSADM`) se va a migrar. Antes de iniciar el proceso de migración, recopile los siguientes detalles sobre el esquema:
  - Tamaño
  - La cantidad de objetos por tipo de objeto
  - La cantidad de objetos no válidos.

  Esta información ayudará en el proceso de migración.

Limitaciones

- Este escenario se ha probado únicamente con la base de datos PeopleSoft DEMO. No se ha probado con un conjunto de datos grande.

Arquitectura

El siguiente diagrama muestra una instancia que ejecuta una base de datos de Oracle como base de datos de origen y una base de datos Amazon RDS para Oracle como base de datos de destino. Los datos se exportan e importan de la base de datos de Oracle de origen a la base de datos Amazon RDS para Oracle de destino mediante Oracle Data Pump, y los cambios de CDC se replican mediante AWS DMS.

1. El paso inicial consiste en extraer los datos de la base de datos de origen mediante Oracle Data Pump y, a continuación, enviarlos a la base de datos de destino Amazon RDS para Oracle.

2. Los datos se envían desde la base de datos de origen a un punto de conexión de origen en AWS DMS.
3. Desde el punto de conexión de origen, los datos se envían a la instancia de replicación de AWS DMS, donde se realiza la tarea de replicación.
4. Una vez completada la tarea de replicación, los datos se envían al punto de conexión de destino en AWS DMS.
5. Desde el punto de conexión de destino, los datos se envían a la instancia de base de datos Amazon RDS para Oracle.

Herramientas

Servicios de AWS

- AWS Database Migration Service (AWS DMS) le permite migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones.
- Amazon Relational Database Service (Amazon RDS) para Oracle le ayuda a configurar, utilizar y escalar una base de datos relacional de Oracle en la nube de AWS.

Otros servicios

- Oracle Data Pump le ayuda a trasladar datos y metadatos de una base de datos a otra a altas velocidades.

Prácticas recomendadas

Migración de LOBs

Si la base de datos de origen contiene objetos binarios de gran tamaño (LOB) que deben migrarse a la base de datos de destino, AWS DMS ofrece las siguientes opciones:

- Full LOB mode: AWS DMS migra todos los LOB (objetos grandes) de la base de datos de origen a la de destino sin importar el tamaño. Aunque la migración es más lenta, la ventaja es que los datos no se truncan. Para obtener un mayor rendimiento, puede crear una tarea independiente en la nueva instancia de replicación para migrar las tablas que contienen LOB de más de unos pocos megabytes.
- Modo LOB limitado: usted especifica el tamaño máximo de los datos de la columna LOB, lo que permite a AWS DMS preasignar los recursos y aplicar los LOB en lotes. Si el tamaño de las

columnas LOB supera el tamaño especificado en la tarea, AWS DMS trunca los datos y envía advertencias al archivo de registro de AWS DMS. Puede mejorar el rendimiento usando el modo LOB limitado si el tamaño de los datos de LOB se encuentra dentro del tamaño de LOB limitado.

- Modo LOB en línea: puede migrar los LOB sin truncar los datos ni ralentizar el rendimiento de la tarea replicando los LOB pequeños y grandes. En primer lugar, especifique un valor para el InlineLobMaxSize parámetro, que solo estará disponible cuando el modo LOB completo esté establecido en true. La tarea de AWS DMS transfiere los pequeños LOB en línea, lo que resulta más eficiente. A continuación, AWS DMS migra los LOB grandes realizando una búsqueda en la tabla de origen. Sin embargo, el modo LOB en línea funciona únicamente en la fase de carga completa.

Generación de valores de secuencia

Tenga en cuenta que, durante el proceso de captura de datos de cambios con AWS DMS, los números de secuencia progresivos no se replican desde la base de datos de origen. Para evitar discrepancias en los valores de secuencia, debe generar el valor de secuencia más reciente del origen para todas las secuencias y aplicarlo a la base de datos Amazon RDS para Oracle de destino.

Administración de credenciales

Para ayudar a proteger sus recursos de AWS, le recomendamos seguir las prácticas recomendadas de AWS Identity and Access Management (IAM).

Epics

Aprovisione una instancia de replicación de AWS DMS con los puntos de conexión de origen y destino

Tarea	Descripción	Habilidades requeridas
Descargue la plantilla de .	Descargue la CloudFormation plantilla de AWS DMS_Instance.yaml para aprovisionar la instancia de replicación de AWS DMS y sus puntos de enlace de origen y destino.	Administrador de la nube, Administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
Inicie la creación de la pila.	1. En la consola de administración de AWS, elija CloudFormation. 2. Seleccione Crear pila. 3. En Specify template (Especificar plantilla), elija Upload a template file (Cargar un archivo de plantilla). 4. Seleccione Elegir archivo. 5. Seleccione el archivo `DMS_instance.yaml` . 6. Elija Siguiente.	Administrador de la nube, Administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
Especifique los parámetros.	1. En Nombre de la pila, introduzca el nombre de la pila. 2. En Parámetros de instancia de AWS DMS, introduzca los siguientes parámetros: • DMS InstanceType: elija la instancia requerida para la instancia de replicación de AWS DMS en función de las necesidades de su empresa. • DMS StorageSize: introduzca el tamaño de almacenamiento de la instancia de AWS DMS, en función del tamaño de la migración. 3. En Configuración de la base de datos de Oracle de origen, introduzca los siguientes parámetros: • SourceOracleEndpointID: el nombre del servidor de base de datos Oracle de origen • SourceOracleDatabaseName— El nombre del servicio de base de datos de origen o el ID de sesión (SID), según proceda	Administrador de la nube, Administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	• SourceOracleUserName— El nombre de usuario de la base de datos de origen (el predeterminado es sistema) • SourceOracledbPassword: la contraseña del nombre de usuario de la base de datos fuente • SourceOracledBPort: el puerto de la base de datos de origen 4. En Configuración de RDS para bases de datos de Oracle, introduzca los siguientes parámetros: • OracleEndpointID de TargetRDS: el punto final de la base de datos RDS de destino • Nombre de TargetRDS: el nombre de la base de datos de RDS de destino OracleDatabase • Nombre del RDS de destino: el nombre de usuario del RDS de destino OracleUser • TargetRDSOracleDBPassword: la contraseña de RDS de destino	

Tarea	Descripción	Habilidades requeridas
	• TargetOracledBPort: el puerto de la base de datos RDS de destino 5. En Configuración de VPC, subred y grupo de seguridad, introduzca los siguientes parámetros: • VPCID: la VPC de la instancia de replicación • SecurityGroupID de VPC: el grupo de seguridad de VPC de la instancia de replicación • DMSSubnet1: la subred de la zona de disponibilidad 1 • DMSSubnet1: la subred de la zona de disponibilidad 2 6. Elija Siguiente.	

Tarea	Descripción	Habilidades requeridas
Cree la pila.	1. En la página Configura r opciones de pila, para Etiquetas, introduzca cualquier valor opcional. 2. Elija Siguiente. 3. En la página Revisar, verifique los detalles y, a continuación, seleccione Enviar. El aprovisionamiento debería completarse en un plazo aproximado de 5 a 10 minutos. Se completa cuando la página de AWS CloudFormation Stacks muestra CREATE_CO MPLETE.	Administrador de la nube, Administrador de bases de datos
Configure los puntos de conexión.	1. En la consola de administr ación de AWS, elija Database Migration Services. 2. En Administración de recursos, elija Instancias de replicación. 3. En Administración de recursos, elija Puntos de conexión.	Administrador de la nube, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
Probar la conectividad.	Cuando los puntos de conexión de origen y destino muestren el estado Activo, pruebe la conectividad. Seleccione Ejecutar prueba en cada punto de conexión (origen y destino) para asegurarse de que el estado sea correcto.	Administrador de la nube, Administrador de bases de datos

Exporte el PeopleSoft esquema de la base de datos Oracle local mediante Oracle Data Pump

Tarea	Descripción	Habilidades requeridas
Genere el SCN.	Cuando la base de datos de origen esté activa y la aplicación la utilice, inicie la exportación de datos con Oracle Data Pump. En primer lugar, debe generar un número de cambio del sistema (SCN) de la base de datos de origen para garantizar la coherencia de datos durante la exportación con Oracle Data Pump. También servirá como punto de partida para la captura de datos de cambios en AWS DMS. Para generar el SCN actual de la base de datos de origen, introduzca la siguiente instrucción SQL.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`SQL> select name from v $database;` `SQL> select name from v $database;` `NAME` `---------` `PSFTDMO` `SQL> SELECT current_s cn FROM v$database;` `CURRENT_SCN` `-----------` `23792008` Guarde el SCN generado. Lo usará para exportar los datos y crear la tarea de replicación de AWS DMS.	

Tarea	Descripción	Habilidades requeridas
Cree el archivo de parámetros.	Para crear un archivo de parámetros para exportar el esquema, puede usar el siguiente código. `$ cat exp_datapmp.par` `userid=system/*******` `directory=DATA_PUMP_DIR` `logfile=export_dms_sample_user.log` `dumpfile=export_dms_sample_data_%U.dmp` `schemas=SYSADM` `flashback_scn=23792008` Nota: También puede definir su propio `DATA_PUMP_DIR` mediante los siguientes comandos, en función de sus necesidades. `SQL> CREATE OR REPLACE DIRECTORY DATA_PUMP_DIR AS '/opt/oracle/product/19c/dbhome_1/dmsdump/';` `Directory created.` `SQL> GRANT READ, WRITE ON DIRECTORY DATA_PUMP_DIR TO system;` `Grant succeeded.` `SQL>` `SQL> SELECT owner, directory_name, directory_path FROM dba_directories WHERE`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	directory_name='DATA_PUMP_DIR'; OWNER DIRECTORY_NAME DIRECTORY_PATH ---------- ---------- ---------- SYS DATA_PUMP_DIR /opt/oracle/product/19c/dbhome_1/dmsdump/	

Tarea	Descripción	Habilidades requeridas
Exporte el esquema.	Realice la exportación con la utilidad `expdp`. `$ expdp parfile=e xp_datapmp.par .... Transferring the dump file with DBMS_FILE _TRANSFER to Target: . . exported "SYSADM". "PS_XML_TEMPLT_LNG" 6.320 KB 0 rows . . exported "SYSADM". "PS_XML_TEMPLT_LNK" 6.328 KB 0 rows . . exported "SYSADM". "PS_XML_XLATDEF_LNG" 6.320 KB 0 rows . . exported "SYSADM". "PS_XML_XLATITM_LNG" 7.171 KB 0 rows . . exported "SYSADM". "PS_XPQRYRUNCNTL" 7.601 KB 0 rows . . exported "SYSADM". "PS_XPQRYRUNPARM" 7.210 KB 0 rows . . exported "SYSADM". "PS_YE_AMOUNTS" 9.351 KB 0 rows . . exported "SYSADM". "PS_YE_DATA" 16.58 KB 0 rows . . exported "SYSADM". "PS_YE_EE" 6.75 KB 0 rows . . exported "SYSADM". "PS_YE_W2CP_AMOUNTS" 9.414 KB 0 rows`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	. . exported "SYSADM". "PS_YE_W2CP_DATA" 20.94 KB 0 rows . . exported "SYSADM". "PS_YE_W2C_AMOUNTS" 10.27 KB 0 rows . . exported "SYSADM". "PS_YE_W2C_DATA" 20.95 KB 0 rows . . exported "SYSADM". "PS_ZBD_JOBCODE_TBL" 14.60 KB 0 rows . . exported "SYSADM". "PTGRANTTBL" 5.468 KB 0 rows Master table "SYSTEM". "SYS_EXPORT_SCHEMA _01" successfully loaded/unloaded ** Dump file set for SYSTEM.SYS_EXPORT_ SCHEMA_01 is: /opt/oracle/pr oduct/19c/dbhome_1 /dmsdump/export_dm s_sample_data_01.dmp Job "SYSTEM"."SYS_EXPO RT_SCHEMA_01" successfully completed at Mon Dec 19 20:13:57 2022 elapsed 0 00:38:22	

Importe el PeopleSoft esquema a la base de datos Amazon RDS for Oracle mediante Oracle Data Pump

Tarea	Descripción	Habilidades requeridas
Transfiera el archivo de volcado a la instancia de destino.	Para transferir sus archivos mediante `DBMS_FILE_TRANSFER`, debe crear un enlace de base de datos desde la base de datos de origen a la instancia de Amazon RDS para Oracle. Una vez establecido el enlace, la utilidad le permitirá transferir los archivos de Data Pump directamente a la instancia de RDS. Como alternativa, puede transferir los archivos de Data Pump a Amazon Simple Storage Service (Amazon S3) y, a continuación, importarlos a la instancia de Amazon RDS para Oracle. Para más información sobre esta opción, consulte la sección Información adicional. Para crear un enlace de base de datos `ORARDSDB` que conecte con el usuario principal de Amazon RDS en la instancia de base de datos de destino, ejecute los siguientes comandos en la base de datos de origen.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`$sqlplus / as sysdba` `$ SQL> create database link orardsdb connect to admin identified by "*****" using '(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = testpsft.*******.us-west-2.rds.amazonaws.com)(PORT = 1521))(CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = orcl)))';` `Database link created.`	
Pruebe el enlace de la base de datos.	Pruebe el enlace de la base de datos para asegurarse de que puede conectarse mediante sqlplus a la base de datos de destino de Amazon RDS para Oracle. `SQL>` `SQL> select name from v$database@orardsdb;` `NAME` `---------` `ORCL` `SQL>`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Transfiera el archivo de volcado a la base de datos de destino.	Para copiar el archivo de volcado a la base de datos de Amazon RDS para Oracle, puede usar el directorio predeterminado `DATA_PUMP_DIR` o bien crear su propio directorio con el siguiente código. `exec rdsadmin.rdsadmin_util.create_directory(p_directory_name => 'TARGET_PUMP_DIR') ;` El siguiente script copia un archivo de volcado denominado `export_dms_sample_data_01.dmp` desde la instancia de origen a una base de datos de Amazon RDS para Oracle usando el enlace de la base de datos denominado `orardsdb`. `$ sqlplus / as sysdba SQL> BEGIN DBMS_FILE_TRANSFER .PUT_FILE( source_directory_object => 'DATA_PUMP_DIR', source_file_name => 'export_dms_sample_data_01.dmp',`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`destination_directory _object => 'TARGET_P UMP_DIR'', destination_file_name => 'export_dms_sample _data_01.dmp', destination_database => 'orardsdb' ); END; / PL/SQL procedure successfully completed .`	
Incluya el archivo de volcado en la base de datos de destino.	Una vez completado el procedimiento PL/SQL, puede incluir el archivo de volcado de datos en la base de datos de Amazon RDS para Oracle mediante el siguiente código. `SQL> select * from table (rdsadmin.rds_file _util.listdir(p_di rectory => 'TARGET_P UMP_DIR'));`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Inicie la importación en la base de datos de destino.	Antes de iniciar el proceso de importación, configure los roles, esquemas y espacios de tabla en la base de datos de destino Amazon RDS para Oracle mediante el archivo de volcado de datos. Para realizar la importación, acceda a la base de datos de destino con la cuenta de usuario maestra de Amazon RDS y use el nombre de la cadena de conexión del archivo `tnsnames.ora` , que incluye el `tns-entry` de la base de datos Amazon RDS para Oracle. Si es necesario , puede incluir una opción de reasignación para importar el archivo de volcado de datos a un espacio de tabla diferente o con un nombre de esquema diferente. Para iniciar la importación, utilice el siguiente código. `impdp admin@orardsdb directory=TARGET_PUMP_DIR logfile=import.log dumpfile=export_dms_sample_data_01.dmp`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	Para garantizar una importación correcta, compruebe la ausencia de errores en el archivo de registro de importación y revise detalles como el número de objetos, el número de filas y los objetos no válidos. Si hay algún objeto no válido, repita la compilación. Compare también los objetos de la base de datos de origen y destino para confirmar que coinciden.	

Cree una tarea de replicación de AWS DMS usando CDC para realizar la replicación en vivo

Tarea	Descripción	Habilidades requeridas
Crear una tarea de replicación.	Cree la tarea de replicación de AWS DMS siguiendo estos pasos: 1. En la consola de AWS DMS, en Conversión y migración, seleccione Tarea de migración de base de datos. 2. En Configuración de tareas, en Identificador de tareas, introduzca su identificador de tarea. 3. En Instancia de replicación, elija la instancia de replicación DMS que creó.	Administrador de la nube, Administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	4. En Punto de conexión de base de datos de origen, seleccione el punto de conexión de origen. 5. En Punto de conexión de base de datos de destino, seleccione la base de datos de destino Amazon RDS para Oracle. 6. En Tipo de migración, seleccione Replicar solo cambios de datos. Si recibe un mensaje en el que se indica que es necesario activar el registro adicional , siga las instrucciones de la sección Información adicional. 7. En Configuración de tarea, seleccione Especificar número de secuencia de registro. 8. En Número de cambio del sistema, introduzca el SCN de la base de datos de Oracle que generó en la base de datos de Oracle de origen. 9. Seleccione Activar validación. 10. Seleccione Habilitar CloudWatch registros.	

Tarea	Descripción	Habilidades requeridas
	Al activar esta función, puede validar los datos y los registros de Amazon para revisar CloudWatch los registros de las instancias de replicación de AWS DMS. 11. En Reglas de selección, complete lo siguiente: • Para Esquema, elija Introducir un esquema. • En Nombre del esquema, introduzca SYSADM. • En Nombre de la tabla, introduzca %. • En Acción, elija Incluir. 12. En Reglas de transformación, complete lo siguiente: • En Destino, elija Tabla. • Para Nombre de esquema, elija Introducir un esquema. • En Nombre del esquema, introduzca SYSADM. • En Acción, seleccione Cambiar nombre a. 13. Seleccione Crear tarea. Tras crear la tarea, se migra el CDC a la instancia de base de datos Amazon RDS para	

Tarea	Descripción	Habilidades requeridas
	Oracle desde el SCN que proporcionó en el modo de inicio de CDC. También puede verificarlos revisando los CloudWatch registros.	

Valide el esquema de la base de datos de Amazon RDS para Oracle

Tarea	Descripción	Habilidades requeridas
Valide la transferencia de datos.	Una vez iniciada la tarea de AWS DMS, puede consultar la pestaña Estadísticas de tabla en la página Tareas para ver los cambios realizados en los datos. Puede supervisar el estado de la replicación en curso desde la consola, en la página Tareas de migración de bases de datos. Para más información, consulte Validación de datos de AWS DMS	Administrador de la nube, Administrador de bases de datos

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Detención de la replicación.	Interrumpa el procedimiento de replicación y detenga los	Administrador de la nube, Administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	servicios de la aplicación de origen.	
Lanza el nivel PeopleSoft medio.	Lance la aplicación de nivel PeopleSoft medio de destino en AWS y diríjala a la base de datos Amazon RDS for Oracle migrada recientemente. Cuando acceda a la aplicación, verá que todas las conexiones de la aplicación se establecen ahora con la base de datos Amazon RDS para Oracle.	DBA, administrador PeopleSoft
Desactive la base de datos de origen.	Tras haber confirmado que no hay más conexiones a la base de datos de origen, puede desactivarla.	Administrador de base de datos

Recursos relacionados

- Introducción a AWS Database Migration Service (AWS DMS)
- Buenas prácticas de AWS Database Migration Service (AWS DMS)
- Migración de bases de datos de Oracle a la nube de AWS

Información adicional

Cómo transferir archivos con Amazon S3

Para transferir los archivos a Amazon S3, puede utilizar la CLI de AWS o la consola de Amazon S3. Tras transferir los archivos a Amazon S3, puede usar la instancia de Amazon RDS para Oracle para importar los archivos de Data Pump desde Amazon S3.

Si prefiere transferir el archivo de volcado usando la integración de Amazon S3 como método alternativo, siga estos pasos:

1. Cree un bucket de S3.
2. Exporte los datos de la base de datos de origen utilizando Oracle Data Pump.
3. Suba los archivos de Data Pump al bucket de S3.
4. Descargue los archivos de Data Pump desde el bucket de S3 en la base de datos de destino Amazon RDS para Oracle.
5. Realice la importación con los archivos de Data Pump.

Nota: Para transferir archivos de datos de gran tamaño entre instancias de S3 y RDS, se recomienda usar la característica Amazon S3 Transfer Acceleration.

Active el registro adicional

Si recibe un mensaje de advertencia solicitando habilitar el registro adicional en la base de datos de origen para la replicación continua, siga estos pasos.

```
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (ALL) COLUMNS;
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (PRIMARY KEY) COLUMNS;
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (UNIQUE) COLUMNS;
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (FOREIGN KEY) COLUMNS;
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (PRIMARY KEY) COLUMNS
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (UNIQUE) COLUMNS;
```

Migrar una base de datos MySQL en las instalaciones a Amazon RDS para MySQL

Documento creado por Lorenzo Mota (AWS)

Entorno: PoC o piloto	Origen: Base de datos MySQL en las instalaciones	Destino: Amazon RDS para MySQL
Tipo R: redefinir la plataforma	Carga de trabajo: código abierto	Tecnologías: Migración; bases de datos
Servicios de AWS: Amazon RDS		

Resumen

Este patrón proporciona una guía para migrar una base de datos MySQL en las instalaciones a Amazon Relational Database Service (Amazon RDS) para MySQL. El patrón analiza el uso del AWS Database Migration Service (AWS DMS) o de herramientas nativas de MySQL, como mysqldbcopy y mysqldump, para una migración completa de bases de datos. Este patrón está pensado principalmente para administradores de bases de datos y arquitectos de soluciones. Se puede usar en proyectos pequeños o grandes como un procedimiento de prueba (recomendamos al menos un ciclo de prueba) o como procedimiento de migración definitiva.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos MySQL de origen en un centro de datos en las instalaciones

Limitaciones

- Límite de tamaño de la base de datos: 64 TB

Versiones de producto

- Versiones de MySQL 5.5, 5.6, 5.7, 8.0. Para ver la lista actualizada de versiones compatibles, consulte MySQL en Amazon RDS en la documentación de AWS. Si utiliza AWS DMS, consulte también Using a MySQL-Compatible Database as a Target for AWS DMS (Uso de una base de datos compatible con MySQL como destino para las versiones de AWS DMS) para conocer las versiones de MySQL compatibles actualmente con AWS DMS.

Arquitectura

Pila de tecnología de origen

- Una base de datos MySQL en las instalaciones

Pila de tecnología de destino

- Una instancia de base de datos de Amazon RDS que ejecute MySQL

Arquitectura de destino

En el diagrama siguiente se muestra la implementación de Amazon RDS para MySQL en el destino tras la migración.

Arquitectura de migración de datos de AWS

Uso de AWS DMS:

El diagrama siguiente muestra la arquitectura de migración de datos cuando se utiliza AWS DMS para enviar cambios completos e incrementales hasta la transición. La conexión de red de las instalaciones a AWS depende de sus requisitos y no se incluye en el alcance de este patrón.

Uso de herramientas MySQL nativas:

El diagrama siguiente muestra la arquitectura de migración de datos cuando se utilizan herramientas nativas de MySQL. Los archivos de volcado de exportación se copian en Amazon Simple Storage Service (Amazon S3) y se importan a la base de datos de Amazon RDS para MySQL en AWS antes de la transición. La conexión de red de las instalaciones a AWS depende de sus requisitos y no se incluye en el alcance de este patrón.

Notas:

- Según los requisitos de tiempo de inactividad y el tamaño de la base de datos, el uso de AWS DMS o de una herramienta de captura de datos de cambios (CDC) minimiza el tiempo de transición. AWS DMS puede ayudar a reducir al mínimo el tiempo de transición hasta el nuevo destino (normalmente en minutos). Una estrategia fuera de línea con mysqldump o mysqldbcopy puede ser suficiente si el tamaño de la base de datos y la latencia de la red permiten un período breve. (Recomendamos efectuar pruebas para obtener un tiempo aproximado).
- Por lo general, una estrategia de CDC como AWS DMS requiere más supervisión y complejidad que las opciones fuera de línea.

Herramientas

- Servicios de AWS: AWS Database Migration Service (AWS DMS) ayuda a migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en las instalaciones y en la nube. Para obtener información sobre las bases de datos de origen y destino de MySQL compatibles con AWS DMS, consulte Migrating MySQL-Compatible Databases to AWS (Migración de bases de datos compatibles con MySQL a AWS). Si su base de datos de origen no es compatible con AWS DMS, debe elegir otro método para migrar los datos.
- Herramientas nativas de MySQL: mysqldbcopy y mysqldump
- Herramientas de terceros: Percona XtraBackup

Epics

Planificar la migración

Tarea	Descripción	Habilidades requeridas
Valide las versiones de las bases de datos.	Valide las versiones de las bases de datos de origen y de destino.	Administrador de base de datos
Identifique los requisitos de hardware.	Identifique los requisitos de hardware del servidor de destino.	Administrador de base de datos, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Identifique los requisitos de almacenamiento.	Identifique los requisitos de almacenamiento (como el tipo y la capacidad de almacenamiento) de la base de datos de destino.	Administrador de base de datos, administrador de sistemas
Seleccione el tipo de instancia.	Seleccione el tipo de instancia de destino en función de la capacidad, las características de almacenamiento y las características de red.	Administrador de base de datos, administrador de sistemas
Identifique los requisitos de acceso a la red.	Identifique requisitos de seguridad para acceder a la red de las bases de datos de origen y destino.	Administrador de base de datos, administrador de sistemas
Identifique los objetos no compatibles.	Identifique los objetos no compatibles (si los hay) y determine el esfuerzo de migración.	Administrador de base de datos
Identifique las dependencias.	Identifique cualquier dependencia en las bases de datos remotas.	Administrador de base de datos
Determine la estrategia de migración de la aplicación.	Determine la estrategia para migrar las aplicaciones cliente.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Configure la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC).	Configure las tablas de enrutamiento, las puertas de enlace de Internet, las puertas de enlace NAT y las subredes. Para obtener más informaci ón, consulte VPC and Amazon RDS en la documentación de Amazon RDS.	Administrador de sistemas
Cree los grupos de seguridad.	Configure los puertos y los rangos de CIDR o las IP específicas en función de sus requisitos. El puerto predeterm inado para MySQL es el 3306. Para obtener más información, consulte Controlling access with security groups (Control de acceso con grupos de seguridad) en la documenta ción de Amazon RDS.	Administrador de sistemas
Configure e inicie una instancia de base de datos de Amazon RDS para MySQL.	Para obtener instrucciones, consulte Creating an Amazon RDS DB instance (Crear una instancia de base de datos de Amazon RDS) en la documentación de Amazon RDS. Compruebe si hay versiones compatibles.	Administrador de sistemas

Migrar datos: opción 1 (con herramientas nativas)

Tarea	Descripción	Habilidades requeridas
Utilice las herramien tas nativas de MySQL o herramientas de terceros para migrar los objetos y datos de la base de datos.	Para obtener instrucciones, consulte la documentación de las herramientas de MySQL, como mysqldbcopy, mysqldump y Percona (para la migración física). XtraBackup Para obtener más información sobre las opciones, consulte la entrada del blog Opciones de migración de MySQL a Amazon RDS para MySQL o Amazon Aurora MySQL.	Administrador de base de datos

Migrar datos: opción 2 (con AWS DMS)

Tarea	Descripción	Habilidades requeridas
Migrar datos con AWS DMS.	Para obtener instrucciones, consulte la AWS DMS documentation (Document ación de AWS DMS).	Administrador de base de datos

Llevar a cabo las tareas preliminares antes de la transición

Tarea	Descripción	Habilidades requeridas
Corrija cualquier discrepancia en el recuento de objetos.	Recopile los recuentos de objetos de la base de datos de origen y de la nueva base de datos de destino. Corrija	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	cualquier discrepancia en la base de datos objetivo.	
Compruebe las dependencias.	Compruebe si las dependencias (los enlaces) con destino y origen en otras bases de datos son válidas y funcionan según lo previsto.	Administrador de base de datos
Efectúe pruebas.	Si se trata de un ciclo de pruebas, lleve a cabo pruebas de consulta, recopile métricas y solucione los problemas.	Administrador de base de datos

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Cambie a la base de datos de destino.	Cambie las aplicaciones cliente a la nueva infraestructura.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas
Proporcione soporte para las pruebas.	Proporcione soporte para las pruebas de aplicaciones funcionales.	Administrador de base de datos

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cierre los recursos.	Cierre los recursos temporales de AWS que creó para la migración.	Administrador de base de datos, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Valide los documentos del proyecto.	Revise y valide los documentos del proyecto.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas
Recopile métricas.	Recopile métricas como el tiempo de migración, el porcentaje de esfuerzo manual frente al automatizado, el ahorro de costos, etc.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas
Cerrar el proyecto.	Cerrar el proyecto y enviar comentarios.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas
Reitre de servicio la base de datos de origen.	Una vez completadas todas las tareas de migración y transición, retire la base de datos en las instalaciones.	Administrador de base de datos, administrador de sistemas

Recursos relacionados

Referencias

- Estrategia de migración para bases de datos relacionales
- Sitio web de AWS DMS
- Documentación de AWS DMS
- Documentación de Amazon RDS
- Precios de Amazon RDS
- VPC y Amazon RDS
- Implementaciones Multi-AZ de Amazon RDS
- Migre bases de datos MySQL locales a Aurora MySQL mediante Percona, XtraBackup Amazon EFS y Amazon S3

Tutoriales

- Introducción a AWS DMS
- Introducción a Amazon RDS

Migración de una base de datos de Microsoft SQL Server en las instalaciones a Amazon RDS para SQL Server

Creado por Henrique Lobao (AWS), Jonathan Pereira Cruz (AWS) y Vishal Singh (AWS)

Entorno: PoC o piloto	Origen: Microsoft SQL Server	Destino: Amazon RDS para SQL Server
Tipo R: redefinir la plataforma	Carga de trabajo: Microsoft	Tecnologías: migración; bases de datos
Servicios de AWS: Amazon RDS		

Resumen

Este patrón proporciona una guía para migrar una base de datos de Microsoft SQL Server en las instalaciones a Amazon Relational Database Service (Amazon RDS) para SQL Server. Describe dos opciones de migración: utilizar AWS Data Migration Service (AWS DMS) o utilizar herramientas nativas de Microsoft SQL Server como Copy Database Wizard.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos de origen Microsoft SQL Server en un centro de datos en las instalaciones

Limitaciones

- Límite de tamaño de la base de datos: 16 TB

Versiones de producto

- Las versiones 2014 a 2019 de SQL Server para las ediciones Enterprise, Standard, Workgroup y Developer. Para ver la lista actualizada de versiones y características compatibles, consulte

Microsoft SQL Server en Amazon RDS en la documentación de AWS. Si utiliza AWS DMS, consulte también Uso de una base de datos de Microsoft SQL Server como destino para AWS DMS para conocer las versiones de SQL Server compatibles con AWS DMS.

Arquitectura

Pila de tecnología de origen

- Base de datos de Microsoft SQL Server en las instalaciones

Pila de tecnología de destino

- Instancia de base de datos de Amazon RDS para SQL Server

Arquitectura de origen y destino

Uso de AWS DMS:

Uso de herramientas nativas de SQL Server:

Herramientas

- AWS DMS admite varios tipos de bases de datos de origen y destino. Para obtener más información, consulte AWS DMS Step-by-Step Walkthroughs (Guías paso a paso de AWS DMS) Si AWS DMS no es compatible con la base de datos de origen, seleccione otro método para migrar los datos.
- Las Herramientas nativas de Microsoft SQL Server incluyen copia de seguridad y restauración, Copy Database Wizard y la función de copiar y adjuntar bases de datos.

Epics

Planificar la migración

Tarea	Descripción	Habilidades requeridas
Validar la versión y el motor de la base de datos de origen y de destino.		Administrador de base de datos
Identifique los requisitos de hardware de la instancia del servidor de destino.		Administrador de base de datos, administrador de sistemas
Identificar los requisitos de almacenamiento (el tipo y la capacidad de almacenam iento).		Administrador de base de datos, administrador de sistemas
Elegir el tipo de instancia correcto en función de la capacidad, las características de almacenamiento y las características de la red.		Administrador de base de datos, administrador de sistemas
Identificar los requisitos de seguridad del acceso a la red para las bases de datos de origen y destino.		Administrador de base de datos, administrador de sistemas
Identificar la estrategia de migración de aplicaciones.		Administrador de base de datos, administrador de sistemas

Configure la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC).		Administrador de sistemas
Creación de los grupos de seguridad.		Administrador de sistemas
Configurar e iniciar una instancia de base de datos de Amazon RDS.		Administrador de base de datos, administrador de sistemas

Migrar datos: opción 1

Tarea	Descripción	Habilidades requeridas
Utilice las herramientas nativas de SQL Server o herramientas de terceros para migrar los objetos y datos de la base de datos.		Administrador de base de datos

Migrar datos: opción 2

Tarea	Descripción	Habilidades requeridas
Migrar datos con AWS DMS.		Administrador de base de datos

Migrar la aplicación

Tarea	Descripción	Habilidades requeridas
Seguir la estrategia de migración de aplicaciones.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Cambiar los clientes de la aplicación a la nueva infraestructura.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cerrar los recursos temporales de AWS.		Administrador de base de datos, administrador de sistemas
Revise y valide los documentos del proyecto.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas
Recopile métricas como el tiempo de migración, el porcentaje de esfuerzo manual frente al automatizado y el ahorro de costos.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Cerrar el proyecto y enviar comentarios.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Recursos relacionados

Referencias

- Implementación de Microsoft SQL Server en Amazon Web Services
- Sitio web de AWS DMS
- Precios de Amazon RDS
- Productos de Microsoft en AWS
- Licencias de Microsoft en AWS
- Microsoft SQL Server en AWS
- Uso de la autenticación de Windows con una instancia de base de datos de Microsoft SQL Server
- Implementaciones de zonas de disponibilidad múltiple de Amazon RDS

Tutoriales y videos

- Introducción a AWS DMS
- Introducción a Amazon RDS
- AWS DMS (vídeo)
- Amazon RDS (vídeo)

Migre datos de Microsoft Azure Blob a Amazon S3 mediante Rclone

Creado por Suhas Basavaraj (AWS), Aidan Keane (AWS) y Corey Lane (AWS)

Entorno: PoC o piloto	Origen: contenedor de almacenamiento de Microsoft Azure	Destino: bucket de Amazon S3
Tipo R: redefinir la plataforma	Carga de trabajo: Microsoft	Tecnologías: migración, almacenamiento y respaldo
Servicios de AWS: Amazon S3		

Resumen

Este patrón describe cómo usar Rclone para migrar datos del almacenamiento de objetos Blob de Microsoft Azure a un bucket de Amazon Simple Storage Service (Amazon S3). Puede usar este patrón para realizar una migración única o una sincronización continua de los datos. Rclone es un programa de línea de comandos escrito en Go. Se usa para mover datos a través de diversas tecnologías de almacenamiento de los proveedores de la nube.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Datos almacenados en el servicio de contenedor Blob de Azure

Arquitectura

Pila de tecnología de origen

- Contenedor de almacenamiento Blob de Azure

Pila de tecnología de destino

- Bucket S3 de Amazon
- Instancia de Linux de Amazon Elastic Compute Cloud (Amazon EC2)

Arquitectura

Herramientas

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Rclone es un programa de línea de comandos de código abierto inspirado en rsync. Se usa para administrar archivos en numerosas plataformas de almacenamiento en la nube.

Prácticas recomendadas

Al migrar datos de Azure a Amazon S3, tenga en cuenta estas consideraciones para evitar costos innecesarios o lentitud en la velocidad de transferencia:

- Cree su infraestructura de AWS en la misma región geográfica que la cuenta de almacenamiento de Azure y el contenedor Blob, por ejemplo, en la región de AWS `us-east-1` (Virginia del Norte) y la región de Azure `East US`.
- Evite usar puerta de enlace NAT si es posible, ya que genera tarifas de transferencia de datos tanto para el ancho de banda de entrada como para el de salida.
- Use un punto de conexión de puerta de enlace VPC para Amazon S3 a fin de aumentar el rendimiento.
- Considere la posibilidad de usar una instancia EC2 basada en el procesador AWS Graviton2 (ARM) para reducir el coste y aumentar el rendimiento en comparación con las instancias x86 de Intel. Rclone presenta compilación cruzada y proporciona un binario ARM precompilado.

Epics

Prepare los recursos en la nube de AWS y Azure

Tarea	Descripción	Habilidades requeridas
Prepare un bucket de S3 de destino.	Cree un nuevo bucket de S3 en la región de AWS correspondiente, o bien elija un bucket existente como destino de los datos que desee migrar.	Administrador de AWS
Cree un rol de instancia IAM para Amazon EC2.	Cree un nuevo rol de AWS Identity and Access Management (IAM) para Amazon EC2. Este rol proporciona a la instancia EC2 acceso de escritura al bucket de S3 de destino.	Administrador de AWS
Adjunte una política al rol de la instancia de IAM.	Use la consola de IAM o la interfaz de la línea de comandos de AWS (AWS CLI) para crear una política en línea para el rol de instancia EC2 que permita obtener permisos de acceso de escritura al bucket de S3 de destino. Para un ejemplo de política, consulte la sección Información adicional.	Administrador de AWS
Lanzar una instancia EC2.	Lance una instancia EC2 de Amazon Linux 2 configurada para usar el rol de servicio de IAM recién creado. Esta instancia también necesitar	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	á acceder a los puntos de conexión de la API pública de Azure a través de Internet. Nota: considere la posibilidad de usar instancias EC2 basadas en AWS Graviton para reducir los costos. Rclone proporciona binarios compilados en ARM.	
Cree una entidad principal de servicio de Azure AD.	Use la CLI de Azure para crear una entidad principal de servicio de Azure Active Directory (Azure AD) con acceso de solo lectura al contenedor de almacenamiento Blob de Azure de origen. Para obtener instrucciones, consulte la sección Información adicional. Guarde estas credenciales en la instancia EC2, en la ubicación `~/azure-principal.json` .	Administrador de la nube, Azure

Instalar y configurar Rclone

Tarea	Descripción	Habilidades requeridas
Descargar e instalar Rclone.	Descargue e instale el programa de línea de comandos Rclone. Para instrucciones sobre la instalación, consulte la documentación de instalación de Rclone.	AWS general, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Configure Rclone.	Copie el siguiente archivo de ejemplo `rclone.conf` . Sustituya `AZStorageAccount` por el nombre de su cuenta de Azure Storage y `us-east-1` por la región de AWS en la que se encuentra su bucket de S3. Guarde este archivo en la ubicación `~/.config/rclone/rclone.conf` de su instancia EC2. `[AZStorageAccount]` `type = azureblob` `account = AZStorageAccount` `service_principal_file = azure-principal.json` `[s3]` `type = s3` `provider = AWS` `env_auth = true` `region = us-east-1`	AWS general, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Verifique la configuración de Rclone.	Para confirmar que Rclone está configurado y que los permisos funcionan correctamente, compruebe que Rclone puede analizar el archivo de configuración y que los objetos del contenedor Blob de Azure y del bucket de S3 sean accesibles. Consulte a continuación algunos ejemplos de comandos de validación. • Enumere los controles remotos configurados en el archivo de configuración. Esto garantizará que el archivo de configuración se esté analizando correctamente. Revise el resultado para asegurarse de que coincide con su archivo `rclone.conf` . `rclone listremotes` `AZStorageAccount:` `s3:` • Enumere los contenedores Blob de Azure en la cuenta configurada. Sustituya `AZStorageAccount` por el nombre de la cuenta de almacenamiento que ha usado en el archivo `rclone.conf` .	AWS general, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	`rclone lsd AZStorage Account:` `2020-04-29 08:29:26 docs` • Enumere los archivos del contenedor Blob de Azure. Sustituya los documento s de este comando por un nombre de contenedor de Blob real en su cuenta de almacenamiento de Azure. `rclone ls AZStorage Account:docs` `824884 administr ator-en.a4.pdf` • Enumere los buckets en su cuenta de AWS. `[root@ip-10-0-20-157 ~]# rclone lsd s3:` `2022-03-07 01:44:40 examplebu cket-01` `2022-03-07 01:45:16 examplebu cket-02` `2022-03-07 02:12:07 examplebu cket-03` • Enumere los archivos en el bucket de S3.	

Tarea	Descripción	Habilidades requeridas
	`[root@ip-10-0-20-157 ~]# rclone ls s3:examplebucket-01` `template0.yaml` `template1.yaml`	

Migre los datos con Rclone

Tarea	Descripción	Habilidades requeridas
Migre los datos de sus contenedores.	Ejecute los comandos de Rclone copy o sync. Ejemplo: copy Este comando copia datos del contenedor Blob de Azure de origen al bucket de S3 de destino. `rclone copy AZStorageAccount:blob-container s3:examplebucket-01` Ejemplo: sync Este comando sincroniza los datos entre el contenedor Blob de Azure de origen y el bucket de S3 de destino. `rclone sync AZStorageAccount:blob-conta`	AWS general, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	`iner s3:exampl ebucket-01` Importante: al usar el comando sync, los datos que no estén en el contenedor de origen se eliminarán del bucket S3 de destino.	
Sincronice sus contenedores.	Una vez completada la copia inicial, ejecute el comando de Rclone sync para continuar con la migración. Solo se copiarán los archivos nuevos que no estén ya en el bucket de S3 de destino.	AWS general, administrador de la nube
Compruebe que los datos se hayan migrado correctamente.	Para comprobar que los datos se han copiado correctamente en el bucket de S3 de destino, ejecute los comandos lsd y ls de Rclone.	AWS general, administrador de la nube

Recursos relacionados

- Guía del usuario de Amazon S3 (documentación de AWS)
- Roles de IAM para Amazon EC2 (documentación de Amazon AWS)
- Creación de un contenedor Blob de Microsoft Azure (documentación de Microsoft Azure)
- Comandos de Rclone (documentación de Rclone)

Información adicional

Ejemplo de política de roles para instancias de EC2

Esta política otorga a su instancia de EC2 acceso de lectura y escritura a un bucket específico de su cuenta. Si este bucket usa una clave administrada por el cliente para realizar el cifrado en el lado del servidor, es posible que la política necesite obtener acceso adicional a AWS Key Management Service (AWS KMS).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": [
              "arn:aws:s3:::BUCKET_NAME/*",
              "arn:aws:s3:::BUCKET_NAME"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "s3:ListAllMyBuckets",
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

Crear una entidad principal de servicio de Azure AD de solo lectura

Una entidad principal de servicio de Azure es una identidad de seguridad que usan las aplicaciones, los servicios y las herramientas de automatización de los clientes para acceder a recursos específicos de Azure. Considérelo como una identidad de usuario (nombre de usuario y contraseña o certificado) con un rol específico, y con permisos estrictamente controlados para acceder a sus recursos. Para crear una entidad principal de servicio de solo lectura, con permisos de privilegio mínimo, y proteger los datos de Azure ante eliminaciones accidentales, siga estos pasos:

1. Inicia sesión en el portal de tu cuenta en la nube de Microsoft Azure e inicia Cloud Shell PowerShell o usa la interfaz de línea de comandos (CLI) de Azure en tu estación de trabajo.

2. Cree una entidad principal de servicio y configúrela con acceso de solo lectura a su cuenta de almacenamiento Blob de Azure. Guarde la salida JSON de este comando en un archivo local llamado `azure-principal.json`. El archivo se cargará en su instancia de EC2. Sustituya las variables de marcador de posición que aparecen entre corchetes (`{` y `}`) por el identificador de suscripción de Azure, el nombre del grupo de recursos y el nombre de la cuenta de almacenamiento.

```
az ad sp create-for-rbac `
--name AWS-Rclone-Reader `
--role "Storage Blob Data Reader" `
--scopes /subscriptions/{Subscription ID}/resourceGroups/{Resource Group Name}/
providers/Microsoft.Storage/storageAccounts/{Storage Account Name}
```

Migración de Couchbase Server a Couchbase Capella en AWS

Creado por Battulga Purevragchaa (AWS), Mark Gamble y Saurabh Shanbhag (AWS)

Entorno: producción	Origen: Couchbase Server	Destino: Couchbase Capella
Tipo R: redefinir la plataforma	Carga de trabajo: todas las demás cargas de trabajo	Tecnologías: migración; análisis; bases de datos

Resumen

Couchbase Capella es una base de datos NoSQL como servicio (DBaaS) totalmente gestionada para aplicaciones de misión crítica (por ejemplo, perfiles de usuario o catálogos en línea y gestión de inventario). Couchbase Capella gestiona su carga de trabajo de DBaaS en una cuenta de Amazon Web Services (AWS) gestionada por Couchbase. Capella facilita la ejecución y la administración de la replicación de múltiples clústeres, múltiples regiones de AWS, multinube y nube híbrida dentro de una sola interfaz.

Couchbase Capella le ayuda a escalar al instante sus aplicaciones de Couchbase Server, lo que le permite crear clústeres de varios nodos en cuestión de minutos. Couchbase Capella es compatible con todas las características de Couchbase Server, incluidas SQL++, Full Text Search, Eventing Service y Analytics Service. También elimina la necesidad de gestionar las instalaciones, las actualizaciones, las copias de seguridad y el mantenimiento general de las bases de datos.

Este patrón describe los pasos y las prácticas recomendadas para migrar un entorno de Couchbase Server autogestionado a la nube de AWS. El patrón proporciona un proceso repetible para migrar datos e índices desde los clústeres de Couchbase Server, que se ejecutan en las instalaciones o en la nube, a Couchbase Capella. El uso de estos pasos le ayuda a evitar problemas durante la migración y acelera el proceso general de migración.

Este patrón proporciona las dos opciones de migración siguientes:

- La opción 1 es adecuada si tiene que migrar menos de 50 índices.
- La opción 2 es adecuada si tiene que migrar más de 50 índices.

También puede configurar datos de muestra en su Couchbase Server autogestionado para seguir la guía de migración.

Si elije la opción de migración 2, o si utiliza ámbitos o colecciones distintos del valor predeterminado, debe utilizar el archivo de configuración de ejemplo, que se encuentra en la sección Información adicional.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de pago de Couchbase Capella existente. También puede crear una cuenta de Couchbase Capella en AWS y utilizar la prueba gratuita de Couchbase Capella y, a continuación, actualizar a una cuenta de pago para configurar el clúster para la migración. Para empezar con la versión de prueba, siga las instrucciones de Introducción a Couchbase Capella.
- Un entorno de Couchbase Server autogestionado existente, ya sea en las instalaciones o implementado en un proveedor de servicios en la nube.
- Para la opción de migración 2, Couchbase Shell y un archivo de configuración. Para crear el archivo de configuración, puede usar el archivo de ejemplo que se encuentra en la sección de Información adicional.
- Familiaridad con la administración de Couchbase Server y Couchbase Capella.
- Familiaridad con la apertura de puertos TCP y la ejecución de comandos en una interfaz de la línea de comandos (CLI).

El proceso de migración también requiere los roles y la experiencia que se describen en la siguiente tabla.

Rol	Experiencia	Responsabilidades
Administrador de Couchbase	• Familiaridad con Couchbase Server y Couchbase Capella • El conocimiento básico de la línea de comandos es útil pero no obligatorio	• Couchbase Server y Capella: tareas específicas
Administrador de sistemas; administrador de TI	• Familiaridad con el entorno y la administración del	• Abrir puertos y determina r las direcciones IP en

	sistema Couchbase Server autogestionado	los nodos de clústeres de Couchbase Server autogestionados

Limitaciones

- Este patrón se utiliza para migrar datos, índices e índices de búsqueda de texto completo de Couchbase desde Couchbase Server a Couchbase Capella en AWS. El patrón no se aplica a la migración de Couchbase Eventing Service ni a Couchbase Analytics.
- Couchbase Capella se encuentra disponible en varias regiones de AWS. Para up-to-date obtener información sobre las regiones compatibles con Capella, consulte Amazon Web Services en la documentación de Couchbase.

Versiones de producto

- Couchbase Server (Community o Enterprise) Edition, versión 5.x o posterior

Arquitectura

Pila de tecnología de origen

- Couchbase Server

Pila de tecnología de destino

- Couchbase Capella

Arquitectura de destino

1. Para acceder a Couchbase Capella, utilice el plano de control de Capella. Puede utilizar el plano de control de Capella para hacer lo siguiente:
   - Controlar y supervisar su cuenta.
   - Gestionar clústeres y datos, índices, usuarios y grupos, permisos de acceso, supervisión y eventos.

2. Se han creado clústeres.
3. El plano de datos de Capella se encuentra en la cuenta de AWS gestionada por Couchbase. Tras crear un clúster nuevo, Couchbase Capella lo implementa en varias zonas de disponibilidad de la región de AWS seleccionada.
4. Puede desarrollar e implementar aplicaciones de Couchbase en una VPC de su cuenta de AWS. Normalmente, esta VPC accede al plano de datos de Capella a través del emparejamiento de VPC.

Herramientas

- La replicación cruzada de centros de datos (XDCR) de Couchbase ayuda a replicar los datos en clústeres ubicados en diferentes proveedores de nube y diferentes centros de datos. Se utiliza para migrar datos a Couchbase Capella desde clústeres de servidores Couchbase autogestionados.

  Nota: XDCR no se puede usar con Couchbase Server Community Edition para migrar a Couchbase Capella. En su lugar, puede utilizar cbexport. Para obtener más información, consulte la épica sobre cómo migrar datos de Community Edition.
- Couchbase Shell es un intérprete de comandos de línea para que Couchbase Server y Couchbase Capella accedan a clústeres de Couchbase locales y remotos. En este patrón, Couchbase Shell se usa para migrar índices.
- cbexport es una utilidad de Couchbase para exportar datos del clúster de Couchbase. Incluido en las herramientas CLI de Couchbase Server.

Epics

Preparativos para la migración

Tarea	Descripción	Habilidades requeridas
Evaluar el tamaño del clúster de Couchbase Server autogestionado.	Inicie sesión en la consola web de Couchbase para Couchbase Server y evalúe los nodos y los buckets de su clúster autogestionado.	Administrador de Couchbase

Tarea	Descripción	Habilidades requeridas
	1. Para mostrar una lista de los nodos del clúster, seleccione la pestaña Servers (Servidores) en la barra de navegación. 2. Registre el número de nodos y, a continuación, seleccione cada nodo de la lista para ver sus propiedades. 3. Registre la memoria y el almacenamiento de cada nodo individual. 4. Seleccione la pestaña Buckets en la barra de navegación y, a continuación, elija cada bucket de la lista para ver sus propiedades. Registre la cuota de RAM y la configuración de resolución de conflictos de cada bucket. Utilizará las configuraciones de clúster de Couchbase Server autogestionadas como guía general para dimensionar y configurar el clúster de destino en Couchbase Capella. Si necesita ayuda con un ejercicio de dimensionamiento más detallado del Couchbase	

Tarea	Descripción	Habilidades requeridas
	Capella, póngase en contacto con Couchbase.	
Registre la distribución del servicio Couchbase en el clúster de Couchbase Server autogestionado.	1. En la consola web de Couchbase, seleccione la pestaña Servers (Servidor es) para ver la lista de nodos del clúster. 2. Elija cada nodo para mostrar sus propiedades y, a continuación, registre la distribución del servicio de Couchbase para cada nodo (Data Service (Servicio de datos), Query Service (Servicio de consultas), Index Service (Servicio de índice), Search Service (Servicio de búsqueda), Analytics Service (Servicio de análisis) y Eventing Service (Servicio de eventos)).	Administrador de Couchbase
Registre las direcciones IP de los nodos del clúster de Couchbase Server autogesti onados.	(Ignore este paso si utiliza Community Edition). Registre la dirección IP de cada nodo del clúster. Se añadirán a la lista de permitidos de su clúster de Couchbase Capella más adelante.	Administrador de Couchbase, administrador de sistemas

Implemente y configure los recursos en Couchbase Capella

Tarea	Descripción	Habilidades requeridas
Elija una plantilla.	1. Inicie sesión en su plano de control Couchbase Capella, elija la pestaña Dashboard (Panel de control) o la pestaña Clusters (Clústeres) en la navegación principal y, a continuación, elija Create Cluster (Crear clúster). 2. Con la información que registró en la evaluación de su clúster de Couchbase Server autogestionado, elija la plantilla de clúster que cumpla con los requisito s de la configuración. Si no encuentra una plantilla adecuada, elija Custom Template (Plantilla personalizada) en el editor de Cluster Sizing (Tamaño de clústeres).	Administrador de Couchbase
Elija y configure los nodos.	Elija y configure los nodos para que se adapten a su entorno de clústeres de Couchbase Server autogesti onado, incluida la cantidad de nodos, la distribución, el procesamiento o la RAM de los servicios y el almacenam iento.	Administrador de Couchbase

Tarea	Descripción	Habilidades requeridas
	Couchbase Capella utiliza las prácticas recomendadas de escalado multidimensional. Los servicios y los nodos solo se pueden elegir de acuerdo con las prácticas recomenda das de implementación. Esto puede significar que no puede igualar exactamente las configuraciones de su clúster de Couchbase Server autogestionado.	

Tarea	Descripción	Habilidades requeridas
Implementación del clúster.	El conocimiento básico de la línea de comandos es útil pero no obligatorio Para obtener instrucciones y pasos detallados, consulte Create a cluster (Crear un clúster) en la documentación de Couchbase . Importante: si está utilizando la versión de prueba gratuita de Couchbase Capella, debe convertirla en una cuenta de pago antes de comenzar la migración. Para convertir su cuenta, abra la sección Billing (Facturación) del plano de control de Couchbase Capella y, a continuación, seleccion e Add Activation ID (Añadir un ID de activación). El ID de activación se envía a su dirección de correo electróni co de contacto de facturaci ón después de completar un acuerdo de compra con Couchbase Sales o después de realizar una compra a través de AWS Marketplace.	Administrador de Couchbase

Tarea	Descripción	Habilidades requeridas
Crear un usuario con credenciales de base de datos.	Un usuario con credenciales de base de datos es específico de un clúster y consta de un nombre de usuario, una contraseña y un conjunto de privilegios de bucket. Este usuario es necesario para crear buckets y acceder a los datos del bucket. En el plano de control de Couchbase Capella, cree una credencial de base de datos para el nuevo clúster siguiendo las instrucciones de Configure database credentials (Configurar las credenciales de la base de datos) de la documentación de Couchbase Capella. Nota: Un usuario de la organización necesita que se le asignen credenciales de rol organizacional si quiere acceder a los datos del bucket en un clúster en particular, ya sea de forma remota o a través de la interfaz de usuario de Couchbase Capella. Esto es independiente de las credenciales de la base de datos, que suelen utilizar las aplicaciones y las integraciones. La creación del usuario	Administrador de Couchbase

Tarea	Descripción	Habilidades requeridas
	organizacional le permite crear y administrar los buckets de destino en su clúster de Couchbase Capella.	
Si utiliza la opción de migración 2, instale Couchbase Shell.	Puede instalar Couchbase Shell en cualquier sistema que tenga acceso de red tanto a su Couchbase Server autogestionado como a los clústeres de Couchbase Capella. Para obtener más información, consulte Instalar la versión 1.0.0-beta.5 de Couchbase Shell en la documentación de Couchbase Shell. Confirme que Couchbase Shell esté instalado probando una conexión a su clúster autogestionado en un terminal de línea de comandos.	Administrador de Couchbase, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Permitir direcciones IP.	1. En el plano de control de Couchbase Capella, elija Clústeres y, a continuación, elija su clúster de destino. 2. Elija la pestaña Connect (Conectar) del clúster y registre el punto de conexión del clúster que aparece en Manage Allowed IP (Administrar la IP permitida). 3. Para añadir la dirección IP del sistema en el que instaló Couchbase Shell y la dirección IP de las instancias de clúster de Couchbase Server autogestionadas como direcciones IP permitidas, haga lo siguiente: a. En Wide Area Network (Red de área amplia), elija Manage Allowed IP (Administrar la IP permitida). b. Seleccione Add Allowed IP (Añadir la IP permitida), introduzca la dirección IP del sistema en el que instaló Couchbase Shell y, a continuac ión, seleccione Add IP (Añadir IP).	Administrador de Couchbase, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	c. Repita el paso anterior para añadir la dirección IP de la instancia de clúster autogestionada de Couchbase Server. Para obtener más información sobre las direcciones IP permitidas, consulte Configurar las direcciones IP permitidas en la documentación de Couchbase.	

Tarea	Descripción	Habilidades requeridas
Configuración de los certificados.	1. Para descargar el certificado raíz de su clúster, en Root Certificate (Certificado raíz), seleccione Download (Descargar). 2. Guarde el certificado raíz con la extensión de archivo .pem en una carpeta del sistema en la que se ejecute Couchbase Shell. 3. A continuación, inicie sesión en la consola web autogestionada de Couchbase Server, seleccione Security (Seguridad) en la barra de navegación izquierda y, a continuación, seleccione la pestaña Certificates (Certificados). 4. Copie el certificado raíz de su clúster de Couchbase Server autogestionado y guárdelo como un archivo .pem en la misma carpeta en la que guardó el archivo de certificado raíz de su clúster de Couchbase Capella. Para obtener más información acerca del certificado raíz, consulte Certificado raíz	Administrador de Couchbase, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	en la documentación de Couchbase Server.	
Crear el archivo de configuración para Couchbase Shell.	Cree un archivo dotfile de configuración en el directorio principal de la instalación de Couchbase Shell (por ejemplo, `/<HOME_DIRECTORY>/.cbsh/config`). Para obtener más información, consulte Dotfiles de configuración en la documentación de Couchbase. Añada las propiedades de conexión de los clústeres de origen y destino al archivo de configuración. Puede usar el archivo de ejemplo de configuración que se encuentra en la sección de Información adicional y editar los ajustes de los clústeres. Guarde el archivo de configuración con los ajustes actualizados en la carpeta `.cbsh` (por ejemplo, `/<HOME_DIRECTORY>/.cbsh/config`).	Administrador de Couchbase, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Cree buckets de destino.	Para cada bucket de origen, cree un bucket de destino en su clúster de Couchbase Capella siguiendo las instrucciones de la documentación de Couchbase para crear un bucket. Las configuraciones de los buckets de destino deben coincidir con los nombres de los buckets, los ajustes de memoria y los ajustes de resolución de conflictos de los buckets de su clúster de Couchbase Server autogestionado.	Administrador de Couchbase

Tarea	Descripción	Habilidades requeridas
Crear ámbitos y colecciones.	Cada bucket contiene un ámbito y una colección predeterminados con el espacio de claves `_default._default` . Si utiliza otros espacios de clave para el ámbito y la colección, debe crear espacios de clave idénticos en el clúster de Capella de destino. 1. Abra el terminal de línea de comandos del sistema en el que instaló Couchbase Shell. 2. Para iniciar Couchbase Shell, ejecute el siguiente comando. `./cbsh` 3. Para cada bucket que desee migrar, cree ámbitos y colecciones en el clúster de Capella ejecutando los siguientes comandos. Asegúrese de reemplaza r <BUCKET_NAME> por el nombre del bucket que desea migrar. `scopes --clusters "On-Prem-Cluster" --bucket <BUCKET_NAME> | select scope | where scope !`	Administrador de Couchbase

Tarea	Descripción	Habilidades requeridas
	`= "_default" | each { |it| scopes create $it.scope --clusters "Capella-Cluster" } collections --clusters "On-Prem-Cluster" --bucket <BUCKET_NAME> | select scope collection | where $it.scope != "_default" | where $it.collection != "_default" | each { |it| collections create $it.collection --clusters "Capella-Cluster" --bucket <BUCKET_NAME> --scope $it.scope }`	

Migración de los datos de Enterprise Edition

Tarea	Descripción	Habilidades requeridas
Abrir los puertos TCP en los nodos del clúster autogestionado de Couchbase Server.	Asegúrese de que los puertos adecuados estén abiertos para la comunicación XDCR en los nodos del clúster de Couchbase Server autogestionado. Para obtener más información, consulte la documentación sobre puertos de Couchbase Server.	Administrador de Couchbase, administrador de sistemas
Si utiliza Couchbase Server Enterprise Edition, configure Couchbase XDCR.	1. En el plano de control de navegación central de Couchbase Capella, elija Clústeres y, a continuación,	Administrador de Couchbase

Tarea	Descripción	Habilidades requeridas
	elija su clúster de destino para la migración. 2. En Root Certificate (Certificado raíz), seleccione Copy (Copiar). 3. Inicie sesión en la consola web autogestionada de Couchbase Server y, en la barra de navegación principal, seleccione XDCR. A continuación, seleccione Add remote (Agregar remoto). 4. Ingrese la siguiente configuración: • Nombre del clúster: un nombre para la conexión del clúster de Capella • IP/nombre de host: el punto de conexión de su clúster de Couchbase Capella • Nombre de usuario para el clúster remoto: el usuario de la base de datos de su clúster de Couchbase Capella • Contraseña: la contraseña de usuario de la base de datos para su clúster de Couchbase Capella • Habilitar conexión segura: seleccionado	

Tarea	Descripción	Habilidades requeridas
	• Completo (encripta la contraseña y los datos con TLS): seleccionado 5. Pegue el certificado raíz del clúster de Capella que copió anteriormente y, a continuación, seleccione Save (Guardar).	
Iniciar Couchbase XDCR.	1. En la consola web autogestionada de Couchbase Server, elija XDCR en la barra de navegación principal, y luego seleccione Agregar replicación. 2. Ingrese la siguiente configuración: • Replicar desde un bucket: seleccione el bucket de origen para la migración. • Bucket remoto: introduzca el nombre del bucket de destino. • Clúster remoto: seleccione el clúster de destino que creó anteriormente. 3. Elija Save Replication (Guardar replicación). El proceso de replicación debería comenzar en unos segundos.	Administrador de Couchbase

Migración de los índices mediante la opción 1

Tarea	Descripción	Habilidades requeridas
Migración de los índices de clústeres autogestionados a Couchbase Capella.	Importante: recomendamos este proceso si tiene que migrar menos de 50 índices. Si tiene que migrar más de 50 índices, le recomendamos que utilice la opción de migración 2. 1. En la consola web de Couchbase, elija Indexes (Índices). 2. En la lista de índices, seleccione el primer índice que desea migrar. A continuación, se muestra la definición del índice. 3. Copie la definición del índice mediante la instrucción `CREATE`, pero no copie `WITH { "defer_build":true }` . Por ejemplo, del siguiente ejemplo de definición de índice, solo copiaría `CREATE INDEX` `` `cityindex` ON `travel-sample`(`city`) `` . `CREATE INDEX `cityindex` ON `travel-sample`(`city`)`	Administrador de Couchbase, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	`WITH { "defer_build":true }` 4. En el plano de control de Couchbase Capella, elija Clústeres y, a continuación, elija el clúster de destino. 5. En la lista desplegable Herramientas, elija Query Workbench. Pegue la instrucción `CREATE` que copió anteriormente en el Query Editor (Editor de consultas) y, a continuación, seleccione Execute (Ejecutar). Esto crea y desarrolla el índice. 6. Para confirmar que se ha creado el índice, elija Indexes (Índices) en la lista desplegable Tools (Herramientas). La lista muestra que el índice se creó y se desarrolló. 7. Repita este proceso para cada índice que desee migrar.	

Migración de los índices mediante la opción 2

Tarea	Descripción	Habilidades requeridas
Migre las definiciones del índice.	Importante: recomendamos este proceso si tiene que	Administrador de Couchbase, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	migrar más de 50 índices. Si tiene que migrar menos de 50 índices, le recomendamos que utilice la opción de migración 1. 1. Abra el terminal de línea de comandos del sistema en el que instaló Couchbase Shell. 2. Para iniciar Couchbase Shell, ejecute el siguiente comando. `./cbsh` 3. Para conectarse al clúster de Couchbase Server autogestionado, ejecute el siguiente comando. `cb-env cluster On-Prem-Cluster` 4. Para migrar las definiciones de índice del clúster de Couchbase Server autogestionado al clúster de Couchbase Capella, ejecute el siguiente comando para cada bucket que desee migrar. Asegúrese de reemplazarlas por el nombre del bucket `<BUCKET_NAME>` que corresponda a los índices	

Tarea	Descripción	Habilidades requeridas
	que desee migrar. Esta opción de migración requiere que los nombres de los buckets de destino sean idénticos a los nombres de los buckets de origen. `query indexes --definitions | where bucket =~ <BUCKET_NAME>| get definition | each { |it| query $it --clusters Capella-Cluster }`	

Tarea	Descripción	Habilidades requeridas
Crear las definiciones del índice.	1. Para cambiar de contexto al clúster de Couchbase Capella, ejecute el siguiente comando: `cb-env cluster Capella-Cluster` 2. Para crear las definiciones de índice que se migraron al clúster de Couchbase Capella, ejecute el siguiente comando y sustitúya <BUCKET_NAME> por el nombre del bucket que corresponda a los índices que desee crear. `query 'SELECT RAW CONCAT("BUILD INDEX ON ", k , "(['", CONCAT2 ("','", inames), "']);") FROM system:indexes AS s LET bid = CONCAT("` ",s.bucket_id, "`"), sid = CONCAT("`", s.scope_id, "`"), kid = CONCAT("` ", s.keyspace_id, "`"), k = NVL2(bid, CONCAT2(".", bid, sid, kid), kid) WHERE s.namespa ce_id = "default" AND s.bucket_id = "" GROUP BY k LETTING inames = ARRAY_AGG (s.name) FILTER`	Administrador de Couchbase, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	(WHERE s.state = 'deferred') HAVING ARRAY_LENGTH(iname s) > 0;' | each { | it| query $it } 3. Repita este proceso para cada bucket.	

Migración de índices de búsqueda de texto completo

Tarea	Descripción	Habilidades requeridas
Migre los índices de búsqueda de texto completo de clústeres autogestionados a Couchbase Capella.	1. En la consola web de Couchbase, elija Search (Buscar). 2. En la lista de índices de búsqueda de texto completo (FTS), elija el primer índice FTS que desee migrar, elija Show index definition JSON (Mostrar definición de índice JSON) y elija Copy to Clipboard (Copiar al portapapeles). Anote el nombre del índice y el bucket al que pertenece. 3. En el plano de control de Couchbase Capella, elija Clústeres y, a continuación, elija su clúster de destino. 4. En la lista desplegable de herramientas, seleccione	Administrador de Couchbase

Tarea	Descripción	Habilidades requeridas
	Full Text Search (Búsqueda de texto completo). 5. Seleccione Import Index (Importar índice) y pegue la definición del índice FTS. 6. Introduzca el Index Name (Nombre del índice), seleccione el bucket correcto, tal y como se indica en el clúster autogestionado, y, a continuación, pulse Create (Crear). 7. Repita este proceso para cada índice FTS que desee migrar.	

Migración de los datos de Couchbase Community Edition

Tarea	Descripción	Habilidades requeridas
Exportar datos desde Couchbase Server Community Edition autogestionada.	El XDCR cifrado no está disponible en Couchbase Community Edition. Puede exportar los datos de Couchbase Community Edition y luego importarlos manualmente a Couchbase Capella. Para exportar datos del bucket de origen, utilice `cbexport` en la línea de comandos.	Administrador de Couchbase

Tarea	Descripción	Habilidades requeridas
	Puede ver un ejemplo en el siguiente comando: `cbexport json \` `--cluster localhost \` `--bucket <SOURCE BUCKET NAME> \` `--format lines \` `--username <USERNAME> \` `--password <PASSWORD> \` `--include-key cbkey \` `--scope-field cbscope \` `--collection-field cbcoll \` `--output cbexported_data.json` Tenga en cuenta que `cbkey`, `cbscope`, `cbcoll` y `cbexported_data.json` son etiquetas arbitrarias. Se hará referencia a ellas más adelante en el proceso, así que si decide asignarles un nombre diferente, anótelo.	

Tarea	Descripción	Habilidades requeridas
Importar datos a Couchbase Capella.	1. En el plano de control de Couchbase Capella, elija Clústeres y, a continuación, elija el clúster de destino. 2. En la lista desplegable Tools (Herramientas), seleccione Import (Importar). Se abrirá un asistente con los seis pasos siguientes: a. Bucket: elija el bucket de destino. b. File (Archivo): elija JSON, elija Lines (Líneas) y, a continuac ión, elija Using your web browser (Usar su navegador web). Si tiene una gran cantidad de datos, puede explorar la opción Manually (Manualmente). Seleccione el archivo creado por `cbexport`. c. Colecciones: elija un Custom Collection Mapping (asignación de colecciones personali zado). Si su base de datos de Community Edition no usa ámbitos ni coleccion es, o solo usa _default, puede elegir la opción	Administrador de Couchbase

Tarea	Descripción	Habilidades requeridas
	Select Single Collection (Seleccionar colección única) en su lugar. Para Collection Mapping Expression (Expresión de asignación de colección), introduzca `%cbscope%.%cbcoll%` . Para comprobar que esta expresión funciona correctamente, puede pegar datos de ejemplo, como los siguientes. `{ "cbscope" :"inventory", "cbcoll":"landmark", "cbkey":" landmark_3991" }` d. Clave: elija Customer Generation (Generación de clientes). (Si no le importa conservar las claves de los datos que va a importar, puede seleccionar el Automatically Generated UUID (UUID generado automáticamente) en su lugar y continuar con el paso 5). En Key Name Generator Expression (Expresión del generador de nombres de clave),	

Tarea	Descripción	Habilidades requeridas
	introduzca %cbkey%. Para comprobar que esta expresión funciona correctamente, pegue datos de ejemplo. e. Configuraciones: elija Ignore fields (Ignorar campos) e introduzca cbscope, cbcoll o cbkey. Estos campos contienen información transitor ia que no necesita estar en el bucket de destino después de una importación. No cambie los valores predeterm inados de los demás ajustes. f. Importar: revise y seleccione Import (Importar) cuando esté listo. Espere a que se carguen y se importen los datos. Para archivos grandes, Couchbase Capella admite la importación por línea de comandos mediante cURL. Puede explorar las opciones de importación con más detalle en Import data (Importar datos) en la	

Tarea	Descripción	Habilidades requeridas
	documentación de Couchbase Capella.	

Probar y verificar la migración

Tarea	Descripción	Habilidades requeridas
Comprobación de la migración de datos.	1. En el plano de control de Couchbase Capella, elija Clústeres y, a continuación, elija el clúster de destino de su lista de clústeres. 2. Seleccione la pestaña Buckets para el clúster de destino. Compruebe que el número de elementos (documentos) del bucket de destino coincide con el número de elementos del bucket de origen. 3. En el clúster de destino, en la lista desplegable Tools (Herramientas), seleccione Documents (Documentos). Compruebe que se hayan migrado todos los documentos. 4. (Opcional) Una vez migrados todos los datos, puede cerrar la replicación eliminándola. Para obtener más información, consulte Delete a replication (Eliminación	Administrador de Couchbase

Tarea	Descripción	Habilidades requeridas
	de una replicación) en la documentación de Couchbase.	
Verificar la migración del índice.	En el plano de control de Couchbase Capella, en la lista desplegable Tools (Herramientas) del clúster de destino, seleccione Indexes (Índices). Compruebe que los índices se hayan migrado y creado.	Administrador de Couchbase
Verificar los resultados de consulta.	1. En el plano de control de Couchbase Capella, en la lista desplegable Tools (Herramientas) del clúster de destino, seleccione Query Workbench. 2. Ejecute un ejemplo de consulta de N1QL o una consulta utilizada en su aplicación. Asegúrese de recibir los mismos resultados que cuando ejecutó la consulta en su clúster de Couchbase Server autogestionado.	Administrador de Couchbase

Tarea	Descripción	Habilidades requeridas
Verificar los resultados de la búsqueda de texto completo (aplicable si migró los índices FTS).	1. En el plano de control de Couchbase Capella, en la lista desplegable Herramientas del clúster de destino, seleccione Full Text Search (Búsqueda de texto completo). 2. Seleccione un índice FTS eligiendo su nombre. 3. Elija Buscar. 4. Introduzca un ejemplo de consulta de búsqueda y seleccione Search (Buscar). 5. Compruebe que los resultados sean los mismos que cuando ejecutó la búsqueda en el clúster autogestionado.	Administrador de Couchbase

Recursos relacionados

Preparativos para la migración

- Comience con la prueba gratuita de Couchbase Capella
- Requisitos de proveedor de servicios en la nube para Couchbase Capella
- Pautas de tamaños de Couchbase Capella

Migración de datos e índices

- Couchbase XDCR
- Documentación de Couchbase Shell

SLA y soporte de Couchbase Capella

- Acuerdos de nivel de servicio (SLA) de Couchbase Capella
- Política de soporte del servicio Couchbase Capella

Información adicional

El siguiente código es un ejemplo de archivo de configuración para Couchbase Shelll.

```
Version = 1

[[clusters]]
identifier = "On-Prem-Cluster"
hostnames = ["<SELF_MANAGED_COUCHBASE_CLUSTER>"]
default-bucket = "travel-sample"
username = "<SELF_MANAGED_ADMIN>"
password = "<SELF_MANAGED_ADMIN_PWD>"
tls-cert-path = "/<ABSOLUTE_PATH_TO_SELF_MANAGED_ROOT_CERT>"
data-timeout = "2500ms"
connect-timeout = "7500ms"
query-timeout = "75s"

[[clusters]]
identifier = "Capella-Cluster"
hostnames = ["<COUCHBASE_CAPELLA_ENDPOINT>"]
default-bucket = "travel-sample"
username = "<CAPELLA_DATABASE_USER>"
password = "<CAPELLA_DATABASE_USER_PWD>"
tls-cert-path = "/<ABSOLUTE_PATH_TO_COUCHBASE_CAPELLA_ROOT_CERT>"
data-timeout = "2500ms"
connect-timeout = "7500ms"
query-timeout = "75s"
```

Antes de guardar el archivo de configuración, utilice la siguiente tabla para asegurarse de haber agregado su propia información de clúster de origen y destino.

<SELF_MANAGED_COUCHBASE_CLUSTER>	Use las direcciones IP para su clúster de Couchbase Server autogestionado.

<SELF_MANAGED_ADMIN>	Use el usuario administrador para su clúster de Couchbase Server autogestionado.
<ABSOLUTE_PATH_TO_SELF_MANAGED_ROOT_CERT>	Use la ruta absoluta al archivo de certificado raíz guardado para su clúster de Couchbase Server autogestionado.
<COUCHBASE_CAPELLA_ENDPOINT>	Use el punto de conexión de su clúster de Couchbase Capella.
<CAPELLA_DATABASE_USER>	Use el usuario de la base de datos para su clúster de Couchbase Capella.
<CAPELLA_DATABASE_USER_PWD>	Use la contraseña de usuario de la base de datos para su clúster de Couchbase Capella.
<ABSOLUTE_PATH_TO_COUCHBASE_CAPELLA_ROOT_CERT>	Use la ruta absoluta al archivo de certificado raíz guardado para su clúster de Couchbase Capella.

Migre de IBM WebSphere Application Server a Apache Tomcat en Amazon EC2

Creado por Neal Ardeljan (AWS) y Afroz Khan (AWS)

Entorno: Producción	Origen: aplicaciones	Destino: Apache Tomcat en una instancia de Amazon EC2
Tipo R: redefinir la plataforma	Carga de trabajo: IBM; código abierto	Tecnologías: migración; aplicaciones web y móviles
Servicios de AWS: Amazon EC2		

Resumen

Este patrón le guía por los pasos para migrar de un sistema Red Hat Enterprise Linux (RHEL) 6.9 o posterior local que ejecute IBM WebSphere Application Server (WAS) a RHEL 8 con Apache Tomcat en una instancia de Amazon Elastic Compute Cloud (Amazon EC2).

Este patrón se puede aplicar a las siguientes versiones de origen y destino:

- WebSphere Application Server 7.x a Apache Tomcat 8 (con Java 7 o posterior)
- WebSphere Del servidor de aplicaciones 8.x a Apache Tomcat 8 (con Java 7 o posterior)
- WebSphere Del servidor de aplicaciones 8.5.5.x a Apache Tomcat 9 (con Java 8 o posterior)
- WebSphere Del servidor de aplicaciones 8.5.5.x a Apache Tomcat 10 (con Java 8 o posterior)

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Código fuente de Java, con las siguientes suposiciones:
  - Emplea la versión de Java Development Kit (JDK) de Java 7 o posterior
  - Emplea el marco Spring o Apache Struts

  - No utiliza el framework Enterprise Java Beans (EJB) ni ninguna otra funcionalidad de WebSphere servidor que no esté fácilmente disponible para Tomcat
  - Emplea principalmente servlets o Java Server Pages (JSP)
  - Emplea conectores de Java Database Connectivity (JDBC) para conectar a las bases de datos
- Fuente: IBM WebSphere Application Server versión 7.x o superior
- Destino: Apache Tomcat, versión 8.5 o superior

Arquitectura

Pila de tecnología de origen

- Una aplicación web creada con el marco Apache Struts Model-View-Controller (MVC)
- Una aplicación web que se ejecuta en las versiones 7.x u 8.x de IBM WebSphere Application Server
- Una aplicación web que emplea un conector Lightweight Directory Access Protocol (LDAP) para conectar a un directorio LDAP (iPlanet/eTrust)
- Una aplicación que emplea la conectividad de IBM Tivoli Access Manager (TAM) para actualizar la contraseña del usuario de TAM (en la presente implementación, las aplicaciones usan PD.jar)

Bases de datos en las instalaciones

- Oracle Database 21c (21.0.0.0)
- Oracle Database 19c (19.0.0.0)
- Oracle Database 12c Versión 2 (12.2.0.1)
- Oracle Database 12c Release 1 (12.1.0.2)

Pila de tecnología de destino

- Apache Tomcat versión 8 (o posterior) ejecutado en RHEL en una instancia de EC2
- Amazon Relational Database Service (Amazon RDS) para Oracle

Para obtener más información sobre las versiones de Oracle compatibles con Amazon RDS, consulte el sitio web de Amazon RDS para Oracle.

Arquitectura de destino

Herramientas

- Nivel de aplicación: reconstrucción de una aplicación Java en un archivo WAR.
- Nivel de base de datos: copia de seguridad y restauración nativas de Oracle.
- Herramienta de migración de Apache Tomcat para Jakarta EE. Esta herramienta toma una aplicación web escrita para Java EE 8 y ejecutada en Apache Tomcat 9 y la convierte automáticamente para ejecutarla en Apache Tomcat 10, que implementa Jakarta EE 9.

Epics

Planificación de la migración

Tarea	Descripción	Habilidades requeridas
Complete el descubrimiento de las aplicaciones, el estado actual y la línea base de rendimiento.		BA, líder de migración
Valide las versiones de las bases de datos de origen y de destino.		Administrador de base de datos
Identifique los requisitos de hardware para la instancia EC2 del servidor de destino.		DBA, SysAdmin
Identifique los requisitos de almacenamiento (como el tipo y la capacidad de almacenam iento).		DBA, SysAdmin
Elija el tipo de instancia de EC2 adecuado en función de la capacidad, las caracterí		DBA, SysAdmin

Tarea	Descripción	Habilidades requeridas
sticas de almacenamiento y las características de red.		
Identifique los requisitos de seguridad de acceso a la red para las bases de datos de origen y destino.		DBA, SysAdmin
Identifique la estrategia y las herramientas de migración de aplicaciones.		Administrador de base de datos, líder de migración
Complete el diseño de la migración y la guía de migración de la aplicación.		Responsable de compilación, líder de migración
Complete el manual de procedimientos de migración de aplicaciones.		Responsable de compilación, líder de transición, líder de pruebas, líder de migración

Configuración de la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC).		SysAdmin
Creación de grupos de seguridad.		SysAdmin
Configure e inicie Amazon RDS para Oracle.		DBA, SysAdmin

Migración de datos

Tarea	Descripción	Habilidades requeridas
Cree o acceda a los puntos de conexión para recuperar los archivos de copia de seguridad de la base de datos.		Administrador de base de datos
Utilice el motor de base de datos nativo o una herramien ta de terceros para migrar los objetos y datos de la base de datos.	Para obtener más información, consulte “Migración de objetos y datos de bases de datos” en la sección de Información adicional.	Administrador de base de datos

Migración de la aplicación

Tarea	Descripción	Habilidades requeridas
Presente la solicitud de cambio (CR) para la migración .		Líder de transición
Obtenga la aprobación de la CR para la migración.		Líder de transición
Siga la estrategia de migración de aplicaciones según el manual de procedimi entos de migración de aplicaciones.	Para obtener más información, consulte “Configurar el nivel de aplicación” en la sección de Información adicional.	Administrador de base de datos, ingeniero de migracion es, propietario de la aplicación
Actualice la aplicación (si es necesario).		Administrador de base de datos, ingeniero de migracion es, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Complete las pruebas funcionales y no funcionales, de validación de datos, de acuerdo de nivel de servicio y de rendimiento.		Líder de pruebas, propietario de la aplicación, usuarios de la aplicación

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Obtenga la aprobación del propietario de la aplicación o del propietario de la empresa.		Líder de transición
Cambie los clientes de aplicaciones a la nueva infraestructura.		Administrador de base de datos, ingeniero de migracion es, propietario de la aplicación

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cerrar los recursos temporale s de AWS.		DBA, ingeniero de migración, SysAdmin
Revise y valide los documento s del proyecto.		Líder de migración
Recopile métricas como el tiempo de migración, el porcentaje de esfuerzo manual en comparación con el automatizado y el ahorro de costos.		Líder de migración

Tarea	Descripción	Habilidades requeridas
Cerrar el proyecto y enviar comentarios.		Líder de migración, propietario de la aplicación

Recursos relacionados

Referencias

- Documentación de Apache Tomcat 10.0
- Documentación de Apache Tomcat 9.0
- Documentación de Apache Tomcat 8.0
- Guía de instalación de Apache Tomcat 8.0
- Documentación de JNDI de Apache Tomcat
- Sitio web de Amazon RDS para Oracle
- Precios de Amazon RDS
- Oracle y Amazon Web Services
- Oracle en Amazon RDS
- Implementaciones Multi-AZ de Amazon RDS

Tutoriales y videos

- Introducción a Amazon RDS

Información adicional

Migración de objetos y datos de bases de datos

Por ejemplo, si usa las utilidades de copia de seguridad y restauración nativas de Oracle:

1. Cree la copia de seguridad de Amazon Simple Storage Service (Amazon S3) para los archivos de copia de seguridad de la base de datos (opcional).
2. Haga una copia de seguridad de los datos de la base de datos de Oracle en la carpeta compartida de la red.
3. Inicie sesión en el servidor transitorio de migración para mapear la carpeta compartida de la red.

4. Copie los datos de la carpeta de recursos compartidos de la red al bucket de S3.
5. Solicite una implementación de Amazon RDS Multi-AZ para Oracle.
6. Restaure la copia de seguridad de la base de datos en las instalaciones en Amazon RDS para Oracle.

Configurar el nivel de aplicación

1. Instale Tomcat 8 (o 9/10) desde el sitio web de Apache Tomcat.
2. Empaquete la aplicación y las bibliotecas compartidas en un archivo WAR.
3. Implemente el archivo WAR en Tomcat.
4. Supervise el registro de inicio para detectar `Linux cat` cualquier biblioteca compartida que falte. WebSphere
5. Observe el registro de inicio de `Linux cat` cualquier WebSphere extensión descriptora de despliegue específica.
6. Recopile del servidor las bibliotecas Java dependientes que falten. WebSphere
7. Modifique los elementos descriptores de despliegue WebSphere específicos con equivalentes compatibles con Tomcat.
8. Reconstruya el archivo WAR con las bibliotecas Java dependientes y los descriptores de implementación actualizados.
9. Actualice la configuración de LDAP y la configuración de la base de datos y pruebe las conexiones (consulte las instrucciones de configuración de Realm y las instrucciones de JNDI Datasource en la documentación de Apache Tomcat).
10. Pruebe la aplicación instalada con la base de datos de Amazon RDS para Oracle restaurada.
11. Cree una imagen de máquina de Amazon (AMI) para Linux a partir de una instancia EC2.
12. Inicie la arquitectura completa con el equilibrador de carga de aplicación y el grupo de escalado automático.
13. Actualice las URL (mediante el cruce WebSEAL) para que apunten al equilibrador de carga de aplicación.
14. Actualice la base de datos de administración de configuración (CMDB).

Migre de IBM WebSphere Application Server a Apache Tomcat en Amazon EC2 con Auto Scaling

Tipo R: redefinir la plataforma	Origen: aplicaciones	Destino: Apache Tomcat en una instancia de Amazon EC2 con escalado automático habilitado
Creado por: AWS	Entorno: PoC o piloto	Tecnologías: aplicaciones web y móviles; migración
Carga de trabajo: código abierto; IBM	Servicios de AWS: Amazon EC2	

Resumen

Este patrón proporciona orientación para migrar una aplicación Java de IBM WebSphere Application Server a Apache Tomcat en una instancia de Amazon Elastic Compute Cloud (Amazon EC2) con Amazon EC2 Auto Scaling activado.

Con el uso de este patrón, puede lograr lo siguiente:

- Una reducción de los costos de licencias de IBM
- Alta disponibilidad mediante la Implementación multi-AZ
- Aumento de la resiliencia de las aplicaciones con Amazon EC2 Auto Scaling

Requisitos previos y limitaciones

Requisitos previos

- Las aplicaciones Java (versión 7.x o 8.x) deben desarrollarse en pilas LAMP.
- El estado de destino es alojar aplicaciones Java en hosts Linux. Este patrón se ha implementado con éxito en un entorno de Red Hat Enterprise Linux (RHEL) 7. Otras distribuciones de Linux pueden seguir este patrón, pero consultando siempre la configuración de la distribución de Apache Tomcat.
- Debe comprender las dependencias de la aplicación Java.

- Debe tener acceso al código fuente de la aplicación Java para poder realizar cambios.

Limitaciones y redefiniciones de plataforma

- Debe comprender los componentes del archivo empresarial (EAR) y comprobar que todas las bibliotecas estén empaquetadas en archivos WAR de componentes web. Debe configurar el complemento WAR de Apache Maven y producir artefactos en los archivos WAR.
- Al usar Apache Tomcat 8, existe un conflicto conocido entre servlet-api.jar y los archivos jar integrados en el paquete de la aplicación. Para resolver este problema, elimine servlet-api.jar del paquete de la aplicación.
- Debe configurar WEB-INF/Resources, ubicado en classpath de la Configuración de Apache Tomcat. De forma predeterminada, las bibliotecas JAR no se cargan en el directorio. Como alternativa, puede implementar todos los recursos en src/main/resources.
- Compruebe si hay alguna raíz de contexto con codificación rígida en la aplicación Java y actualice la nueva raíz de contexto de Apache Tomcat.
- Para configurar las opciones de tiempo de ejecución de JVM, puede crear el archivo de configuración setenv.sh en la carpeta bin de Apache Tomcat; por ejemplo, JAVA_OPTS, JAVA_HOME, etc.
- La autenticación se configura a nivel de contenedor, como un dominio en las configuraciones de Apache Tomcat. La autenticación se establece para cualquiera de los tres dominios siguientes:
  - JDBC Database Realm busca los usuarios en una base de datos relacional a la que se accede mediante el controlador JDBC.
  - DataSource Database Realm busca los usuarios en una base de datos a la que accede JNDI.
  - JNDI Directory Realm busca a los usuarios en el directorio de Lightweight Directory Access Protocol (LDAP) al que accede el proveedor de JNDI. Las búsquedas requieren:
    - Detalles de la conexión LDAP: base de búsqueda de usuarios, filtro de búsqueda, base de roles, filtro de roles
    - Dominio clave del directorio JNDI: se conecta a LDAP, autentica a los usuarios y recupera todos los grupos de los que un usuario es miembro
- Autorización: en el caso de un contenedor con una autorización basada en roles que compruebe las restricciones de autorización en web.xml, los recursos web deben definirse y compararse con los roles indicados en las restricciones. Si LDAP no tiene una asignación de roles de grupo, debe establecer el atributo <security-role-ref> en web.xml para lograr la asignación de roles de grupo. Para ver un ejemplo de un documento de configuración, consulte la documentación de Oracle.

- Conexión de base de datos: cree una definición de recurso en Apache Tomcat con una URL y detalles de conexión de un punto de conexión Amazon Relational Database Service (Amazon RDS). Actualice el código de la aplicación para que haga referencia a DataSource mediante la búsqueda JNDI. Una conexión de base de datos existente definida en no WebSphere funcionaría, ya que utiliza sus nombres WebSphere JNDI. Puede añadir una <resource-ref>entrada en el archivo web.xml con el nombre y la definición del DataSource tipo del JNDI. Para ver un ejemplo de documento de configuración, consulte la documentación de Apache Tomcat.
- Registro: de forma predeterminada, Apache Tomcat inicia sesión en la consola o en un archivo de registro. Puede habilitar el rastreo a nivel de dominio actualizando logging.properties (consulte Registros en Tomcat). Si usa Apache Log4j para añadir registros a un archivo, debe descargar tomcat-juli y añadirlo al classpath.
- Gestión de sesiones: si va a usar IBM WebSeal como equilibrador de carga de aplicación y gestión de sesiones, no es necesario realizar ningún cambio. Si utiliza un Application Load Balancer o Network Load Balancer en AWS para reemplazar el componente IBM WebSeal, debe configurar la administración de sesiones mediante una instancia de ElastiCache Amazon con un clúster de Memcached y configurar Apache Tomcat para que utilice la administración de sesiones de código abierto.
- Si usa el proxy de reenvío WebSeal de IBM, debe configurar un nuevo equilibrador de carga de red en AWS. Use las direcciones IP proporcionadas por el equilibrador de carga de red para la configuración de uniones WebSeal.
- Configuración SSL: le recomendamos que utilice Secure Sockets Layer (SSL) para las comunicaciones. end-to-end Para configurar un servidor SSL en Apache Tomcat, siga las instrucciones de la documentación de Apache Tomcat.

Arquitectura

Pila de tecnología de origen

- Servidor WebSphere de aplicaciones IBM

Pila de tecnología de destino

- La arquitectura usa Elastic Load Balancing (versión 2). Si usa IBM WebSeal para la gestión de identidades y el equilibrio de carga, puede seleccionar un equilibrador de carga de red en AWS para integrarlo con el proxy inverso IBM WebSeal.

- Las aplicaciones Java se implementan en un servidor de aplicaciones Apache Tomcat. Este se ejecuta en una instancia de EC2 de un grupo de Amazon EC2 Auto Scaling. Puedes configurar una política de escalado basada en CloudWatch las métricas de Amazon, como el uso de la CPU.
- Si va a dejar de utilizar IBM WebSeal para el equilibrio de carga, puede utilizar Amazon for Memcached ElastiCache para la gestión de sesiones.
- En la base de datos de backend, puede implementar alta disponibilidad (Multi-AZ) para Amazon RDS y seleccionar un tipo de motor de base de datos.

Arquitectura de destino

Herramientas

- AWS CloudFormation
- Interfaz de la línea de comandos de AWS (AWS CLI)
- Apache Tomcat (versión 7.x o 8.x)
- RHEL 7 o Centos 7
- Implementación de Amazon RDS Multi-AZ
- Amazon ElastiCache para Memcached (opcional)

Epics

Configure el VPC

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC).		
Cree subredes.		
Cree tablas de enrutamiento si es necesario.		

Tarea	Descripción	Habilidades requeridas
Crear listas de control de acceso (ACL) a la red		
Configure AWS Direct Connect o una conexión VPN corporativa.		

Redefina la plataforma de la aplicación

Tarea	Descripción	Habilidades requeridas
Refactorice la configuración de Maven en compilación de la aplicación para generar los artefactos de WAR.		
Refactorice los orígenes de datos de dependencia de las aplicaciones en Apache Tomcat.		
Refactorice los códigos fuente de las aplicaciones para que usen nombres JNDI en Apache Tomcat.		
Implemente los artefactos WAR en Apache Tomcat.		
Complete las validaciones y pruebas de las aplicaciones.		

Configurar la red

Tarea	Descripción	Habilidades requeridas
Configure el firewall corporativo para permitir la conexión a los servicios de dependencia.		
Configure el firewall corporativo para permitir el acceso de los usuarios finales a Elastic Load Balancing en AWS.		

Cree la infraestructura de aplicaciones

Tarea	Descripción	Habilidades requeridas
Cree e implemente la aplicación en una instancia de EC2.		
Cree un clúster de Amazon ElastiCache for Memcached para la administración de sesiones.		
Cree una instancia de Amazon RDS Multi-AZ para la base de datos de backend.		
Cree certificados SSL e impórtelos a AWS Certificate Manager (ACM).		
Instale certificados SSL en los equilibradores de carga.		

Tarea	Descripción	Habilidades requeridas
Instale certificados SSL para los servidores Apache Tomcat.		
Complete las validaciones y pruebas de las aplicaciones.		

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Desactive la infraestructura existente.		
Restaure la base de datos de producción a Amazon RDS.		
Realice cambios en el DNS para interrumpir la aplicación.		

Recursos relacionados

Referencias

- Documentación de Apache Tomcat 7.0
- Guía de instalación de Apache Tomcat 7.0
- Documentación de JNDI de Apache Tomcat
- Implementaciones Multi-AZ de Amazon RDS
- Amazon ElastiCache para Memcached

Tutoriales y videos

- Introducción a Amazon RDS

Migración de una aplicación .NET de Microsoft Azure App Service a AWS Elastic Beanstalk

Creado por Raghavender Madamshitti (AWS)

Entorno: PoC o piloto	Origen: aplicaciones	Destino: AWS Elastic Beanstalk
Tipo R: redefinir la plataforma	Carga de trabajo: Microsoft	Tecnologías: migración; aplicaciones web y móviles

Resumen

Este patrón describe cómo migrar una aplicación web .NET alojada en Microsoft Azure App Service a AWS Elastic Beanstalk. Hay dos formas de migrar aplicaciones a Elastic Beanstalk:

- Mediante AWS Toolkit para Visual Studio: este complemento para el IDE de Microsoft Visual Studio proporciona la forma más fácil y sencilla de implementar aplicaciones .NET personalizadas en AWS. Puede utilizar este enfoque para implementar código .NET directamente en AWS y crear recursos de apoyo, como Amazon Relational Database Service (Amazon RDS) para bases de datos de SQL Server, directamente desde Visual Studio.
- Mediante carga e implementación en Elastic Beanstalk: cada Azure App Service incluye un servicio en segundo plano llamado Kudu que resulta útil para capturar los volcados de memoria y los registros de implementación, ver los parámetros de configuración y acceder a los paquetes de implementación. Puede usar la consola Kudu para acceder al contenido de Azure App Service, extraer el paquete de implementación y, a continuación, cargar el paquete en Elastic Beanstalk mediante la opción de carga e implementación de la consola de Elastic Beanstalk.

Este patrón describe el segundo enfoque (cargar la aplicación en Elastic Beanstalk a través de Kudu). El patrón también utiliza los siguientes servicios de AWS: AWS Elastic Beanstalk, Amazon Virtual Private Cloud (Amazon VPC), Amazon, Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (CloudWatchAmazon EC2) Auto Scaling, Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) y Amazon Route 53.

La aplicación web .NET se implementa en AWS Elastic Beanstalk, que se ejecuta en un grupo de Amazon EC2 Auto Scaling. Puedes configurar una política de escalado basada en CloudWatch las

métricas de Amazon, como el uso de la CPU. Para una base de datos, puede utilizar Amazon RDS en un entorno Multi-AZ o Amazon DynamoDB, según los requisitos empresariales y de la aplicación.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una aplicación web .NET que se ejecute en Azure App Service
- Permiso para usar la consola Kudu de Azure App Service

Versiones de producto

- .NET Core (x64) 1.0.1, 2.0.0 o posterior, o .NET Framework 4.x, 3.5 (consulte el historial de la plataforma .NET en Windows Server)
- Internet Information Services (IIS) versión 8.0 o posterior que se ejecute en Windows Server 2012 o posterior
- .NET 2.0 o 4.0 Runtime.

Arquitectura

Pila de tecnología de origen

- Aplicación desarrollada con .NET Framework 3.5 o posterior, o .NET Core 1.0.1, 2.0.0 o posterior, y alojada en Azure App Service (aplicación web o aplicación API)

Pila de tecnología de destino

- AWS Elastic Beanstalk en un grupo de Amazon EC2 Auto Scaling

Arquitectura de migración

Flujo de trabajo de una implementación

Herramientas

Herramientas

- .NET Core o .NET Framework
- C#
- IIS
- Consola Kudu

Servicios y características de AWS

- AWS Elastic Beanstalk: Elastic Beanstalk es un servicio para implementar y easy-to-use escalar aplicaciones web.NET. Elastic Beanstalk administra automáticamente el aprovisionamiento de capacidad, el equilibrio de carga y el escalado automático.
- Grupo de escalado automático de Amazon EC2: Elastic Beanstalk incluye un grupo de escalado automático que administra las instancias de Amazon EC2 en el entorno. En un entorno de una sola instancia, el grupo de escalado automático garantiza que siempre haya una instancia en ejecución. En un entorno con equilibrio de carga, se configura el grupo con una serie de instancias para ejecutarse, y Amazon EC2 Auto Scaling agrega o elimina instancias según sea necesario, en función de la carga.
- Elastic Load Balancing: cuando se habilita el equilibrio de carga en AWS Elastic Beanstalk, se crea un equilibrador de carga que distribuye el tráfico entre las instancias de EC2 del entorno.
- Amazon CloudWatch: Elastic Beanstalk CloudWatch utiliza Amazon automáticamente para proporcionar información sobre los recursos de su aplicación y entorno. Amazon CloudWatch admite métricas estándar, métricas personalizadas y alarmas.
- Amazon Route 53: Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad. Puede usar los registros de alias de Route 53 para asignar nombres de dominio personalizados a los entornos de AWS Elastic Beanstalk.

Epics

Configurar una VPC

Tarea	Descripción	Habilidades requeridas
Configure una nube privada virtual (VPC).	En su cuenta de AWS, cree una VPC con la información requerida.	Administrador de sistemas
Cree subredes.	Cree dos o más subredes en la VPC.	Administrador de sistemas
Cree una tabla de enrutamie nto.	Cree una tabla de enrutamie nto según sus necesidades.	Administrador de sistemas

Configurar Elastic Beanstalk

Tarea	Descripción	Habilidades requeridas
Acceda a la consola Kudu de Azure App Service.	Para acceder a Kudu a través del portal de Azure, diríjase al panel de control de App Service y, a continuación, seleccione Advanced Tools (Herramientas avanzadas) y Go (Ir). O bien, puede modificar la URL del servicio de aplicaciones de Azure de la siguiente manera: `https://<appservicename>.scm.azurewebsites.net` .	Desarrollador de aplicaciones, administrador de sistemas
Descargue el paquete de implementación de Kudu.	Navegue a Windows PowerShell seleccionando la DebugConsoleopción. De esta forma se abrirá la consola	Desarrollador de aplicaciones, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	Kudo. Vaya a la carpeta `wwwroot` y descárguela. Se descargará el paquete de implementación de Azure App Service como un archivo zip. Para ver un ejemplo, consulte el archivo adjunto.	
Cree un paquete para Elastic Beanstalk.	Descomprima el paquete de implementación que descargó de Azure App Service. Cree un archivo JSON llamado `aws-windows-deployment-manifest.json` (este archivo solo es necesario para las aplicaciones .NET Core). Cree un archivo zip que incluya el archivo `aws-windows-deployment-manifest.json` del paquete de implementación de Azure App Service. Para ver un ejemplo, consulte el archivo adjunto.	Desarrollador de aplicaciones, administrador de sistemas
Cree una nueva aplicación de Elastic Beanstalk.	Abra la consola de Elastic Beanstalk. Seleccione una aplicación existente o cree una nueva.	Desarrollador de aplicaciones, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Cree el entorno.	En el menú Actions (Acciones) de la consola de Elastic Beanstalk, seleccione Create environment (Crear entorno). Seleccione el entorno del servidor web y la plataform a .NET/IIS. En código de aplicación, seleccione Cargar. Cargue el archivo zip que preparó para Elastic Beanstalk y, a continuación, seleccion e Create Environment (Crear entorno).	Desarrollador de aplicaciones, administrador de sistemas
Configura Amazon CloudWatc h.	De forma predeterminada, la CloudWatch supervisión básica está habilitada. Si desea cambiar la configura ción, en el asistente de Elastic Beanstalk, seleccione la aplicación publicada y, a continuación, Monitoring (Supervisión).	Administrador de sistemas
Compruebe que el paquete de implementación se encuentre en Amazon S3.	Una vez creado el entorno de la aplicación, encontrará el paquete de implementación en el bucket de S3.	Desarrollador de aplicaciones, administrador de sistemas
Probar la aplicación.	Una vez creado el entorno, utilice la URL proporcionada en la consola de Elastic Beanstalk para probar la aplicación.	Administrador de sistemas

Recursos relacionados

- Conceptos AWS Elastic Beanstack (documentación de Elastic Beanstalk)
- Getting Started with .NET on Elastic Beanstalk (Introducción a .NET en Elastic Beanstalk (documentación de Elastic Beanstalk)
- Consola Kudu () GitHub
- Using «Kudu» to Manage Azure Web Apps (Uso de «Kudu» para administrar aplicaciones web de Azure) (artículo de GS Lab)
- Custom ASP.NET Core Elastic Beanstalk Deployments (Implementaciones personalizadas de ASP.NET Core Elastic Beanstalk) (Guía del usuario del kit de herramientas de AWS para Visual Studio)
- Documentación de Elastic Load Balancing
- AWS Elastic Beanstalk Supported Platforms (Plataformas compatibles con AWS Elastic Beanstalk (documentación de Elastic Beanstalk)
- Deploy a Web Application to AWS (Implementación de una aplicación web en AWS) (artículo de C# Corner)
- Scaling the Size of Your Auto Scaling Group (Escalar el tamaño de su grupo de escalado automático) (documentación de EC2)
- High Availability (Multi-AZ) for Amazon RDS (Alta disponibilidad (Multi-AZ) para Amazon RDS) (documentación de Amazon RDS)

Información adicional

Notas

- Si va a migrar una base de datos en las instalaciones o de Azure SQL Server a Amazon RDS, también debe actualizar los detalles de conexión a la base de datos.
- Para realizar las pruebas, se adjunta un ejemplo de aplicación de demostración.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Migración de un entorno de MongoDB autoalojado a MongoDB Atlas en la nube de AWS

Origen: MongoDB	Destino: MongoDB Atlas en AWS	Tipo R: redefinir la plataforma
Entorno: producción	Tecnologías: migración; análisis; bases de datos	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon EC2; Amazon VPC		

Resumen

Este patrón describe los pasos para migrar de un entorno de MongoDB autoadministrado (que incluye MongoDB Community Server, Enterprise Server, Enterprise Advanced, MLab o cualquier clúster de MongoDB administrado) a MongoDB Atlas en la nube de Amazon Web Services (AWS). Utiliza Atlas Live Migration Service para ayudar a acelerar la migración de los datos de MongoDB a MongoDB Atlas.

El patrón complementa la guía Migrating from MongoDB to MongoDB Atlas on the AWS Cloud (Migrar de MongoDB a MongoDB Atlas en la nube de AWS) de las Recomendaciones de AWS. Proporciona los pasos de implementación de la migración.

El patrón se ha diseñado para los socios de AWS Service Integrator de (socios SI) y para los usuarios de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Un entorno MongoDB de origen para migrar a MongoDB Atlas

Experiencia

- Este patrón requiere estar familiarizado con los servicios de MongoDB, MongoDB Atlas y AWS. Para obtener más información, consulte Roles y responsabilidades en la guía Migrar de MongoDB a MongoDB Atlas en la nube de AWS del sitio web de Recomendaciones de AWS.

Versiones de producto

- Para MongoDB versión 2.6 o posterior

Arquitectura

Para ver las arquitecturas de referencia de MongoDB Atlas que admiten diferentes situaciones de uso, consulte Arquitecturas de referencia de MongoDB Atlas en AWS en la guía Migración de MongoDB a MongoDB Atlas en la nube de AWS en el sitio web de Recomendaciones de AWS.

Herramientas

- Atlas Live Migration Service: un programa de utilidad gratuito de MongoDB que ayuda a migrar bases de datos a Atlas. Este servicio mantiene la base de datos de origen sincronizada con la base de datos de destino hasta la transición. Cuando esté todo a punto para realizar la transición, detenga las instancias de la aplicación, diríjalas al clúster Atlas de destino y reinícielas.

Epics

Descubrimiento y evaluación

Tarea	Descripción	Habilidades requeridas
Determine el tamaño del clúster.	Calcule el tamaño del conjunto de trabajo utilizando la información de db.stats( ) para el espacio total del índice. Presuponga que se accederá con frecuenci a a un porcentaje de su espacio de datos. O bien, puede estimar las necesidad es de memoria en función	Administrador de base de datos de MongoDB, arquitecto de aplicaciones

Tarea	Descripción	Habilidades requeridas
	de sus propias presuposi ciones. Esta tarea puede necesitar aproximadamente una semana. Para obtener más información y ejemplos de esta y otras historias de esta Epic, consulta los enlaces de la sección «Recursos relacionados».	

Tarea	Descripción	Habilidades requeridas
Calcule los requisitos de ancho de banda de la red.	Para calcular los requisitos de ancho de banda de la red, multiplique el tamaño medio de los documentos por el número de documentos servidos por segundo. Tenga en cuenta el tráfico máximo que soportará cualquier nodo del clúster como base. Para calcular las velocidades de transferencia de datos descendentes del clúster a las aplicaciones cliente, utilice la suma del total de documentos devueltos durante un período de tiempo. Si sus aplicaciones leen desde nodos secundarios, divida este número total de documentos por el número de nodos que pueden realizar operaciones de lectura. Para encontrar el tamaño medio de los documentos de una base de datos, utilice db.stats (). avgObjSize comando. Esta tarea suele necesitar un día.	Administrador de base de datos de MongoDB
Seleccione la capa de Atlas.	Siga las instrucciones de la documentación de MongoDB para seleccionar la capa del clúster de Atlas correcta.	Administrador de base de datos de MongoDB
Planifique la transición de la aplicación.		Administrador de base de datos de MongoDB, arquitecto de aplicaciones

Configurar un nuevo entorno de MongoDB Atlas en AWS

Tarea	Descripción	Habilidades requeridas
Cree un nuevo clúster de MongoDB Atlas en AWS.	En MongoDB Atlas, seleccione «Build a Cluster» (Crear un clúster) para que aparezca el cuadro de diálogo «Create New Cluster» (Crear nuevo clúster). Seleccione AWS como proveedor de la nube.	Administrador de base de datos de MongoDB
Seleccione las regiones y la configuración del clúster global.	Seleccione una de las regiones de AWS disponibles para su clúster de Atlas. Configure clústeres globales si es necesario.	Administrador de base de datos de MongoDB
Seleccione la capa del clúster.	Seleccione la capa del clúster que prefiera. La selección de la capa determina factores como la memoria, el almacenamiento y las especificaciones de IOPS.	Administrador de base de datos de MongoDB
Configure los ajustes adicionales del clúster.	Configure los ajustes adicionales del clúster, como la versión de MongoDB, la copia de seguridad y las opciones de cifrado. Para obtener más información sobre estas opciones, consulte la sección «Recursos relacionados».	Administrador de base de datos de MongoDB

Configure la seguridad y el cumplimiento

Tarea	Descripción	Habilidades requeridas
Configure la lista de acceso.	Para conectarse al clúster de Atlas, debe agregar una entrada a la lista de acceso del proyecto. Atlas utiliza seguridad de la capa de transporte (TLS) / Capa de conexión segura (SSL) para cifrar las conexiones a la nube privada virtual (VPC) de su base de datos. Para configura r la lista de acceso al proyecto y obtener más información sobre las historias de esta Epic, consulte los enlaces de la sección «Recursos relacionados».	Administrador de base de datos de MongoDB
Autentique y autorice a los usuarios.	Debe crear y autenticar a los usuarios de la base de datos que accederán a los clústeres de MongoDB Atlas. Para acceder a los clústeres de un proyecto, los usuarios deben pertenecer a ese proyecto y pueden pertenecer a varios proyectos.	Administrador de base de datos de MongoDB
Cree roles personalizados.	(Opcional) Atlas admite la creación de roles personali zados en los casos en que los privilegios de usuario integrados en la base de datos	Administrador de base de datos de MongoDB

Tarea	Descripción	Habilidades requeridas
	Atlas no cubran el conjunto de privilegios deseado.	
Configure las interconexiones con VPC.	(Opcional) Atlas admite el emparejamiento de VPC con otras VPC de AWS, Azure o Google Cloud Platform (GCP).	Administrador de base de datos de MongoDB
Configure un PrivateLink punto de conexión de AWS.	(Opcional) Puede configurar puntos de enlace privados en AWS mediante AWS PrivateLink.	Administrador de base de datos de MongoDB
Habilitar la autenticación en dos pasos.	(Opcional) Atlas admite la autenticación en dos pasos (2FA) para ayudar a los usuarios a controlar el acceso a sus cuentas de Atlas.	Administrador de base de datos de MongoDB
Configure la autenticación y la autorización de los usuarios con LDAP.	(Opcional) Atlas admite realizar la autenticación y autorización de los usuarios con el Protocolo ligero de acceso a directorios (LDAP).	Administrador de base de datos de MongoDB
Configure el acceso unificado a AWS.	(Opcional) Algunas características de Atlas, como Atlas Data Lake y el cifrado en reposo mediante la administración de claves de cliente, utilizan las funciones de AWS Identity and Access Management (AWS IAM) para la autenticación.	Administrador de base de datos de MongoDB

Tarea	Descripción	Habilidades requeridas
Configure el cifrado en reposo mediante AWS KMS.	(Opcional) Atlas admite el uso del AWS Key Managemen t System (AWS KMS) para cifrar los motores de almacenamiento y las copias de seguridad del proveedor de la nube.	Administrador de base de datos de MongoDB
Configure el cifrado en el nivel de campo del cliente.	(Opcional) Atlas admite el cifrado en el nivel de campo del cliente, incluido el cifrado automático de los campos.	Administrador de base de datos de MongoDB

Migración de datos

Tarea	Descripción	Habilidades requeridas
Lance el conjunto de réplicas de destino en MongoDB Atlas.	Lance el conjunto de réplicas de destino en MongoDB Atlas. En Atlas Live Migration Service, seleccione «I’m ready to migrate» (Todo está listo para migrar).	Administrador de base de datos de MongoDB
Agregue Atlas Live Migration Service a la lista de acceso de su clúster de origen de AWS.	Esto ayuda a preparar el entorno de origen para conectarse al clúster de Atlas de destino.	Administrador de base de datos de MongoDB
Valide sus credenciales de AWS con Atlas Live Migration Service.	Seleccione «Start Migration » (Iniciar migración). Cuando el botón «Prepare to Cutover» (Preparación de la transición) se ponga en verde, realice la transición. Revise	Administrador de base de datos de MongoDB

Tarea	Descripción	Habilidades requeridas
	las métricas de rendimiento de los clústeres de Atlas.	

Configurar la integración operativa

Tarea	Descripción	Habilidades requeridas
Conéctese al clúster de MongoDB Atlas.		Desarrollador de aplicaciones
Interactúe con los datos del clúster.		Desarrollador de aplicaciones
Supervise los clústeres.		Administrador de base de datos de MongoDB
Realice copias de seguridad y restaure los datos del clúster.		Administrador de base de datos de MongoDB

Recursos relacionados

Guía para la migración

- Migración de MongoDB a MongoDB Atlas en la nube de AWS

Detectar y evaluar

- Memoria
- Ejemplo de dimensionamiento con conjuntos de datos de muestra de Atlas
- Ejemplo de dimensionamiento para aplicaciones móviles
- Tráfico de red
- Escalado automático de clústeres
- Plantilla de dimensionamiento de Atlas

Configure la seguridad y el cumplimiento

- Configurar entradas de la lista de acceso IP
- Configurar usuarios de la base de datos
- Acceso de usuario a Atlas
- Configurar roles personalizados
- Privilegios de usuario de base de datos
- Configurar un emparejamiento de red
- Configurar un punto de conexión privado
- Autenticación en dos pasos
- Configurar la autenticación y la autorización de usuarios con LDAP
- Lago de datos Atlas
- Cifrado en reposo mediante la administración de claves de cliente
- Usar roles de IAM
- Configurar el cifrado en el nivel de campo del cliente
- Configurar el cifrado automático en el nivel de campo del cliente
- Seguridad de MongoDB Atlas
- Centro de confianza de MongoDB
- Características y configuración de seguridad

Configurar un nuevo entorno de MongoDB Atlas en AWS

- Proveedores y regiones de la nube
- Clústeres globales
- Capa de clúster
- Ajustes adicionales del clúster
- Introducción a Atlas
- Acceso de usuario a Atlas
- Clústeres

Migración de datos

- Supervisar los clústeres

Integrar operaciones

- Conectarse a un clúster
- Realizar operaciones CRUD en Atlas
- Supervisar el clúster
- Realizar copias de seguridad y restaurar datos del clúster

Migre de Oracle WebLogic a Apache Tomcat (ToMEE) en Amazon ECS

Tipo R: redefinir la plataforma	Origen: contenedores	Destino: Apache Tomcat (ToMEE) en Amazon ECS
Creado por: AWS	Entorno: PoC o piloto	Tecnologías: contenedores y microservicios; migración
Carga de trabajo: Oracle	Servicios de AWS: Amazon ECS	

Resumen

Este patrón describe los pasos para migrar un sistema Oracle Solaris SPARC local que ejecuta Oracle WebLogic a una instalación basada en contenedores Docker que ejecuta Apache ToMEE (Apache Tomcat con soporte adicional para contenedores) con Amazon Elastic Container Service (Amazon ECS).

Para obtener información sobre la migración de las bases de datos asociadas a las aplicaciones que va a migrar de Oracle a Tomcat, consulte los patrones de migración de bases de datos de este WebLogic catálogo.

Prácticas recomendadas

Los pasos para migrar las aplicaciones web de Java y Java Enterprise Edition (Java EE) varían según la cantidad de recursos específicos del contenedor que utilice la aplicación. Las aplicaciones basadas en Spring suelen ser más fáciles de migrar, ya que tienen un número reducido de dependencias en el contenedor de implementación. Por el contrario, las aplicaciones Java EE que utilizan recursos empresariales JavaBeans (EJB) y de contenedores gestionados, como los grupos de subprocesos, el Servicio de autenticación y autorización de Java (JAAS) y la persistencia gestionada por contenedores (CMP), requieren más esfuerzo.

Las aplicaciones desarrolladas para Oracle Application Server utilizan con frecuencia la suite Oracle Identity Management. Los clientes que migran a servidores de aplicaciones de código abierto suelen optar por volver a implementar la gestión de identidades y accesos mediante una federación basada en SAML. Otros utilizan Oracle HTTP Server Webgate en casos en los que la migración desde la suite Oracle Identity Management no es una opción.

Las aplicaciones web Java y Java EE son excelentes candidatas para su implementación en los servicios de AWS basados en Docker, como AWS Fargate y Amazon ECS. Los clientes suelen elegir una imagen de Docker con la última versión del servidor de aplicaciones de destino (como ToMEE) y el kit de desarrollo de Java (JDK) preinstalados. Instalan sus aplicaciones sobre la imagen de Docker base, la publican en su registro Amazon Elastic Container Registry (Amazon ECR) y la utilizan para la implementación escalable de sus aplicaciones en AWS Fargate o Amazon ECS.

Lo ideal es que la implementación de aplicaciones sea elástico, es decir, que el número de instancias de aplicaciones se amplíe o disminuya en función del tráfico o la carga de trabajo. Esto significa que las instancias de aplicaciones deben estar en línea o cancelarse para ajustar la capacidad a la demanda.

Cuando traslade una aplicación Java a AWS, considere convertirla en apátrida. Este es un principio arquitectónico clave del Marco de AWS Well-Architected que permitirá el escalado horizontal mediante el almacenaje en contenedores. Por ejemplo, la mayoría de las aplicaciones web basadas en Java almacenan la información de las sesiones de los usuarios de forma en las instalaciones. Para sobrevivir a la finalización de la instancia de aplicación debido al escalado automático en Amazon Elastic Compute Cloud (Amazon EC2) o por otros motivos, la información de las sesiones de los usuarios debe almacenarse globalmente para que los usuarios de aplicaciones web puedan seguir trabajando sin problemas y de forma transparente sin tener que volver a conectarse a una aplicación web ni volver a iniciar sesión en ella. Existen varias opciones de arquitectura para este enfoque, como Amazon ElastiCache for Redis o el almacenamiento del estado de la sesión en una base de datos global. Los servidores de aplicaciones, como ToMEE, tienen complementos que permiten almacenar y administrar las sesiones a través de Redis, bases de datos y otros almacenes de datos globales.

Utilice una herramienta común y centralizada de registro y depuración que se integre fácilmente con Amazon CloudWatch y AWS X-Ray. La migración brinda la oportunidad de mejorar las capacidades del ciclo de vida de las aplicaciones. Por ejemplo, es posible que desee automatizar el proceso de creación para que los cambios se puedan realizar fácilmente mediante una canalización de integración y entrega continuas (CI/CD). Esto puede requerir cambios en la aplicación para que pueda implementarse sin tiempo de inactividad.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Código fuente de Java y JDK

- Aplicación de origen creada con Oracle WebLogic
- Solución definida para Identity and Access Management (SAML u Oracle Webgate)
- Solución definida para la gestión de las sesiones de la aplicación (like-for-like trasladarla o con Amazon ElastiCache, o hacer que la aplicación quede sin estado si es necesario)
- Sepa si el equipo necesita refactorizar las bibliotecas específicas de J2EE para poder transferirlas a Apache ToMEE (consulte el estado de implementación de Java EE 7 en el sitio web de Apache)
- Imagen reforzada de ToMEE en función de sus requisitos de seguridad
- Imagen de contenedor con el objetivo ToMee preinstalado
- Se acuerda e implementa la corrección de la aplicación si es necesaria (por ejemplo, registro, depuración, compilación o autenticación)

Versiones de producto

- Oracle WebLogic OC4J, 9i, 10 g
- Tomcat 7 (con Java 1.6 o versiones posteriores)

Arquitectura

Pila de tecnología de origen

- Aplicación web creada con Oracle WebLogic
- Aplicación web que utiliza la autenticación Oracle Webgate o SAML
- Aplicaciones web conectadas a la versión 10g y posteriores de Oracle Database

Pila de tecnología de destino

- ToMEE (Apache Tomcat con soporte adicional para contenedores) que se ejecuta en Amazon ECS (consulte también Implementación de aplicaciones web Java y microservicios Java en Amazon ECS)
- Amazon Relational Database Service (Amazon RDS) para Oracle; para ver las versiones de Oracle compatibles con Amazon RDS, consulte Amazon RDS para Oracle

Arquitectura de destino

Herramientas

Para funcionar en ToMEE, una aplicación Java debe reconstruirse en un archivo.war. En algunos casos, es posible que sea necesario realizar cambios en la aplicación para que funcione en ToMee; debe comprobar que las opciones de configuración y las propiedades del entorno necesarias estén definidas correctamente.

Además, las búsquedas de la interfaz de nombres y directorios de Java (JNDI) y los espacios de nombres de JavaServer páginas (JSP) deben definirse correctamente. Considere la posibilidad de comprobar los nombres de los archivos utilizados por la aplicación para evitar colisiones de nombres con las bibliotecas T integradas. Por ejemplo, persistence.xml es un nombre de archivo utilizado por el marco Apache OpenJPA (que se incluye con OpenEJB en ToMEE) con fines de configuración. El archivo persistence.xml de PUI contiene las declaraciones Bean de Spring Framework.

La versión 7.0.3 y posteriores de ToMee (Tomcat 8.5.7 y posteriores) devuelve una respuesta HTTP 400 (solicitud incorrecta) para las direcciones URL sin procesar (sin codificar) con caracteres especiales. La respuesta del servidor aparece como una página en blanco para el usuario final. Las versiones anteriores de ToMee y Tomcat permitían el uso de ciertos caracteres especiales no codificados en las URL; sin embargo, se considera inseguro, como se indica en el sitio web CVE-2016-6816. Para resolver el problema de codificación de las URL, las URL que se pasan directamente al navegador JavaScript deben codificarse con el método encodeURI () en lugar de utilizarse como cadenas sin procesar.

Tras implementar el archivo.war en ToMEE, supervise el registro de inicio de Linux cat para ver si faltan bibliotecas compartidas y extensiones específicas de Oracle para añadir los componentes que falten de las bibliotecas de Tomcat.

Procedimiento general

- Configure la aplicación en ToMee.
- Identifique y reconfigure los archivos y recursos de configuración específicos del servidor de aplicaciones desde el formato de origen al formato de destino.
- Identifique y reconfigure los recursos de JNDI.
- Ajuste el espacio de nombres y las búsquedas de EJB al formato requerido por el servidor de aplicaciones de destino (si corresponde).
- Reconfigure las funciones de seguridad y las asignaciones principales específicas del contenedor de aplicaciones de JAAS (si corresponde).

- Empaquete la aplicación y las bibliotecas compartidas en un archivo.war.
- Implemente el archivo.war en ToMEE mediante el contenedor de Docker proporcionado.
- Supervise el registro de inicio para identificar cualquier biblioteca compartida o extensión descriptora de implementación que falte. Si encuentra alguna, vuelva a la primera tarea.
- Pruebe la aplicación instalada con la base de datos de Amazon RDS restaurada.
- Inicie la arquitectura completa con un equilibrador de carga y un clúster de Amazon ECS siguiendo las instrucciones de Implementación de contenedores de Docker.
- Actualice las URL para que apunten al equilibrador de carga.
- Actualice la base de datos de administración de configuración (CMDB).

Epics

Planificación de la migración

Tarea	Descripción	Habilidades requeridas
Realice el descubrimiento de aplicaciones (estado actual del entorno y punto de referencia de rendimiento).		BA, líder de migración
Validar versiones y motores de las bases de datos de origen y destino.		Administrador de base de datos
Valide el diseño de la aplicación de origen y destino (gestión de identidades y sesiones).		Administrador de base de datos, ingeniero de migraciones, propietario de la aplicación
Identifique los requisitos de hardware y almacenamiento para la instancia del servidor de destino.		DBA, SysAdmin
Elija el tipo de instancia adecuado en función de la		DBA, SysAdmin

Tarea	Descripción	Habilidades requeridas
capacidad, las características de almacenamiento y las características de red.		
Identifique los requisitos de seguridad de acceso a la red de las bases de datos de origen y destino.		DBA, SysAdmin
Identifique la estrategia y las herramientas de migración de aplicaciones.		Administrador de base de datos, líder de migración
Complete el diseño de la migración y la guía de migración de la aplicación.		Responsable de compilación, líder de migración
Complete el manual de procedimientos de migración de aplicaciones.		Responsable de compilación, líder de transición, líder de pruebas, líder de migración

Configuración de la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC).		SysAdmin
Cree grupos de seguridad.		SysAdmin
Configure e inicie la instancia de base de datos de Amazon RDS.		DBA, SysAdmin
Configure la implementación de Amazon ECS.		SysAdmin

Tarea	Descripción	Habilidades requeridas
Empaquete su aplicación como una imagen de Docker.		SysAdmin
Inserte la imagen en el registro de Amazon ECR (u omita este paso y envíela al clúster de Amazon ECS).		SysAdmin
Configure la definición de tareas para la aplicación y las opciones de servicio de Amazon ECS.		SysAdmin
Configure su clúster, revise los ajustes de seguridad y establezca los roles de AWS Identity and Access Management (IAM).		SysAdmin
Inicie la configuración y ejecute las pruebas de acuerdo con el manual de procedimientos de migración de aplicaciones.		SysAdmin

Migración de datos

Tarea	Descripción	Habilidades requeridas
Obtenga el permiso de su equipo de control de seguridad para trasladar los datos de producción a AWS.		Administrador de base de datos, ingeniero de migracion es, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Cree puntos de conexión y obtenga acceso a ellos para recuperar los archivos de copia de seguridad de la base de datos.		Administrador de base de datos
Utilice el motor de base de datos nativo o herramientas de terceros para migrar los objetos y datos de la base de datos.		Administrador de base de datos
Ejecute las pruebas necesarias del manual de procedimientos de migración de aplicaciones para confirmar que la migración de datos se realizó correctamente.		Administrador de base de datos, ingeniero de migraciones, propietario de la aplicación

Migración de la aplicación

Tarea	Descripción	Habilidades requeridas
Cree una solicitud de cambio (CR) para la migración.		Líder de transición
Obtenga la aprobación de CR para la migración.		Líder de transición
Siga la estrategia de migración de aplicaciones del manual de procedimientos de migración de aplicaciones.		Administrador de base de datos, ingeniero de migraciones, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Actualice la aplicación (si es necesario).		Administrador de base de datos, ingeniero de migracion es, propietario de la aplicación
Realice pruebas funcionales y no funcionales, de validación de datos, de acuerdo de nivel de servicio y de rendimiento.		Líder de pruebas, propietario de la aplicación, usuarios de la aplicación

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Obtenga la aprobación del propietario de la aplicación o de la empresa.		Líder de transición
Realiza un ejercicio sobre un tema de mesa para repasar todos los pasos del manual de procedimientos de transición.		Administrador de base de datos, ingeniero de migracion es, propietario de la aplicación
Cambie los clientes de aplicaciones a la nueva infraestructura.		Administrador de base de datos, ingeniero de migracion es, propietario de la aplicación

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cerrar los recursos temporale s de AWS.		DBA, ingeniero de migración, SysAdmin

Tarea	Descripción	Habilidades requeridas
Revise y valide los documentos del proyecto.		Líder de migración
Recopile métricas sobre el tiempo de migración, el porcentaje de migraciones manuales en comparación con las realizadas con herramientas, el ahorro de costos, etc.		Líder de migración
Cerrar el proyecto y enviar comentarios.		Líder de migración, propietario de la aplicación

Recursos relacionados

Referencias

- Documentación de Apache Tomcat 7.0
- Guía de instalación de Apache Tomcat 7.0
- Documentación de JNDI de Apache Tomcat
- Documentación de Apache ToMee
- Amazon RDS para Oracle
- Precios de Amazon RDS
- Oracle y AWS
- Documentación de Oracle en Amazon RDS
- Implementaciones Multi-AZ de Amazon RDS
- Introducción a Amazon ECS
- Introducción a Amazon RDS

Tutoriales y videos

- Prácticas recomendadas para ejecutar las bases de datos de Oracle en Amazon RDS (re:Invent 2018 presentation)

Migración de una base de datos de Oracle de Amazon EC2 a Amazon RDS para Oracle mediante AWS DMS

Tipo R: redefinir la plataforma	Origen: bases de datos: relacionales	Destino: Amazon RDS para Oracle
Creado por: AWS	Entorno: PoC o piloto	Tecnologías: bases de datos; migración
Carga de trabajo: Oracle	Servicios de AWS: Amazon EC2; Amazon RDS	

Resumen

Este patrón describe los pasos para migrar una base de datos de Oracle en Amazon Elastic Compute Cloud (Amazon EC2) a Amazon Relational Database Service (Amazon RDS) para Oracle usando AWS Database Migration Service (AWS DMS). El patrón también utiliza Oracle SQL Developer o SQL *Plus para conectarse a la instancia de base de datos de Oracle e incluye una CloudFormation plantilla de AWS que automatiza algunas de las tareas.

La migración a Amazon RDS para Oracle le permite centrarse en su empresa y en sus aplicaciones, mientras que Amazon RDS se encarga de las tareas de administración de bases de datos, como el aprovisionamiento de bases de datos, las copias de seguridad y la recuperación, los parches de seguridad, las actualizaciones de versiones y la administración del almacenamiento.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una Imagen de máquina de Amazon (AMI) para Oracle Database en Amazon EC2

Versiones de producto

- AWS DMS es compatible con las versiones de Oracle 11g (versiones 11.2.0.3.v1 y posteriores), 12c y 18c para bases de datos de instancias de Amazon RDS para las ediciones Enterprise,

Standard, Standard One y Standard Two. Para obtener la información más reciente sobre las versiones compatibles, consulte Uso de una base de datos de Oracle como origen para AWS DMS en la documentación de AWS. (Las CloudFormation plantillas de AWS adjuntas utilizan la versión 12c de Oracle como base de datos de origen).

- Desarrollador SQL de Oracle 4.0.3

Arquitectura

Arquitectura de origen

- Base de datos de Oracle en Amazon EC2

Arquitectura de destino

- Amazon RDS para Oracle

Arquitectura de migración

Herramientas

- AWS DMS: AWS Database Migration Service (AWS DMS) le ayuda a migrar los datos de forma rápida y segura a AWS. Admite migraciones homogéneas y heterogéneas. Para obtener información sobre las versiones y ediciones de bases de datos de Oracle compatibles, consulte Uso de una base de datos de Oracle como origen para AWS DMS y Uso de una base de datos de Oracle como destino para AWS DMS en la documentación de AWS.
- Oracle SQL Developer o SQL *Plus: estas herramientas le permiten conectarse a la instancia de base de datos de Amazon RDS para Oracle.

Epics

Configurar la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Crear una instancia de base de datos de Amazon RDS para Oracle.	Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/. Cree una instancia de base de datos de Oracle seleccionando el motor, la plantilla, la configuración de credenciales de base de datos, el tipo de instancia, el almacenamiento, la configuración de multi-AZ, la nube privada virtual (VPC) y la configuración, las credenciales de inicio de sesión y las configuraciones adicionales para la base de datos de Oracle. Para obtener instrucciones, consulte los enlaces de la sección "Recursos relacionados". O utilice la CloudFormation plantilla de AWS (Create_RDS.yaml) del archivo adjunto para crear la instancia de base de datos Amazon RDS for Oracle.	Desarrollador
Conéctese a Amazon RDS y conceda privilegios al usuario de Oracle.	Modifique el grupo de seguridad para abrir los puertos adecuados para conectarse desde la máquina	Desarrollador

Tarea	Descripción	Habilidades requeridas
	local y la instancia de replicación de AWS DMS. Al configurar la conectividad, asegúrese de que la opción «Accesible públicamente» esté seleccionada para poder conectarse a la base de datos desde fuera de la VPC. Conéctese a Amazon RDS con Oracle SQL Developer o SQL *Plus mediante las credenciales de inicio de sesión, cree un usuario de AWS DMS y proporcione los privilegios necesarios al usuario de AWS DMS para modificar la base de datos.	

Configure el grupo de seguridad de la instancia EC2 de origen

Tarea	Descripción	Habilidades requeridas
Compruebe si la base de datos de Oracle está en funcionamiento.	Utilice Secure Shell (SSH) para conectarse a la instancia EC2 e intente conectarse a la base de datos de Oracle mediante SQL *Plus.	Desarrollador
Modifique el grupo de seguridad.	Modifique el grupo de seguridad de la instancia EC2 para abrir los puertos adecuados, de modo que pueda conectarse desde su	Desarrollador

Tarea	Descripción	Habilidades requeridas
	máquina local y la instancia de replicación de AWS DMS.	

Configure AWS DMS

Tarea	Descripción	Habilidades requeridas
Cree una instancia de replicación de AWS DMS.	En AWS DMS, cree una instancia de replicación en la misma VPC que su instancia de base de datos Amazon RDS para Oracle. Especifique el nombre y la descripción de la instancia de replicación, elija la clase de instancia y la versión del motor de replicación (utilice la predeterminada), elija la VPC en la que creó la instancia de base de datos de Amazon RDS, establezca la configuración de multi-AZ en caso necesario, asigne almacenamiento, especifique la zona de disponibilidad y configure ajustes adicionales. Como alternativa, puede usar la CloudFormation plantilla de AWS (DMS.yaml) del archivo adjunto para implementar este paso.	Administrador de base de datos
Conéctese a los puntos de conexión de las bases de datos de origen y destino.	Cree los puntos de conexión de la base de datos de origen y destino especificando el identificador del punto de	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	conexión, el motor, el servidor, el puerto, las credenciales de inicio de sesión y los atributos de conexión adicionales. Para el servidor de origen, utilice el DNS público de la instancia EC2 que aloja la base de datos de Oracle. Para el servidor de destino, utilice el punto de conexión de Amazon RDS para Oracle. Realice una prueba para comprobar que las conexiones de origen y destino funcionan. Como alternativa, puede usar la CloudFormation plantilla de AWS (DMS.yaml) del archivo adjunto para implementar este paso.	

Tarea	Descripción	Habilidades requeridas
Cree una tarea de AWS DMS.	Cree una tarea de AWS DMS para migrar los datos del punto de conexión de origen al punto de conexión de destino, para configurar la replicación entre el punto de conexión de origen y destino, o ambos. Al crear la tarea de AWS DMS, especifique la instancia de replicación, el punto de conexión de origen, el punto de conexión de destino, el tipo de migración (solo datos, solo replicación o ambos), el mapeo de tablas y el filtro. Ejecute la tarea de AWS DMS, supervise la tarea, compruebe las estadísticas de la tabla y compruebe los registros en Amazon CloudWatch. Como alternativa, puede usar la CloudFormation plantilla de AWS (DMS.yaml) del archivo adjunto para implementar este paso.	Administrador de base de datos

Recursos relacionados

- Creación de una instancia de base de datos de Amazon RDS
- Conexión a una instancia de base de datos que ejecuta el motor de base de datos de Oracle
- Documentación de AWS DMS
- AWS DMS Step-by-Step Walkthroughs (Guías paso a paso de AWS DMS)
- Migración de bases de datos de Oracle a la nube de AWS

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Migre una base de datos Oracle local a Amazon OpenSearch Service mediante Logstash

Documento creado por Aditya Goteti (AWS)

Entorno: PoC o piloto	Origen: base de datos de Oracle	Objetivo: Amazon OpenSearch Service
Tipo R: redefinir la plataforma	Carga de trabajo: Oracle	Tecnologías: migración; bases de datos
Servicios de AWS: Amazon OpenSearch Service		

Resumen

Este patrón describe cómo mover datos de una base de datos Oracle local a Amazon OpenSearch Service mediante Logstash. Incluye consideraciones arquitectónicas y algunos conjuntos de habilidades necesarias y recomendaciones. Los datos pueden proceder de una sola tabla o de varias tablas en las que será necesario realizar una búsqueda de texto completo.

OpenSearch El servicio se puede configurar dentro de una nube privada virtual (VPC) o se puede colocar públicamente con restricciones basadas en IP. Este patrón describe un escenario en el que el OpenSearch servicio se configura dentro de una VPC. Logstash se utiliza para recopilar los datos de la base de datos de Oracle, analizarlos en formato JSON y, a continuación, introducir los datos en Service. OpenSearch

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Java 8 (requerido por Logstash 6.4.3)
- Conectividad entre los servidores de bases de datos en las instalaciones y las instancias de Amazon Elastic Compute Cloud (Amazon EC2) en una VPC, establecida mediante AWS Virtual Private Network (AWS VPN)

- Una consulta para recuperar los datos necesarios para enviarlos a OpenSearch Service desde la base de datos
- Controladores de Oracle Java Database Connectivity (JDBC)

Limitaciones

- Logstash no puede identificar los registros que se han eliminado definitivamente de la base de datos

Versiones de producto

- Oracle Database 12c
- OpenSearch Servicio 6.3
- Logstash 6.4.3

Arquitectura

Pila de tecnología de origen

- Base de datos Oracle en las instalaciones
- AWS VPN en las instalaciones

Pila de tecnología de destino

- VPC
- Instancia EC2
- OpenSearch Servicio
- Logstash
- Puerta de enlace NAT (para actualizar el sistema operativo en instancias de EC2 e instalar Java 8, Logstash y complementos)

Arquitectura de migración de datos

Herramientas

- Logstash 6.4.3
- Complemento de entrada JDBC (descarga y más información)
- Complemento de salida de Logstash (logstash-output-amazon_es)
- Controladores JDBC de Oracle

Epics

Planificar la migración

Tarea	Descripción	Habilidades requeridas
Identificar el tamaño de la base de datos de origen.	El tamaño de los datos de origen es uno de los parámetros que se utilizan para determinar el número de particiones que se van a configurar en un índice.	Administrador de base de datos, Desarrollador de base de datos
Analizar los tipos de datos de cada columna y los datos correspondientes.	OpenSearch El servicio mapea dinámicamente el tipo de datos cuando encuentra en el documento un campo que no se había visto anteriorm ente. Si hay algún tipo o formato de datos específic o (por ejemplo, campos de fecha) que deba declararse de forma explícita, identifique los campos y defina la asignació n de esos campos durante la creación del índice.	Propietario de la aplicación, desarrollador, desarrollador de bases de datos
Determinar si hay columnas con claves principales o únicas.	Para evitar la duplicación de registros en Amazon OpenSearch Service durante	Propietario de la aplicación, desarrollador

Tarea	Descripción	Habilidades requeridas
	las actualizaciones o insercion es, debes configurar el `document_id` ajuste en la sección de resultados del `amazon_es` complemento (por ejemplo, `document_id => "%{customer_id}"` dónde `customer_id` está la clave principal).	
Analizar el número y la frecuencia de los nuevos registros que se agregan; comprobar la frecuencia con la que se eliminan los registros.	Esta tarea es necesaria para comprender la tasa de crecimiento de los datos de origen. Si los datos se leen de forma intensiva y las insercion es son poco frecuentes, puede tener un índice único. Si se insertan nuevos registros con frecuencia y no hay eliminaci ones, el tamaño de la partición puede superar fácilmente el tamaño máximo recomenda do de 50 GB. En este caso, se puede crear un índice de forma dinámica configura ndo los patrones de índice en Logstash y en el código al que se puede acceder mediante un alias.	Propietario de la aplicación, desarrollador
Determinar cuántas réplicas se necesitan.		Propietario de la aplicación, desarrollador

Tarea	Descripción	Habilidades requeridas
Determinar la cantidad de particiones que se van a configurar en el índice.		Propietario de la aplicación, desarrollador
Identificar los tipos de instancias para los nodos maestros dedicados, los nodos de datos y la instancia EC2.	Para obtener más información, consulte la sección Recursos relacionados.	Propietario de la aplicación, desarrollador
Determinar el número de nodos maestros dedicados y nodos de datos necesarios.	Para obtener más información, consulte la sección Recursos relacionados.	

Migrar datos

Tarea	Descripción	Habilidades requeridas
Lanzar una instancia EC2.	Lanzar una instancia EC2 dentro de la VPC a la que está conectada la VPN de AWS.	Constructos de Amazon VPC, VPN de AWS
Instalar Logtash en la instancia EC2.		Desarrollador
Instalar los complementos de Logstash.	Instalar los complementos de Logstash necesarios `jdbc-input` y `logstash-output-amazon_es` .	Desarrollador
Configurar Logstash.	Crear el almacén de claves de Logstash para almacenar información confidencial, como las claves de AWS Secrets Manager y las	Desarrollador

Tarea	Descripción	Habilidades requeridas
	credenciales de las bases de datos, y, a continuación, colocar las referencias en un archivo de configuración de Logstash.	
Configurar la cola de mensajes fallidos y la cola persistente.	De forma predeterminada, cuando Logstash detecta un evento que no puede procesar porque los datos contienen un error de mapeo o algún otro problema, la canalización de Logstash bloquea o descarta el evento fallido. Para protegerse de la pérdida de datos en esta situación, puede configurar Logstash para que escriba los eventos fallidos en una cola de mensajes fallidos en lugar de descartarlos. Para evitar la pérdida de datos durante una interrupción anómala, Logstash tiene una caracterí stica de cola persistente que almacenará la cola de mensajes en el disco. Las colas persistentes proporcio nan la durabilidad de los datos en Logstash.	Desarrollador

Tarea	Descripción	Habilidades requeridas
Crea el dominio OpenSearch de Amazon Service.	Cree el dominio de Amazon OpenSearch Service con una política de acceso que no requiera firmar las solicitud es con las credenciales de AWS Identity and Access Management (IAM). El dominio OpenSearch de Amazon Service debe crearse en la misma VPC. También debe seleccionar los tipos de instancias y establecer el número de nodos dedicados y maestros en función de su análisis.	Desarrollador
Configura los registros de Amazon OpenSearch Service necesarios.	Para obtener más información, consulta la documentación del OpenSearch servicio.	
Crear el índice.		Desarrollador
Iniciar Logstash.	Ejecutar Logstash como un servicio en segundo plano. Logstash ejecuta la consulta SQL configurada, extrae los datos, los convierte al formato JSON y los envía a Service. OpenSearch Para la carga inicial, no configure el programador en el archivo de configuración de Logstash.	Desarrollador

Tarea	Descripción	Habilidades requeridas
Consulte los documentos.	Compruebe el número de documentos del índice y si todos los documentos están presentes en la base de datos de origen. Durante la carga inicial, se añaden al índice y se utilizan para detener Logstash. Cambie la configuración de Logstash para agregar un programador que se ejecute en un intervalo fijo según los requisitos del cliente y reinicie Logstash. Logstash seleccionará solo los registros que se hayan actualizado o agregado después de la última ejecución, y la marca temporal de la última ejecución se almacenará en el archivo que está configurado con la propiedad `last_run_metadata_path => “/usr/share/logstash/.logstash_jdbc_last_run”` en el archivo de configuración de Logstash.	Desarrollador

Recursos relacionados

- Alarmas recomendadas CloudWatch
- Nodos maestros OpenSearch de Amazon Service dedicados
- Dimensionamiento de los dominios de Amazon OpenSearch Service

- Documentación de Logstash
- Complemento de entrada JDBC
- Complemento de salida Logstash
- Sitio web OpenSearch de Amazon Service

Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle

Creado por Baji Shaik (AWS) y Pavan Pusuluri (AWS)

Entorno: PoC o piloto	Origen: bases de datos: relacionales	Destino: Amazon RDS para Oracle
Tipo R: redefinir la plataforma	Carga de trabajo: Oracle	Tecnologías: Migración; bases de datos
Servicios de AWS: Amazon RDS; AWS DMS		

Resumen

Este patrón describe los pasos para migrar bases de datos de Oracle en las instalaciones a Amazon Relational Database Service (Amazon RDS) para Oracle. Como parte del proceso de migración, debe crear un plan de migración y tener en cuenta los factores importantes de la infraestructura de la base de datos de destino en función de la base de datos de origen. Puede elegir una de las dos opciones de migración según los requisitos empresariales y el caso de uso:

1. AWS Database Migration Service (AWS DMS): puede usar AWS DMS para migrar bases de datos a la nube de AWS de forma rápida y segura. Su base de datos de origen permanece totalmente operativa durante la migración, lo que minimiza el tiempo de inactividad de las aplicaciones que dependen de ella. Puede reducir el tiempo de migración mediante AWS DMS para crear una tarea que capture los cambios continuos después de completar una migración inicial a carga completa mediante un proceso denominado captura de datos de cambios (CDC). Para obtener más información, consulte Migración de Oracle a Amazon RDS con AWS DMS en la documentación de AWS.
2. Herramientas nativas de Oracle: puede migrar bases de datos mediante herramientas nativas de Oracle, como Oracle y Data Pump Export y Data Pump Import con Oracle GoldenGate for CDC. También puede utilizar herramientas nativas de Oracle, como la utilidad de exportación original y la utilidad de importación original, para reducir el tiempo de carga total.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos de Oracle en las instalaciones
- Una instancia de base de datos (DB) Oracle de Amazon RDS

Limitaciones

- Límite de tamaño de la base de datos: 64 TB

Versiones de producto

- Oracle, versiones 11g (versiones 11.2.0.3.v1 y posteriores) y hasta la 12.2 y la 18c. Para obtener la lista más reciente de versiones y ediciones compatibles, consulte Amazon RDS para Oracle en la documentación de AWS. Para ver las versiones de Oracle compatibles con AWS DMS, consulte Uso de una base de datos de Oracle como origen de AWS DMS en la documentación de AWS DMS.

Arquitectura

Pila de tecnología de origen

- Bases de datos de Oracle en las instalaciones

Pila de tecnología de destino

- Amazon RDS para Oracle

Arquitectura de origen y destino

En el siguiente diagrama se muestra cómo migrar una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle mediante AWS DMS.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Cree o utilice un usuario de base de datos existente, conceda los permisos de AWS DMS necesarios para ese usuario, active el modo ARCHIVELOG y, a continuación, configure el registro adicional.
2. Configure la puerta de enlace de Internet entre la red en las instalaciones y la red de AWS.
3. Configure los puntos de conexión de origen y destino para AWS DMS.
4. Configure las tareas de replicación de AWS DMS para migrar los datos de la base de datos de origen a la base de datos de destino.
5. Complete las actividades posteriores a la migración en la base de datos de destino.

En el siguiente diagrama se muestra cómo migrar una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle mediante herramientas nativas de Oracle.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Cree o utilice un usuario de base de datos existente y otorgue los permisos necesarios para realizar una copia de seguridad de la base de datos de Oracle mediante las utilidades Export (`exp`) e Import (`imp`) de Oracle.
2. Configure la puerta de enlace de Internet entre la red en las instalaciones y la red de AWS.
3. Configure el cliente de Oracle en el host bastión para que tome la base de datos de copias de seguridad.
4. Cargue la copia de seguridad de la base de datos en un bucket de Amazon Simple Storage Service (Amazon S3).
5. Restaure la copia de seguridad de la base de datos de Amazon S3 en una base de datos de Amazon RDS para Oracle.
6. Configure Oracle GoldenGate para CDC.
7. Complete las actividades posteriores a la migración en la base de datos de destino.

Herramientas

- AWS Database Migration Service (AWS DMS) le permite migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en la nube y en las instalaciones.
- Las herramientas nativas de Oracle le ayudan a realizar una migración homogénea. Puede utilizar Oracle Data Pump para migrar datos entre las bases de datos de origen y destino. Este patrón

utiliza Oracle Data Pump para realizar la carga completa desde la base de datos de origen a la base de datos de destino.

- Oracle le GoldenGate ayuda a realizar la replicación lógica entre dos o más bases de datos. Este patrón se utiliza GoldenGate para replicar los cambios delta después de la carga inicial mediante Oracle Data Pump.

Epics

Planificación de la migración

Tarea	Descripción	Habilidades requeridas
Cree documentos del proyecto y registre los detalles de la base de datos.	1. Documente sus objetivos de migración, los requisitos de migración, las principales partes interesadas del proyecto, los hitos del proyecto, los plazos del proyecto, las métricas clave, los riesgos de migración y los planes de mitigación de riesgos. 2. Documente la información fundamental sobre su base de datos de origen, incluida la RAM, las IOPS y las CPU. Más adelante, utilizará esta información para determinar la instancia de base de datos de destino adecuada. 3. Valide las versiones de sus bases de datos de origen y destino.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Identifique los requisitos de almacenamiento.	Identifique y documente sus requisitos de almacenamiento, incluidos los siguientes: 1. Calcule el almacenamiento asignado para la instancia de la base de datos de origen. 2. Recopile las métricas de crecimiento históricas de la instancia de la base de datos de origen. 3. Pronostique el crecimiento futuro para la instancia de la base de datos objetivo. Nota: En el caso de los volúmenes SSD de uso general (gp2), se obtienen tres IOPS por cada 1 GB de almacenamiento. Asigne el almacenamiento calculando el número total de IOPS de lectura y escritura en la base de datos de origen.	DBA, SysAdmin

Tarea	Descripción	Habilidades requeridas
Elija el tipo de instancia adecuado en función de los requisitos de procesamiento.	1. Determine los requisitos de procesamiento de la instancia de base de datos de destino. 2. Identifique problemas de rendimiento. 3. Tenga en cuenta los factores para determinar el tipo de instancia adecuado: • Utilización de la CPU de la instancia de base de datos de origen • IOPS (lectura y escritura) para la instancia de base de datos de origen • Huella de memoria en la instancia de la base de datos de origen	SysAdmin
Identifique los requisitos de seguridad de acceso a la red.	1. Identifique y documente los requisitos de seguridad de acceso a la red para sus bases de datos de origen y destino. 2. Configure los grupos de seguridad adecuados para permitir que la aplicación se comunique con la base de datos.	DBA, SysAdmin

Tarea	Descripción	Habilidades requeridas
Identificar la estrategia de migración de aplicaciones.	1. Determine y documente la estrategia de transición a la migración. 2. Determine y documente el objetivo de tiempo de recuperación (RTO) y el objetivo de punto de recuperación (RPO) de su aplicación y, a continuación, planifique la transición en consecuencia.	DBA, propietario de la aplicación SysAdmin

Tarea	Descripción	Habilidades requeridas
Identifique los riesgos de migración.	Evalúe la base de datos y documente los riesgos y mitigaciones específicos de la migración. Por ejemplo: • Identifique tablas sin registro y destaque el riesgo de pérdida de datos en caso de recuperación. • Extraiga los usuarios y privilegios de la base de datos de origen y destaque los conflictos con los privilegios de Amazon RDS. • Revise el registro de alertas para ver si hay errores o advertencias específicos de Oracle. • Identifique las caracterí sticas compatibles y no compatibles de la instancia de base de datos de destino. • Revise las características obsoletas del motor de la versión de base de datos de destino.	Administrador de base de datos

Configuración de la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una VPC.	Cree una nueva Amazon Virtual Private Cloud (Amazon VPC) para la instancia de base de datos de destino.	SysAdmin
Cree grupos de seguridad.	Cree un grupo de seguridad en la nueva VPC para permitir las conexiones entrantes a la instancia de base de datos.	SysAdmin
Crear una instancia de base de datos de Amazon RDS para Oracle.	Cree la instancia de base de datos de destino con la nueva VPC y el nuevo grupo de seguridad y, a continuación, inicie la instancia.	SysAdmin

(Opción 1) Utilice herramientas nativas de Oracle o de terceros para migrar los datos

Tarea	Descripción	Habilidades requeridas
Prepare la base de datos de origen.	1. Cree un directorio de Data Pump o utilice uno existente. 2. Cree un usuario de migración y conceda permisos para realizar la extracción de Data Pump. 3. Extraiga los roles, los usuarios y los espacios de tabla de la base de datos de origen como un script SQL.	DBA, SysAdmin

Tarea	Descripción	Habilidades requeridas
	4. Transfiera el volcado de Data Pump extraído al directorio `data pump` de la instancia de la base de datos de destino.	

Tarea	Descripción	Habilidades requeridas
Prepare la base de datos de destino.	1. Confirme que todas las opciones de base de datos (por ejemplo, texto y Java) estén instaladas o habilitadas en la instancia de base de datos de Amazon RDS para Oracle. 2. Cree un directorio de Data Pump o utilice uno existente. 3. Cree un usuario de migración y conceda permisos para realizar la importación de Data Pump. 4. Cree los espacios de tabla, los usuarios y los roles necesarios en la instancia de base de datos de destino. 5. Importe el volcado de exportación de Data Pump transferido a la base de datos de destino. 6. Cree los índices excluidos durante la importación o la creación del objeto. 7. Cree cualquier restricción excluida durante la importación. 8. Valide o vuelva a compilar los objetos no válidos. 9. Reconstruya los índices no válidos.	DBA, SysAdmin

Tarea	Descripción	Habilidades requeridas
	10. Valide los recuentos de objetos de la base de datos entre las bases de datos de origen y destino. 11. Resuelva cualquier discrepancia que se encuentre entre los recuentos de objetos.	

(Opción 2) Utilice AWS DMS para migrar datos

Tarea	Descripción	Habilidades requeridas
Prepare los datos.	1. Limpie los datos de la base de datos de origen. 2. Cree una instancia de replicación. 3. Cree un punto de conexión de origen y un punto de conexión de destino. 4. Identifique el número de tablas y objetos que se van a migrar.	Administrador de base de datos
Migre los datos.	1. Elimine las restricciones y los disparadores de clave externa en la base de datos de destino. 2. Elimine los índices secundarios en la base de datos de destino. 3. Configure los ajustes de tareas de carga completa	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	de AWS DMS desde la base de datos de origen a la base de datos de destino. 4. Habilite claves externas. 5. Permita que AWS DMS CDC replique los cambios en curso. 6. Active los desencade nadores. 7. Actualice las secuencias. 8. Valide los datos de origen y destino.	

Realizar la transición a la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Cambie los clientes de aplicaciones a la nueva infraestructura.	1. Detenga todos los servicios de aplicaciones y las conexiones de clientes que apunten a Oracle. 2. Ejecute las tareas de AWS DMS. 3. Configure una tarea de reversión (por ejemplo, revierta el CDC de la base de datos de Amazon RDS a la base de datos de Oracle en las instalaciones). 4. Valide los datos. 5. Inicie los servicios de la aplicación en la nueva	DBA, propietario de la SysAdmin aplicación

Tarea	Descripción	Habilidades requeridas
	base de datos de destino configurando Amazon Route 53 en la nueva instancia de base de datos de Amazon RDS para Oracle. 6. Añada la CloudWatch monitorización de Amazon a su nueva instancia de base de datos de Amazon RDS for Oracle.	
Implemente su plan de reversión.	1. Detenga todos los servicios de aplicaciones que apunten a la instancia de base de datos de Amazon RDS para Oracle. 2. Revierta los cambios en la base de datos de Oracle en las instalaciones de origen mediante una tarea de AWS DMS. 3. Detenga la ejecución de las tareas de AWS DMS desde la base de datos de Oracle en las instalaciones a la base de datos Amazon RDS para Oracle. 4. Vuelva a configurar las aplicaciones en la base de datos de Oracle de origen. 5. Confirme que se ha completado la implement ación de la reversión.	Administrador de base de datos, propietario de la aplicación

Cerrar el proyecto de migración

Tarea	Descripción	Habilidades requeridas
Limpiar recursos.	Cierre o elimine los recursos temporales de AWS, como la instancia de replicación de AWS DMS y el bucket de S3.	DBA, SysAdmin
Revise los documentos del proyecto.	Revise los documentos y objetivos de planificación de la migración y, a continuación, confirme que ha completado todos los pasos de migración necesarios.	DBA, propietario de la SysAdmin aplicación
Recopile métricas.	Registre las métricas clave de la migración, como el tiempo que se tardó en completar la migración, el porcentaje de tareas manuales en comparación con las tareas basadas en herramientas, el ahorro de costos y otras métricas relevantes.	DBA, propietario de la SysAdmin aplicación
Cerrar el proyecto.	Cierre el proyecto de migración y obtenga comentarios sobre el esfuerzo.	DBA, propietario de la SysAdmin aplicación

Recursos relacionados

Referencias

- Estrategias para migrar bases de datos de Oracle a AWS (documento técnico de AWS)
- AWS Database Migration Service (AWS DMS) (documentación de AWS DMS)
- Precios de Amazon RDS (documentación de Amazon RDS)

Tutoriales y videos

- Introducción a AWS Database Migration Service (AWS DMS) (documentación de AWS DMS)
- Recursos de Amazon RDS (documentación de Amazon RDS)
- AWS Database Migration Service (DMS) (YouTube)

Migrar una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle mediante Oracle Data Pump

Documento creado por Mohan Annam (AWS) y Brian Motzer (AWS)

Entorno: PoC o piloto	Origen: bases de datos: relacionales	Destino: Amazon RDS para Oracle
Tipo R: redefinir la plataforma	Carga de trabajo: Oracle	Tecnologías: migración; bases de datos
Servicios de AWS: Amazon RDS		

Resumen

Este patrón describe cómo migrar una base de datos de Oracle de un centro de datos en las instalaciones a una instancia de base de datos de Amazon Relational Database Service (Amazon RDS) para Oracle mediante Oracle Data Pump.

El patrón implica crear un archivo de volcado de datos a partir de la base de datos de origen, almacenar el archivo en un bucket de Amazon Simple Storage Service (Amazon S3) y, a continuación, restaurar los datos en una instancia de base de datos de Amazon RDS para Oracle. Este patrón resulta útil cuando se encuentra con limitaciones al utilizar AWS Database Migration Service (AWS DMS) para la migración.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Los permisos necesarios para crear roles en AWS Identity and Access Management (IAM) y para la carga multiparte a Amazon S3
- Los permisos necesarios para exportar datos desde la base de datos de origen
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada

Versiones de producto

- Oracle Data Pump solo está disponible para Oracle Database 10g, versión 1 (10.1) y versiones posteriores.

Arquitectura

Pila de tecnología de origen

- Bases de datos Oracle en las instalaciones

Pila de tecnología de destino

- Amazon RDS para Oracle
- Cliente SQL (desarrollador de Oracle SQL)
- Un bucket de S3

Arquitectura de origen y destino

Herramientas

Servicios de AWS

- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos. En este patrón, la IAM se utiliza para crear los roles y políticas necesarios para migrar datos de Amazon S3 a Amazon RDS para Oracle.
- Amazon Relational Database Service (Amazon RDS) para Oracle le ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Otras herramientas

- Oracle Data Pump le ayuda a trasladar datos y metadatos de una base de datos y otra a altas velocidades. En este patrón, Oracle Data Pump se utiliza para exportar el archivo de volcado de

datos (.dmp) al servidor de Oracle e importarlo a Amazon RDS para Oracle. Para obtener más información, consulte Importación de datos a Oracle en Amazon RDS en la documentación de Amazon RDS.

- Oracle SQL Developer es un entorno de desarrollo integrado que simplifica el desarrollo y la administración de bases de datos de Oracle, tanto en implementaciones tradicionales como en implementaciones basadas en la nube. Interactúa con la base de datos Oracle en las instalaciones y con Amazon RDS para Oracle para ejecutar los comandos SQL necesarios para exportar e importar datos.

Epics

Cree un bucket de S3

Tarea	Descripción	Habilidades requeridas
Crear el bucket.	Para crear el bucket de S3, siga las instrucciones que figuran en la Documentación de AWS.	Administrador de sistemas de AWS

Crear el rol de IAM y asignar políticas

Tarea	Descripción	Habilidades requeridas
Configurar los permisos de IAM.	Para configurar los permisos, siga las instrucciones que figuran en la Documentación de AWS.	Administrador de sistemas de AWS

Crear la instancia de base de datos de Amazon RDS para Oracle y asociar el rol de integración de Amazon S3

Tarea	Descripción	Habilidades requeridas
Crear la instancia de la base de datos de destino de Amazon RDS para Oracle.	Para crear la instancia de Amazon RDS para Oracle, siga las instrucciones que figuran en la Documentación de AWS.	Administrador de sistemas de AWS
Asociar el rol con la instancia de base de datos.	Para asociar el rol a la instancia, siga las instrucciones que figuran en la Documentación de AWS.	Administrador de base de datos

Crear el usuario de la base de datos en la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Crear el usuario .	Conectarse a la base de datos de destino de Amazon RDS para Oracle desde Oracle SQL Developer o SQL*Plus y ejecutar el siguiente comando SQL para crear el usuario al que importar el esquema. `create user SAMPLE_SCHEMA identified by <PASSWORD>;` `grant create session, resource to <USER NAME>;` `alter user <USER NAME> quota 100M on users;`	Administrador de base de datos

Crear el archivo de exportación a partir de la base de datos Oracle de origen

Tarea	Descripción	Habilidades requeridas
Crear un archivo de volcado de datos.	Para crear un archivo de volcado con el nombre `sample.dmp` indicado en el directorio `DATA_PUMP_DIR` para exportar al usuario `SAMPLE_SCHEMA`, utilice el siguiente script. `DECLARE` `hdnl NUMBER;` `BEGIN` `hdnl := dbms_data pump.open(operation => 'EXPORT',` `job_mode => 'SCHEMA',` `job_name => NULL);` `dbms_datapump.add_ file( handle => hdnl,` `filename => 'sample.dmp',` `directory => 'DATA_PUMP_DIR',` `filetype => dbms_datapump.ku$_ file_type_dump_file);` `dbms_datapump.add_ file(handle => hdnl,`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	<pre>filename => 'export.log', directory => 'DATA_PUMP_DIR', filetype => dbms_datapump.ku$_file_type_log_file); dbms_datapump.metadata_filter(hdnl, 'SCHEMA_EXPR', 'IN ('''SAMPLE_SCHEMA''')'); dbms_datapump.start_job(hdnl); END; /</pre> Revise los detalles de la exportación revisando el archivo `export.log` en su directorio `DATA_PUMP_DIR` local.	

Cargue el archivo de volcado en el bucket de S3

Tarea	Descripción	Habilidades requeridas
Cargar el archivo de volcado de datos desde el origen hasta el bucket de S3.	Ejecute el siguiente comando utilizando AWS CLI.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`aws s3 cp sample.dmp s3://<bucket_created_epic_1>/`	

Descargar el archivo de exportación del bucket de S3 en la instancia de RDS

Tarea	Descripción	Habilidades requeridas
Descargar el archivo de volcado de datos en Amazon RDS	Para copiar el archivo de volcado `sample.dmp` desde el bucket de S3 hasta la base de datos de Amazon RDS para Oracle, ejecute el siguiente comando SQL. En este ejemplo, el archivo `sample.dmp` se descarga del bucket de S3 `my-s3-integration1` al directorio de Oracle `DATA_PUMP_DIR`. Asegúrese de tener suficiente espacio en el disco asignado a la instancia de RDS para alojar tanto la base de datos como el archivo de exportación. `-- If you want to download all the files in the S3 bucket remove the p_s3_prefix line.` `SELECT rdsadmin.rdsadmin_s3_tasks.download_from_s3(`	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	p_bucket_name => 'my-s3-integration', p_s3_prefix => 'sample.dmp', p_directory_name => 'DATA_PUMP_DIR') AS TASK_ID FROM DUAL; El comando anterior genera un ID de tarea. Para revisar el estado de la descarga mediante la revisión de los datos en el ID de tarea, ejecute el siguiente comando. SELECT text FROM table(rdsadmin.rds_file_util.read_text_file('BDUMP','dbtask-<task_id>.log')); Para ver los archivos en el directorio DATA_PUMP_DIR , ejecute el comando siguiente en el directorio. SELECT filename, type,filesize/1024 /1024 size_megs ,to_char(mtime,'DD -MON-YY HH24:MI:SS') timestamp FROM TABLE(rdsadmin.rds_file_util.listdir (p_directory =>	

Tarea	Descripción	Habilidades requeridas
	upper('DATA_PUMP_DIR'))) order by 4;	

Importar el archivo de volcado a la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Restaurar el esquema y los datos en Amazon RDS.	Para importar el archivo de volcado al esquema de la base de datos `sample_schema`, ejecute el siguiente comando SQL desde SQL Developer o SQL*Plus. `DECLARE hdnl NUMBER; BEGIN hdnl := DBMS_DATAPUMP.OPEN(operation => 'IMPORT', job_mode => 'SCHEMA', job_name=>null); DBMS_DATAPUMP.ADD_FILE(handle => hdnl, filename => 'sample.dmp', directory => 'DATA_PUMP_DIR', filetype => dbms_datapump.ku$_file_type_dump_file); DBMS_DATAPUMP.ADD_FILE(handle => hdnl, filename => 'import.log', directory => 'DATA_PUMP_DIR',`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	filetype => dbms_datapump.ku$_file_type_log_file); DBMS_DATAPUMP.METADATA_FILTER(hdnl,'SCHEMA_EXPR','IN (''SAMPLE_SCHEMA'')'); DBMS_DATAPUMP.START_JOB(hdnl); END; / Para ver el archivo de registro de la importación, ejecute el siguiente comando. SELECT text FROM table(rdsadmin.rds_file_util.read_text_file('DATA_PUMP_DIR','import.log'));	

Eliminar el archivo de volcado del directorio DATA_PUMP_DIR

Tarea	Descripción	Habilidades requeridas
Enumerar y limpiar los archivos de exportación.	Para enumerar y eliminar los archivos de exportación en el directorio DATA_PUMP_DIR , ejecute los siguientes comandos. -- List the files	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	`SELECT filename, type,filesize/1024 /1024 size_megs ,to_char(mtime,'DD -MON-YY HH24:MI:S S') timestamp FROM TABLE(rdsadmin.rds _file_util.listdir (p_directory => upper('DATA_PUMP_D IR'))) order by 4;` `-- Remove the files EXEC UTL_FILE. FREMOVE('DATA_PUMP _DIR','sample.dmp'); EXEC UTL_FILE.FREMOVE(' DATA_PUMP_DIR','im port.log');`	

Recursos relacionados

- Integración de Amazon S3
- Crear una instancia de base de datos
- Importación de datos a Oracle en Amazon RDS
- Documentación de Amazon S3
- documentación de IAM
- Documentación de Amazon RDS
- Documentación de Oracle Data Pump
- Oracle SQL Developer

Migre de PostgreSQL en Amazon EC2 a Amazon RDS para PostgreSQL mediante pglogical

Creado por Rajesh Madiwale (AWS)

Entorno: PoC o piloto	Origen: Amazon EC2	Destino: Amazon RDS para PostgreSQL
Tipo R: redefinir la plataforma	Carga de trabajo: código abierto	Tecnologías: Migración; bases de datos
Servicios de AWS: Amazon RDS		

Resumen

Este patrón describe los pasos para migrar una base de datos PostgreSQL (versión 9.5 y posteriores) de Amazon Elastic Compute Cloud (Amazon EC2) a Amazon Relational Database Service (Amazon RDS) para PostgreSQL mediante la extensión pglogical de PostgreSQL. Amazon RDS ahora admite la extensión pglogical en la extensión para PostgreSQL versión 10.

Requisitos previos y limitaciones

Requisitos previos

- Elija el tipo correcto de instancia de Amazon RDS. Para obtener más información, consulte Tipos de instancia Amazon RDS.
- Asegúrese de que las versiones de origen y destino de PostgreSQL sean las mismas.
- Instale e integre la extensión pglogical con PostgreSQL en Amazon EC2.

Versiones de producto

- PostgreSQL versión 10 y posteriores en Amazon RDS, con las funciones compatibles con Amazon RDS (consulte PostgreSQL en Amazon RDS en la documentación de AWS). Este patrón se probó migrando PostgreSQL 9.5 a la versión 10 de PostgreSQL en Amazon RDS, pero también se aplica a versiones posteriores de PostgreSQL en Amazon RDS.

Arquitectura

Arquitectura de migración de datos

Herramientas

- extensión pglogic
- Utilidades nativas de PostgreSQL: pg_dump y pg_restore

Epics

Migre los datos mediante la extensión pglogical

Tarea	Descripción	Habilidades requeridas
Crear una instancia de base de datos PostgreSQL en Amazon RDS.	Configurar una instancia de base de datos de Amazon RDS. Para obtener instrucciones, consulte la documentación de Amazon RDS para PostgreSQL.	Administrador de base de datos
Obtenga un volcado de esquema de la base de datos PostgreSQL de origen y restaúrelo en la base de datos PostgreSQL de destino.	1. Utilice la utilidad pg_dump con la opción `-s` de generar un archivo de esquema a partir de la base de datos de origen. 2. Utilice la utilidad psql con la opción `-f` de cargar el esquema en la base de datos de destino.	Administrador de base de datos
Habilita la decodificación lógica.	En el grupo de parámetros de base de datos de Amazon RDS, defina el parámetro estático `rds.logic`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`al_replication` como 1. Para obtener instrucciones, consulte la Documentación de Amazon RDS.	
Cree la extensión pglogical en las bases de datos de origen y destino.	1. Cree la extensión `pglogical` en la base de datos PostgreSQL de origen: `psql -h <amazon-ec2-endpoint> -d target-dbname -U target-dbuser -c "create extension pglogical ;"` 2. Cree la extensión `pglogical` en la base de datos PostgreSQL de destino: `psql -h <amazon-rds-endpoint> -d source-dbname -U source-dbuser -c "create extension pglogical ;"`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree un publicador en la base de datos PostgreSQL de origen.	Para crear un publicador, ejecute: `psql -d dbname -p 5432 <<EOF SELECT pglogical .create_n ode( node_name := 'provider1', dsn := 'host=<ec2-endpoin t> port=5432 dbname=so urce-dbname user=sour ce-dbuser' ); EOF`	Administrador de base de datos
Cree un conjunto de réplicas, añada tablas y secuencias.	Para crear un conjunto de réplicas en la base de datos PostgreSQL de origen y añadir tablas y secuencias al conjunto de réplicas, ejecute: `psql -d dbname -p 5432 <<EOF SELECT pglogical .replication_set_a dd_all_tables('def ault', '{public} '::text[],synchron ize_data := true); EOF`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Crear un suscriptor.	Para crear un suscriptor en la base de datos PostgreSQL de destino, ejecute: `psql -h <rds-endpoint> -d target-dbname -U target-dbuser <<EOF SELECT pglogical.create_node( node_name := 'subscriber1', dsn := 'host=<rds-endpoint> port=5432 dbname=target-dbname password=postgres user=target-dbuser' ); EOF`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Crear una suscripción.	Para crear una suscripción en la base de datos PostgreSQL de destino, ejecute: `psql -h <rds-endpoint> -d target -U postgres <<EOF SELECT pglogical.create_subscription( subscription_name := 'subscription1', replication_sets := array['default'], provider_dsn := 'host=<ec2-endpoint> port=5432 dbname=<source-dbname> password=<password> user=source-dbuser' );`	Administrador de base de datos

Validación de sus datos

Tarea	Descripción	Habilidades requeridas
Compruebe las bases de datos de origen y destino.	Compruebe las bases de datos de origen y destino para confirmar que los datos se están replicando correctamente. Puede realizar una validación básica utilizando las tablas `select count(1)` de origen y destino.	Administrador de base de datos

Recursos relacionados

- Amazon RDS
- Replicación lógica para PostgreSQL en Amazon RDS (documentación de Amazon RDS)
- pglogical (repositorio) GitHub
- Limitaciones de pglogical (archivo README del repositorio) GitHub
- Migración de PostgreSQL de un entorno en las instalaciones o de Amazon EC2 a Amazon RDS mediante la replicación lógica (blog de AWS Database)

Migrar una base de datos PostgreSQL en las instalaciones a Aurora PostgreSQL

Creado por Baji Shaik (AWS) y Jitender Kumar (AWS)

Entorno: PoC o piloto	Origen: base de datos PostgreSQL en las instalaciones	Destino: Aurora compatible con PostgreSQL
Tipo R: redefinir la plataforma	Carga de trabajo: código abierto	Tecnologías: migración; bases de datos
Servicios de AWS: Amazon Aurora; AWS DMS		

Resumen

La edición Amazon Aurora compatible con PostgreSQL que combina el rendimiento y la disponibilidad de las bases de datos comerciales de gama alta con la simplicidad y la rentabilidad de las bases de datos de código abierto. Aurora ofrece estos beneficios al escalar el almacenamiento en tres zonas de disponibilidad en la misma región de AWS y admite hasta 15 instancias de réplica de lectura para escalar horizontalmente las cargas de trabajo de lectura y proporcionar alta disponibilidad en una sola región. Al utilizar una base de datos global Aurora, puede replicar las bases de datos PostgreSQL en hasta cinco regiones para el acceso remoto de lectura y la recuperación de desastres en caso de que se produzca un error en una región. Este patrón describe los pasos para migrar una base de datos de origen de PostgreSQL en las instalaciones a una base de datos de Aurora compatible con PostgreSQL. El patrón incluye dos opciones de migración: usar AWS Data Migration Service (AWS DMS) o usar herramientas nativas de PostgreSQL (como pg_dump, pg_restore y psql) o herramientas de terceros.

Los pasos descritos en este patrón también se aplican a bases de datos PostgreSQL de destino en instancias de Amazon Relational Database Service (Amazon RDS) y de Amazon Elastic Compute Cloud (Amazon EC2).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Base de datos de origen de PostgreSQL en un centro de datos en las instalaciones.
- Una instancia de base de datos Aurora compatible con PostgreSQL o una instancia de base de datos de Amazon RDS para PostgreSQL.

Limitaciones

- Los límites de tamaño de la base de datos son 64 TB para Amazon RDS para PostgreSQL y 128 TB para Aurora compatible con PostgreSQL.
- Si utiliza la opción de migración a AWS DMS, consulte las Limitaciones del uso de una base de datos PostgreSQL como fuente de DMS.

Versiones de producto

- Para obtener información sobre el soporte de las versiones principal y secundaria de PostgreSQL en Amazon RDS, consulte Actualizaciones de Amazon RDS para PostgreSQL en la documentación de Amazon RDS.
- Para obtener información sobre la compatibilidad con PostgreSQL en Aurora, consulte Amazon Aurora PostgreSQL updates en la documentación de Aurora.
- Si utiliza la opción de migración a AWS DMS, consulte las versiones de PostgreSQL compatibles en la documentación de AWS DMS.

Arquitectura

Pila de tecnología de origen

- Base de datos PostgreSQL en las instalaciones

Pila de tecnología de destino

- Instancia de base de datos de Aurora compatible con PostgreSQL

Arquitectura de origen

Arquitectura de destino

Arquitectura de migración de datos

Uso de AWS DMS

Uso de herramientas nativas de PostgreSQL

Herramientas

- AWS Database Migration Service (AWS DMS) lo ayuda a migrar los almacenes de datos a la nube de AWS o entre combinaciones de configuraciones en las instalaciones y en la nube. Este servicio admite diferentes bases de datos de origen y destino. Para obtener información sobre cómo validar las versiones y ediciones de las bases de datos de origen y destino de PostgreSQL compatibles para su uso con AWS DMS, consulte Using a PostgreSQL database as an AWS DMS source. Le recomendamos utilizar la versión más reciente de AWS DMS para obtener el soporte de versiones y características más completo.
- Entre las herramientas nativas de PostgreSQL, se incluyen pg_dump, pg_restore y psql.

Epics

Analice la migración

Tarea	Descripción	Habilidades requeridas
Valide las versiones de las bases de datos de origen y de destino.	Si utiliza AWS DMS, asegúrese de que esté utilizando una versión compatible de PostgreSQL.	Administrador de base de datos
Identifique el tipo de almacenamiento y los requisitos de capacidad.	1. Calcule el almacenamiento asignado para la instancia de base de datos de origen.	Administrador de base de datos, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	2. Recopile las métricas de crecimiento históricas de la instancia de base de datos de origen. 3. Anticipe la previsión de crecimiento futuro de la instancia de base de datos de destino. 4. Calcule el número total de IOPS de lectura y escritura en la base de datos de origen para asignar el almacenamiento. Un volumen SSD de uso general (gp2) proporciona 3 IOPS por cada 1 GB de almacenamiento.	

Tarea	Descripción	Habilidades requeridas
Elija el tipo de instancia, la capacidad, las caracterí sticas de almacenamiento y las características de red adecuadas.	Determine los requisitos de procesamiento de la instancia de base de datos de destino. Revise los problemas de rendimiento conocidos que puedan necesitar más atención. Tenga en cuenta los siguientes factores para determinar el tipo de instancia adecuado: • Utilización de la CPU de la instancia de base de datos de origen • IOPS (operaciones de lectura y escritura) para la instancia de base de datos de origen • Huella de memoria en la instancia de base de datos de origen Para obtener más información, consulte Clases de instancia de base de datos de Aurora en la documentación de Aurora.	Administrador de base de datos, administrador de sistemas
Identifique los requisitos de seguridad de acceso a la red para las bases de datos de origen y destino.	Determine los grupos de seguridad adecuados que permitirían a la aplicación comunicarse con la base de datos.	Administrador de base de datos, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Identificar la estrategia de migración de aplicaciones.	• Determine la estrategia de transición de la migración en función de la complejidad de su aplicación. • Determine el objetivo de tiempo de recuperación (RTO) y el objetivo de punto de recuperación (RPO) para la aplicación, y planifique la transición según correspon da.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Configure la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una VPC.	Cree una nueva nube privada virtual (VPC) para la instancia de base de datos de destino.	Administrador de sistemas
Cree grupos de seguridad.	Cree un grupo de seguridad dentro de la VPC (como se determinó en la epopeya anterior) para permitir las conexiones entrantes a la instancia de base de datos.	Administrador de sistemas
Configure e inicie el clúster de base de datos Aurora.	Cree la instancia de base de datos de destino con la nueva VPC y el nuevo grupo de seguridad, e inicie la instancia.	Administrador de sistemas

Migración de datos: opción 1 (con AWS DMS)

Tarea	Descripción	Habilidades requeridas
Complete los pasos previos a la migración.	1. Limpie los datos de la base de datos de origen. 2. Cree una instancia de replicación. 3. Cree los puntos de conexión de origen y de destino. 4. Identifique el número de tablas y objetos disponibles que se van a migrar.	Administrador de base de datos
Complete los pasos de migración.	1. Elimine las restricciones y los disparadores de clave externa en la base de datos de destino. 2. Elimine los índices secundarios en la base de datos de destino. 3. Utilice una tarea de carga completa para migrar los datos de la base de datos de origen a la de destino. 4. Habilite claves externas. 5. Si utiliza una migración instantánea y su aplicación requiere un tiempo de inactividad mínimo, habilite la captura de datos de cambios (CDC) para replicar los cambios en curso	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	6. Active los desencade nadores. 7. Actualice las secuencias. 8. Valide los datos de origen y destino.	
Valide los datos.	Para asegurarse de que los datos se migraron con precisión del origen al destino, siga los pasos de validación de datos de la documentación de AWS DMS.	Administrador de base de datos

Migración de datos: opción 2 (con pg_dump y pg_restore)

Tarea	Descripción	Habilidades requeridas
Prepare la base de datos de origen.	1. Cree un directorio para almacenar la copia de seguridad de pg_dump si aún no existe. 2. Cree un usuario de migración que tenga permisos para ejecutar pg_dump en los objetos de la base de datos. 3. Conéctese a la instancia de EC2 y ejecute pg_dump backup. Para obtener más informaci ón, consulte la documentación	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	de pg_dump y el tutorial en la documentación de AWS DMS.	
Prepare la base de datos de destino.	1. Cree un usuario de migración que tenga permisos para usar pg_restore en los objetos de la base de datos. 2. Importe el volcado de la base de datos mediante pg_restore. Para obtener más informaci ón, consulte la documentación de pg_restore y el tutorial en la documentación de AWS DMS.	Administrador de base de datos
Valide los datos.	1. Compare los recuentos de objetos de la base de datos entre las bases de datos de origen y destino. 2. Resuelva cualquier discrepancia que se encuentre entre los recuentos de objetos.	Administrador de base de datos

Migrar la aplicación

Tarea	Descripción	Habilidades requeridas
Seguir la estrategia de migración de aplicaciones.	Implemente la estrategia de migración de aplicaciones que creó en la primera epopeya.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Realizar la transición a la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Cambiar los clientes de la aplicación a la nueva infraestructura.	1. Detenga todos los servicios de aplicaciones y las conexiones de cliente que apunten a la base de datos PostgreSQL en las instalaciones. 2. Ejecute las tareas de AWS DMS. 3. Configure una tarea de reversión (cambie el CDC de la base de datos de Aurora compatible con PostgreSQL a la base de datos PostgreSQL en las instalaciones) si es necesario. 4. Valide los datos. 5. Para iniciar los servicios de la aplicación en el nuevo destino, configure Amazon Route 53 en la nueva instancia de base de datos de Aurora compatible con PostgreSQL. 6. Añada la supervisión de Amazon CloudWatch y Performance Insights a su nueva instancia de base de datos Aurora compatible con PostgreSQL.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Si necesita revertir la migración, haga lo siguiente.	1. Detenga todos los servicios de aplicaciones que apuntan a la base de datos de Aurora compatible con PostgreSQL. 2. Revierta los cambios en la base de datos PostgreSQL en las instalaciones de origen mediante la tarea de AWS DMS que creó en la historia anterior. 3. Detenga la ejecución de las tareas de AWS DMS desde la base de datos PostgreSQL en las instalaciones a la base de datos de Aurora compatible con PostgreSQL. 4. Configure la aplicación para que apunte de nuevo a la base de datos PostgreSQL en las instalaciones de origen. 5. Confirme que se haya completado toda la implementación de la reversión.	Administrador de base de datos, propietario de la aplicación

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cierre los recursos.	Cerrar los recursos temporales de AWS.	Administrador de base de datos, administrador de sistemas
Valide los documentos.	Revise y valide los documentos del proyecto.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas
Recopile métricas.	Recopile métricas sobre el tiempo de migración, el porcentaje de tareas manuales en comparación con las tareas automatizadas, el ahorro de costos, etc.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas
Cierre el proyecto.	Cierre el proyecto y envíe sus comentarios.	Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Recursos relacionados

Referencias

- AWS Database Migration Service (AWS DMS)
- VPC de Amazon y Amazon Aurora
- Precios de Amazon Aurora
- Using a PostgreSQL database as an AWS DMS source
- How to create an AWS DMS replication instance
- How to create source and target endpoints using AWS DMS

Recursos adicionales

- Introducción a AWS Database Migration Service (AWS DMS)
- step-by-step Tutoriales sobre la migración de datos
- Recursos de Amazon Aurora

Migración de una base de datos de Microsoft SQL Server en las instalaciones a Microsoft SQL Server en Amazon EC2 con Linux

Creado por Tirumala Dasari (AWS)

Entorno: PoC o piloto	Origen: bases de datos: relacionales	Destino: Amazon EC2 Linux con Microsoft SQL Server
Tipo R: redefinir la plataforma	Carga de trabajo: Microsoft	Tecnologías: migración; bases de datos
Servicios de AWS: Amazon EC2		

Resumen

Este patrón describe cómo migrar de una base de datos Microsoft SQL Server en las instalaciones que se ejecuta en Microsoft Windows a Microsoft SQL Server en una instancia de Linux de Amazon Elastic Compute Cloud (Amazon EC2) mediante utilidades de copia de seguridad y restauración.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- AMI de Amazon EC2 Linux (Imagen de máquina de Amazon) con Microsoft SQL Server
- AWS Direct Connect entre Windows en las instalaciones y Microsoft SQL Server en la instancia EC2 de Linux

Arquitectura

Pila de tecnología de origen

- Base de datos de Microsoft SQL Server en las instalaciones

Pila de tecnología de destino

- instancia EC2 de Linux con una base de datos de Microsoft SQL Server

Arquitectura de migración de base de datos

Herramientas

- WinSCP: esta herramienta permite a los usuarios de Windows compartir archivos fácilmente con los usuarios de Linux.
- Sqlcmd: esta utilidad de línea de comandos le permite enviar expresiones o lotes de T-SQL a instancias locales y remotas de SQL Server. La utilidad es extremadamente útil para tareas repetitivas de bases de datos, como el procesamiento por lotes o las pruebas unitarias.

Epics

Prepare la instancia EC2 de Linux con SQL Server

Tarea	Descripción	Habilidades requeridas
Seleccione una AMI que proporcione el sistema operativo Linux e incluya Microsoft SQL Server.		Sysadmin
Configure la AMI para crear una instancia de EC2.		Sysadmin
Cree reglas de entrada y de salida para los grupos de seguridad.		Sysadmin
Configure la instancia EC2 de Linux para una base de datos de Microsoft SQL Server.		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree usuarios y proporcione permisos como en la base de datos de origen.		Appowner, Administrador de base de datos
Instale las herramientas de SQL Server y la utilidad sqlcmd en la instancia EC2 de Linux.		Administrador de base de datos

Realice una copia de seguridad de la base de datos y mueva el archivo de copia de seguridad a la instancia EC2 de Linux

Tarea	Descripción	Habilidades requeridas
Realice una copia de seguridad de la base de datos de SQL Server en las instalaciones.		Administrador de base de datos
Instale WinSCP en Microsoft SQL Server.		Administrador de base de datos
Mueva el archivo de copia de seguridad a la instancia EC2 de Linux que ejecute Microsoft SQL Server.		Administrador de base de datos

Restaure la base de datos en una instancia EC2 de Linux que ejecute SQL Server

Tarea	Descripción	Habilidades requeridas
Restaure la base de datos desde el archivo de copia de		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
seguridad de la base de datos mediante la utilidad sqlcmd.		
Valide los objetos y datos de la base de datos.		Desarrollador, ingeniero de pruebas

Transicione de una instancia EC2 de Windows SQL Server a una instancia EC2 de Windows SQL Server en Linux

Tarea	Descripción	Habilidades requeridas
Valide los objetos y datos de la base de datos.		Desarrollador, ingeniero de pruebas
Transicione de una base de datos de Microsoft SQL Server en las instalaciones a la instancia EC2 de Linux que ejecute Microsoft SQL Server.		Administrador de base de datos

Recursos relacionados

- Cómo configurar SQL Server 2017 en las AMI de Amazon Linux 2 y Ubuntu
- Instalación de herramientas SQL en una instancia de Linux
- Copia de seguridad y restauración desde una base de datos de Microsoft SQL Server en las instalaciones a Microsoft SQL Server en una instancia EC2 de Linux

Migración de bases de datos en las instalaciones de Microsoft SQL Server a Amazon RDS para SQL Server mediante servidores vinculados

Tipo R: redefinir la plataforma	Origen: bases de datos: relacionales	Destino: Amazon RDS para Microsoft SQL Server
Creado por: AWS	Entorno: producción	Tecnologías: bases de datos; migración
Carga de trabajo: Microsoft	Servicios de AWS: Amazon RDS	

Resumen

Los servidores vinculados permiten a Microsoft SQL Server ejecutar expresiones SQL en otras instancias de servidores de bases de datos. Este patrón describe cómo puede migrar su base de datos en las instalaciones de Microsoft SQL Server a Amazon Relational Database Service (Amazon RDS) para Microsoft SQL Server a fin de reducir los costos y aumentar la disponibilidad. En la actualidad, Amazon RDS para Microsoft SQL Server no admite conexiones fuera de una red de Amazon Virtual Private Cloud (Amazon VPC).

Puede utilizar este patrón para lograr los siguientes objetivos:

- Migrar Microsoft SQL Server a Amazon RDS para Microsoft SQL Server sin interrumpir las capacidades del servidor vinculado.
- Priorizar y migrar Microsoft SQL Server vinculado en diferentes oleadas.

Requisitos previos y limitaciones

Requisitos previos

- Compruebe si Microsoft SQL Server en Amazon RDS admite las características que necesita.
- Asegúrese de que puede utilizar Amazon RDS para Microsoft SQL Server con las intercalaciones predeterminadas o las intercalaciones configuradas en los niveles de la base de datos.

Arquitectura

Pila de tecnología de origen

- Base de datos en las instalaciones (Microsoft SQL Server)

Pila de tecnología de destino

- Amazon RDS para SQL Server

Arquitectura de estado de origen

Arquitectura de estado de destino

En el estado de destino, se migra Microsoft SQL Server a Amazon RDS para Microsoft SQL Server mediante servidores vinculados. Esta arquitectura utiliza un Equilibrador de carga de red para enviar por proxy el tráfico de Amazon RDS para Microsoft SQL Server a los servidores en las instalaciones que ejecutan Microsoft SQL Server. El siguiente diagrama muestra la capacidad de proxy inverso del Equilibrador de carga de red.

Herramientas

- AWS CloudFormation
- Equilibrador de carga de red

- Amazon RDS para SQL Server en zonas de disponibilidad múltiple (Multi-AZS)
- AWS Database Migration Service (AWS DMS)

Epics

Crear una VPC de zona de aterrizaje

Tarea	Descripción	Habilidades requeridas
Cree la asignación del CIDR.		AWS SysAdmin
Cree una nube privada virtual (VPC).		AWS SysAdmin
Cree las redes de la VPC.		AWS SysAdmin
Cree las listas de control de acceso (ACL) a la subred.		AWS SysAdmin
Cree las rutas de enrutamie nto de subred.		AWS SysAdmin
Cree una conexión con AWS Direct Connect o una red privada virtual (VPN) de AWS.		AWS SysAdmin

Migración de una base de datos a Amazon RDS

Tarea	Descripción	Habilidades requeridas
Cree una instancia de base de datos de Amazon RDS para Microsoft SQL Server.		AWS SysAdmin
Cree una instancia de replicaci ón de AWS DMS.		AWS SysAdmin

Tarea	Descripción	Habilidades requeridas
Cree puntos de conexión de bases de datos de origen y de destino en AWS DMS.		AWS SysAdmin
Cree la tarea de migración y active la replicación continua después de una carga completa.		AWS SysAdmin
Solicite un cambio de firewall para permitir que Amazon RDS para Microsoft SQL Server acceda a las bases de datos de SQL Server en las instalaciones.		AWS SysAdmin
Crear un equilibrador de carga de red.		AWS SysAdmin
Cree un grupo de destino que se dirija a los servidores de bases de datos de su centro de datos	Le recomendamos que utilice nombres de host en la configuración de destino para incorporar los eventos de conmutación por error del centro de datos (DC).	AWS SysAdmin

Tarea	Descripción	Habilidades requeridas
Ejecute la expresión SQL para la configuración del servidor vinculado.	Ejecute las expresiones SQL para añadir un servidor vinculado mediante la herramienta de administr ación de Microsoft SQL en la instancia de base de datos Amazon RDS para Microsoft SQL Server. En la expresión SQL, configure @datasrc para que utilice el nombre de host de Equilibrador de carga de red. Añada credencia les de inicio de sesión de servidor vinculado mediante la herramienta de administr ación de Microsoft SQL en la instancia de base de datos Amazon RDS para Microsoft SQL Server.	AWS SysAdmin
Pruebe y valide las funciones de SQL Server.		AWS SysAdmin
Cree una transición.		AWS SysAdmin

Recursos relacionados

- Tareas de administración frecuentes para Microsoft SQL Server en Amazon RDS
- Intercalaciones y conjuntos de caracteres para Microsoft SQL Server
- Documentación del Equilibrador de carga de red
- Implementación de servidores vinculados con Amazon RDS para Microsoft SQL Server (entrada del blog)

Migre una base de datos de Microsoft SQL Server en las instalaciones a Amazon RDS para SQL Server mediante métodos nativos de copia de seguridad y restauración

Creado por Tirumala Dasari (AWS), David Queiroz (AWS) y Vishal Singh (AWS)

Entorno: PoC o piloto	Origen: base de datos de Microsoft SQL Server en las instalaciones	Destino: Amazon RDS para SQL Server
Tipo R: redefinir la plataforma	Carga de trabajo: Microsoft	Tecnologías: migración; bases de datos; sistemas operativos
Servicios de AWS: Amazon RDS; Amazon S3		

Resumen

Este patrón describe cómo migrar una base de datos de Microsoft SQL Server en las instalaciones a una instancia de base de datos de Amazon Relational Database Service (Amazon RDS) para SQL Server (migración homogénea). El proceso de migración se basa en los métodos nativos de copia de seguridad y restauración de SQL Server. Utiliza SQL Server Management Studio (SSMS) para crear un archivo de copia de seguridad de la base de datos y un bucket de Amazon Simple Storage Service (Amazon S3) para almacenar el archivo de copia de seguridad antes de restaurarlo en Amazon RDS para SQL Server.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Políticas de rol de AWS Identity and Access Management (IAM) para el acceso al bucket de S3 y a la instancia de base de datos de Amazon RDS para SQL Server.

Limitaciones

- El proceso descrito en este patrón migra solo la base de datos. Los inicios de sesión de SQL o los usuarios de bases de datos, incluidos los trabajos de SQL Server Agent, no se migran porque requieren pasos adicionales.

Versiones de producto

- SQL Server 2012-2017. Para ver la lista actualizada de versiones compatibles, consulte MySQL en Amazon RDS en la documentación de AWS.

Arquitectura

Pila de tecnología de origen

- Base de datos de Microsoft SQL Server en las instalaciones

Pila de tecnología de destino

- Instancia de base de datos de Amazon RDS para SQL Server

Arquitectura de migración de datos

Herramientas

- Microsoft SQL Server Management Studio (SSMS) es un entorno integrado para administrar infraestructuras de SQL Server. Proporciona una interfaz de usuario y un grupo de herramientas con editores de scripts enriquecidos que interactúan con SQL Server.

Epics

Cree una instancia de base de datos de Amazon RDS para SQL Server

Tarea	Descripción	Habilidades requeridas
Seleccione SQL Server como motor de base de datos en		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Amazon RDS para SQL Server.		
Seleccione SQL Server Express Edition.		Administrador de base de datos
Especifique los detalles de la base de datos.	Para obtener más informaci ón acerca de cómo crear una instancia de base de datos, consulte la documentación de Amazon RDS.	Administrador de base de datos, propietario de la aplicación

Cree un archivo de copia de seguridad a partir de la base de datos de SQL Server en las instalaciones

Tarea	Descripción	Habilidades requeridas
Conéctese a la base de datos de SQL Server en las instalaci ones mediante SSMS.		Administrador de base de datos
Cree una copia de seguridad de la base de datos.	Para obtener instrucciones, consulte la documentación de SSMS.	Administrador de base de datos, propietario de la aplicación

Cargue el archivo de copia de seguridad en Amazon S3

Tarea	Descripción	Habilidades requeridas
Cree un bucket de Amazon S3.	Para obtener más información, consulte la documentación de Amazon S3.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cargue el archivo de copia de seguridad en el bucket de S3.	Para obtener más información, consulte la documentación de Amazon S3.	SysOps administrador

Restaure la base de datos en Amazon RDS para SQL Server

Tarea	Descripción	Habilidades requeridas
Añada el grupo de opciones a Amazon RDS.	1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/. 2. En el panel de navegación, elija Option grupos (Grupos de opciones), Create gropu (Crear grupo). 3. Complete la información del grupo de opciones y, a continuación, seleccione Create (Crear). 4. Añada la opción `SQLSERVER_BACKUP_RESTORE` al grupo de opciones y, a continuación, elija Add option (Añadir opción). Para obtener más información, consulte la documentación de Amazon RDS.	SysOps administrador

Tarea	Descripción	Habilidades requeridas
Restaure la base de datos.	1. Conéctese a Amazon RDS para SQL Server mediante SSMS. 2. Para restaurar la base de datos, llame al procedimiento almacenado `msdb.dbo.rds_restore_database` .	Administrador de base de datos

Valide la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Valide los objetos y los datos.	Valide los objetos y los datos entre la base de datos de origen y Amazon RDS para SQL Server. Nota: esta tarea solo migra la base de datos. Los inicios de sesión y los trabajos no se migrarán.	Administrador de base de datos, propietario de la aplicación

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Redirija el tráfico de la aplicación.	Tras la validación, redirija el tráfico de la aplicación a la instancia de base de datos Amazon RDS para SQL Server.	Administrador de base de datos, propietario de la aplicación

Recursos relacionados

- Documentación de Amazon S3
- Documentación de Amazon RDS para SQL Server
- Opciones para el motor de base de datos de Microsoft SQL Server

Migración de una base de datos de Microsoft SQL Server a Aurora MySQL mediante AWS DMS y AWS SCT

Tipo R: redefinir la plataforma	Origen: bases de datos: relacionales	Destino: Amazon Aurora MySQL
Creado por: AWS	Entorno: PoC o piloto	Tecnologías: bases de datos; migración
Carga de trabajo: Microsoft	Servicios de AWS: Amazon Aurora	

Resumen

Este patrón describe cómo migrar una base de datos de Microsoft SQL Server que se encuentra en las instalaciones o en una instancia de Amazon Elastic Compute Cloud (Amazon EC2) a Amazon Aurora MySQL. Este patrón utiliza AWS Database Migration Service (AWS DMS) y Herramienta de conversión de esquemas de AWS (AWS SCT) para la migración de datos y la conversión de esquemas.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos de origen de Microsoft SQL Server en un centro de datos en las instalaciones o en una instancia de EC2
- Controladores de conectividad de bases de datos Java (JDBC) para conectores de AWS SCT instalados en un equipo local o en la instancia de EC2 en la que está instalado AWS SCT

Limitaciones

- Límite de tamaño de la base de datos: 64 TB

Versiones de producto

- Versiones de Microsoft SQL Server 2008, 2008R2, 2012, 2014, 2016 y 2017 para las ediciones Enterprise, Standard, Workgroup y Developer. Las ediciones Web y Express no son compatibles con AWS DMS. Para ver la lista actualizada de versiones compatibles, consulte Using a Microsoft SQL Server Database as a Source for AWS DMS (Usar una base de datos de Microsoft SQL Server como fuente de AWS DMS). Le recomendamos utilizar la versión más reciente de AWS DMS para obtener el soporte más completo de versiones y características. Para obtener información sobre las versiones de Microsoft SQL Server compatibles con AWS SCT, consulte la documentación de AWS SCT.
- Versiones de MySQL 5.5, 5.6 y 5.7. Para ver la lista actualizada de versiones compatibles, consulte Using a MySQL-Compatible Database as a Target for AWS DMS (Usar una base de datos compatible con MySQL como destino para AWS DMS).

Arquitectura

Pila de tecnología de origen

Uno de los siguientes:

- Base de datos de Microsoft SQL Server en las instalaciones
- Una base de datos de Microsoft SQL Server en una instancia de EC2

Pila de tecnología de destino

- Aurora MySQL

Arquitectura de migración de datos

- Desde una base de datos de Microsoft SQL Server que se ejecute en la nube de AWS

- Una base de datos de Microsoft SQL Server que se ejecute en un centro de datos en las instalaciones

Herramientas

- AWS DMS: AWS Data Migration Service (AWS DMS) le permite migrar datos hacia y desde bases de datos comerciales y de código abierto muy utilizadas, incluidas Oracle, SQL Server, MySQL y PostgreSQL. Puede utilizar AWS DMS para migrar datos a la nube de AWS, entre instancias en las instalaciones (a través de una configuración de nube de AWS) o entre combinaciones de configuraciones en las instalaciones y en la nube.
- AWS SCT: La Herramienta de conversión de esquemas de AWS (AWS SCT) gestiona las migraciones de bases de datos heterogéneas al convertir automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado a un formato compatible con la base de datos de destino.

Epics

Preparación para la migración

Tarea	Descripción	Habilidades requeridas
Valide la versión y el motor de la base de datos de origen y de destino.		Administrador de base de datos
Cree un grupo de seguridad saliente para las bases de datos de origen y destino.		SysAdmin
Cree y configure una instancia de EC2 para AWS SCT, si es necesario.		Administrador de base de datos
Descargue la versión más reciente de AWS SCT y los controladores asociados.		Administrador de base de datos
Agregue y valide los usuarios y permisos de los requisitos		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
previos en la base de datos de origen.		
Cree un proyecto de AWS SCT para la carga de trabajo y conéctese a la base de datos de origen.		Administrador de base de datos
Genere un informe de evaluación y evalúe la viabilidad.		Administrador de base de datos

Prepare la base de datos de destino

Tarea	Descripción	Habilidades requeridas
Cree una instancia de base de datos de Amazon RDS de destino con Amazon Aurora como motor de base de datos.		Administrador de base de datos
Extraiga la lista de usuarios, roles y permisos del origen.		Administrador de base de datos
Asigne los usuarios existente s de la base de datos a los nuevos usuarios de la base de datos.		Propietario de la aplicación
Cree usuarios en la base de datos de destino.		Administrador de base de datos
Aplique los roles del paso anterior a la base de datos de destino.		Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Revise las opciones, los parámetros, los archivos de red y los enlaces de la base de datos de origen y, a continuación, evalúe su aplicabilidad a la base de datos de destino.		Administrador de base de datos
Aplique cualquier configuración pertinente al destino.		Administrador de base de datos

Transferir objetos

Tarea	Descripción	Habilidades requeridas
Configure la conectividad de AWS SCT con la base de datos de destino.		Administrador de base de datos
Convierta el esquema con AWS SCT.	AWS SCT convierte automáticamente el esquema de la base de datos de origen y la mayor parte del código personalizado a un formato compatible con la base de datos de destino. Cualquier código que la herramienta no pueda convertir automáticamente está claramente marcado para que pueda convertirlo usted mismo.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Revise el informe SQL generado y guarde los errores y advertencias.		Administrador de base de datos
Aplique los cambios de esquema automatizados al destino o guárdelos como un archivo .sql.		Administrador de base de datos
Valide que AWS SCT haya creado los objetos en el destino.		Administrador de base de datos
Reescriba, rechace o rediseñe manualmente cualquier elemento que no se haya podido convertir automátic amente.		Administrador de base de datos
Aplique los permisos de rol y de usuario generados y revise cualquier excepción.		Administrador de base de datos

Migración de datos

Tarea	Descripción	Habilidades requeridas
Determine el método de migración.		Administrador de base de datos
Cree una instancia de replicaci ón desde la consola de AWS DMS.	Para obtener más informaci ón sobre el uso de AWS DMS, consulte los enlaces de la sección “Recursos relaciona dos”.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Cree los puntos de conexión de origen y de destino.		Administrador de base de datos
Cree una tarea de replicación.		Administrador de base de datos
Inicie la tarea de replicación y supervise los registros.		Administrador de base de datos

Migración de la aplicación

Tarea	Descripción	Habilidades requeridas
Utilice AWS SCT para analizar y convertir los elementos de SQL del código de la aplicación.	Al convertir su esquema de base de datos de un motor a otro, también deberá actualizar el código SQL de las aplicaciones para interactuar con el nuevo motor de base de datos en lugar del antiguo. Puede ver, analizar, editar y guardar el código SQL convertido. Para obtener más información sobre el uso de AWS SCT, consulte los enlaces de la sección “Recursos relacionados”.	Propietario de la aplicación
Cree los nuevos servidores de aplicaciones en AWS.		Propietario de la aplicación
Migre el código de la aplicación a los nuevos servidores.		Propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
Configure el servidor de aplicaciones para los controladores y la base de datos de destino.		Propietario de la aplicación
Corrija cualquier código específico del motor de base de datos de origen de la aplicación.		Propietario de la aplicación
Optimice el código de la aplicación para el motor de destino.		Propietario de la aplicación

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Aplique al destino los nuevos usuarios, los permisos y los cambios de código.		Administrador de base de datos
Bloquee la aplicación para cualquier cambio.		Propietario de la aplicación
Valide que todos los cambios se hayan propagado a la base de datos de destino.		Administrador de base de datos
Apunte el nuevo servidor de la aplicación hacia la base de datos de destino.		Propietario de la aplicación
Vuelva a comprobar todo.		Propietario de la aplicación
Realice la puesta en marcha.		Propietario de la aplicación

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cierre los recursos temporales de AWS (la instancia de replicación de AWS DMS y la instancia EC2 utilizadas para AWS SCT).		Administrador de base de datos, propietario de la aplicación
Actualice los comentarios sobre el proceso de AWS DMS para los equipos internos.		Administrador de base de datos, propietario de la aplicación
Revise el proceso de AWS DMS y mejore la plantilla si es necesario.		Administrador de base de datos, propietario de la aplicación
Revise y valide los documentos del proyecto.		Administrador de base de datos, propietario de la aplicación
Recopile métricas sobre el tiempo de migración, el porcentaje de ahorro de costos manuales en comparación con los de herramientas, etc.		Administrador de base de datos, propietario de la aplicación
Cierre el proyecto y envíe sus comentarios.		Administrador de base de datos, propietario de la aplicación

Recursos relacionados

Referencias

- Guía del usuario de AWS DMS
- Guía del usuario de AWS SCT
- Precios de Amazon Aurora

Tutoriales y videos

- Getting Started with AWS Database Migration Service (AWS DMS) (Introducción a AWS Database Migration Service (AWS DMS))
- Introducción a la Herramienta de conversión de esquemas de AWS
- Recursos de Amazon RDS
- AWS DMS Step-by-Step Walkthroughs (Guías paso a paso de AWS DMS)

Migración de una base de datos de MariaDB en las instalaciones hasta Amazon RDS para MariaDB mediante herramientas nativas

Creado por Shyam Sunder Rakhecha (AWS)

Entorno: PoC o piloto	Origen: bases de datos: relacionales	Destino: Amazon RDS para MariaDB
Tipo R: redefinir la plataforma	Carga de trabajo: código abierto	Tecnologías: migración; bases de datos

Resumen

Este patrón proporciona una guía para migrar una base de datos de MariaDB en las instalaciones a Amazon Relational Database Service (Amazon RDS) para MariaDB mediante herramientas nativas. Si tiene instaladas las herramientas de MySQL, puede utilizar mysql y mysqldump. Si tiene instaladas todas las herramientas de MariaDB, puede utilizar mariadb y mariadb-dump. Las herramientas MySQL y MariaDB tienen el mismo origen, pero hay pequeñas diferencias en la versión 10.6 de MariaDB y las posteriores.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una base de datos de origen MariaDB en un centro de datos en las instalaciones

Limitaciones

- Límite de tamaño de la base de datos: 64 TB

Versiones de producto

- MariaDB, versiones 10.0-10.6 (para ver la lista actualizada de versiones compatibles, consulte MariaDB en Amazon RDS en la documentación de AWS)

Arquitectura

Pila de tecnología de origen

- Base de datos MariaDB en un centro de datos en las instalaciones

Pila de tecnología de destino

- Instancia de base de datos Amazon RDS para MariaDB

Arquitectura de destino

Arquitectura de migración de datos

Herramientas

- Herramientas nativas de MySQL: mysql y mysqldump
- Herramientas nativas de MariaDB: mariadb y mariadb-dump

Epics

Planificación de la migración

Tarea	Descripción	Habilidades requeridas
Validar versiones y motores de las bases de datos de origen y destino.		Administrador de base de datos
Identifique los requisitos de hardware de la instancia del servidor de destino.		Administrador de base de datos, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
Identifique los requisitos de almacenamiento (como el tipo y la capacidad de almacenamiento).		Administrador de base de datos, administrador de sistemas
Elija el tipo de instancia adecuado en función de la capacidad, las características de almacenamiento y las características de red.		Administrador de base de datos, administrador de sistemas
Identificar los requisitos de seguridad del acceso a la red para las bases de datos de origen y destino.		Administrador de base de datos, administrador de sistemas
Identificar la estrategia de migración de aplicaciones.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Configuración de la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC).		Administrador de sistemas
Cree grupos de seguridad.		Administrador de sistemas
Configurar e iniciar una instancia de base de datos de Amazon RDS que ejecute MariaDB.		Administrador de sistemas

Migración de datos

Tarea	Descripción	Habilidades requeridas
Utilizar herramientas nativas para migrar objetos y datos de las bases de datos.	En la base de datos de origen, utilice mysqldump o mariadb-dump para crear un archivo de salida que contenga objetos y datos de la base de datos. En la base de datos de destino, utilice mysql o mariadb para restaurar los datos.	Administrador de base de datos
Valide los datos.	Compruebe las bases de datos de origen y destino para confirmar que la migración de datos se ha realizado correctamente.	Administrador de base de datos

Migración de la aplicación

Tarea	Descripción	Habilidades requeridas
Seguir la estrategia de migración de aplicaciones.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Cambie los clientes de la aplicación a la nueva infraestructura.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cerrar los recursos temporales de AWS.		Administrador de sistemas
Revise y valide los documentos del proyecto.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas
Recopilar métricas sobre tiempo de migración, ahorros de costos conseguidos con las herramientas, etc.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas
Cerrar el proyecto y enviar comentarios.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Recursos relacionados

Referencias de Amazon RDS

- Amazon RDS para MariaDB
- Amazon Virtual Private Cloud VPCs y Amazon RDS
- Implementaciones Multi-AZ de Amazon RDS
- Precios de Amazon RDS

Referencias de MySQL y MariaDB

- mariadb-dump/mysqldump
- mysql Command-line Client

Tutoriales y videos

- Introducción a Amazon RDS

Migrar de una base de datos de MySQL en las instalaciones a Aurora MySQL

Creado por Vinod Kumar Sadu (AWS) e Igor Obradovic (AWS)

Entorno: producción	Origen: Base de datos MySQL en las instalaciones	Destino: edición de Amazon Aurora compatible con MySQL
Tipo R: redefinir la plataforma	Carga de trabajo: código abierto	Tecnologías: Migración; bases de datos
Servicios de AWS: AWS DMS		

Resumen

Este patrón explica cómo migrar una base de datos fuente MySQL local a Amazon Aurora MySQL Compatible Edition. Describe dos opciones de migración: usar AWS Database Migration Service (AWS DMS) o usar herramientas nativas de MySQL, como mysqldbcopy y mysqldump.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Base de datos de origen MySQL en un centro de datos en las instalaciones

Limitaciones

- Límite de tamaño de la base de datos: 64 TB

Versiones de producto

- MySQL versiones 5.7 y 8.0. Para obtener la lista más reciente de versiones compatibles, consulte las versiones de Amazon Aurora en la AWS documentación. Si está utilizandoAWS DMS, consulte también Uso de una base de datos compatible con MySQL como destino para las versiones de AWS DMS MySQL compatibles con. AWS DMS

Arquitectura

Pila de tecnología de origen

- Una base de datos MySQL en las instalaciones

Pila de tecnología de destino

- Amazon Aurora MySQL-Compatible Edition

Arquitectura de destino

Arquitectura de migración de datos

Uso de: AWS DMS

Uso de herramientas MySQL nativas:

Herramientas

- AWS Database Migration Service(AWS DMS) admite varias bases de datos de origen y destino. Para obtener información sobre las bases de datos de origen y destino de MySQL compatibles conAWS DMS, consulte Migración de bases de datos compatibles con MySQL a. AWS Le recomendamos que utilice la última versión de AWS DMS para obtener una compatibilidad más completa con las versiones y funciones.
- mysqldbcopy es una utilidad de MySQL que copia una base de datos MySQL en un único servidor o entre servidores.
- mysqldump es una utilidad de MySQL que crea un archivo de volcado a partir de una base de datos MySQL con fines de copia de seguridad o migración.

Epics

Planificar la migración

Tarea	Descripción	Habilidades requeridas
Validar la versión y el motor de la base de datos de origen y de destino.		Administrador de base de datos
Identifique los requisitos de hardware de la instancia del servidor de destino.		Administrador de base de datos, administrador de sistemas
Identifique los requisitos de almacenamiento (como el tipo y la capacidad de almacenamiento).		Administrador de base de datos, administrador de sistemas
Elegir el tipo de instancia correcto en función de la capacidad, las características de almacenamiento y las características de la red.		Administrador de base de datos, administrador de sistemas
Identificar los requisitos de seguridad del acceso a la red para las bases de datos de origen y destino.		Administrador de base de datos, administrador de sistemas
Identificar la estrategia de migración de aplicaciones.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Configure la infraestructura

Tarea	Descripción	Habilidades requeridas
Cree una nube privada virtual (VPC).		Administrador de sistemas
Creación de los grupos de seguridad.		Administrador de sistemas
Configure e inicie un clúster de base de datos compatible con Aurora MySQL.		Administrador de sistemas

Migrar datos: opción 1

Tarea	Descripción	Habilidades requeridas
Utilizar herramientas nativas de MySQL o herramientas de terceros para migrar los objetos y datos de la base de datos.	Para obtener instrucciones, consulte la documentación de las herramientas de MySQL, como mysqldbcopy y mysqldump.	Administrador de base de datos

Migrar datos: opción 2

Tarea	Descripción	Habilidades requeridas
Migre datos con. AWS DMS	Para obtener instrucciones, consulte Uso de una base de datos compatible con MySQL como fuente y Uso de una base de datos compatible con MySQL como destino en la documentación. AWS DMS	Administrador de base de datos

Migrar la aplicación

Tarea	Descripción	Habilidades requeridas
Seguir la estrategia de migración de aplicaciones.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Cambiar los clientes de la aplicación a la nueva infraestructura.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Cerrar el proyecto

Tarea	Descripción	Habilidades requeridas
Cerrar los recursos temporales de AWS.		Administrador de base de datos, administrador de sistemas
Revise y valide los documentos del proyecto.		Administrador de base de datos, propietario de la aplicación, administrador de sistemas
Recopilar métricas sobre el tiempo necesario para migrar, el porcentaje de migraciones manuales frente a las		Administrador de base de datos, propietario de la aplicación, administrador de sistemas

Tarea	Descripción	Habilidades requeridas
realizadas con herramientas, el ahorro de costos, etc.		
Cerrar el proyecto y enviar comentarios.		

Recursos relacionados

Referencias

- Migración de sus bases de datos a Amazon Aurora
- Sitio web de AWS DMS
- Documentación de AWS DMS
- Precios de Amazon Aurora
- Creación de un clúster de base de datos Aurora MySQL y conexión a él
- Amazon Virtual Private Cloud VPCs y Amazon RDS
- Documentación de Amazon Aurora

Tutoriales y videos

- Introducción a AWS DMS
- Introducción a Amazon Aurora

Migre bases de datos MySQL locales a Aurora MySQL mediante Percona, XtraBackup Amazon EFS y Amazon S3

Creado por Rohan Jamadagni (AWS), Sajith Menon (AWS) y Udayasimha Theepireddy (AWS)

Origen: en las instalaciones	Destino: Aurora MySQL	Tipo R: redefinir la plataforma
Entorno: producción	Tecnologías: bases de datos; migración	Carga de trabajo: código abierto
Servicios de AWS: Amazon S3; Amazon Aurora		

Resumen

Este patrón describe cómo migrar bases de datos MySQL locales de gran tamaño de manera eficiente a Amazon Aurora MySQL mediante XtraBackup Percona. Percona XtraBackup es una utilidad de copia de seguridad de código abierto y sin bloqueo para servidores basados en MySQL. El patrón muestra cómo utilizar Amazon Elastic File System (Amazon EFS) para reducir el tiempo de carga de la copia de seguridad en Amazon Simple Storage Service (Amazon S3) y restaurar la copia de seguridad en Amazon Aurora MySQL. El patrón también proporciona detalles sobre cómo realizar copias de seguridad incrementales de Percona para minimizar la cantidad de registros binarios que se aplicarán a la base de datos Aurora MySQL de destino.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Permisos para crear roles y políticas de AWS Identity and Access Management (IAM).
- Conectividad de red entre la base de datos MySQL en las instalaciones y la nube privada virtual (VPC) en AWS

Limitaciones

- Los servidores de origen deben ser sistemas basados en Linux que puedan instalar un cliente de Network File System (NFS) (nfs-utils/nfs-common).

- El bucket de S3 utilizado para cargar los archivos de copia de seguridad solo admite el cifrado del servidor (SSE-S3/SSE-KMS).
- Amazon S3 limita el tamaño de los archivos de copia de seguridad a 5 TB. Si el archivo de copia de seguridad supera los 5 TB, puede dividirlo en varios archivos más pequeños.
- El número de archivos de origen cargados en un bucket de S3 se limita a un millón de archivos.
- El patrón solo admite la copia de seguridad completa y la copia de seguridad incremental de Percona XtraBackup . No admite copias de seguridad parciales que utilicen `--tables`, `--tables-exclude`, `--tables-file`, `--databases`, `--databases-exclude` o `--databases-file`.
- Aurora no restaura los usuarios, las funciones, los procedimientos almacenados ni la información de zona horaria de la base de datos MySQL de origen.

Versiones de producto

- La base de datos de origen debe ser MySQL versión 5.5, 5.6 o 5.7.
- Para MySQL 5.7, debe usar Percona XtraBackup 2.4.
- Para MySQL 5.6 y 5.6, debe usar Percona XtraBackup 2.3 o 2.4.

Arquitectura

Pila de tecnología de origen

- Sistema operativo basado en Linux
- Servidor de MySQL
- Percona XtraBackup

Pila de tecnología de destino

- Amazon Aurora
- Amazon S3
- Amazon EFS

Arquitectura de destino

Herramientas

Servicios de AWS

- Amazon Aurora es un motor de base de datos relacional completamente administrado que simplifica y hace rentable configurar, usar y escalar las implementaciones de MySQL. Aurora MySQL es un sustituto directo de MySQL.
- Amazon Elastic File System (Amazon EFS) lo ayuda a crear y configurar sistemas de archivos compartidos en la nube de AWS.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Otras herramientas

- Percona XtraBackup es una utilidad de código abierto que realiza copias de seguridad en streaming, comprimidas e incrementales de bases de datos MySQL sin interrumpir ni bloquear sus bases de datos.

Epics

Crear un sistema de archivos de Amazon EFS

Tarea	Descripción	Habilidades requeridas
Cree un grupo de seguridad para asociarlo a los objetivos de montaje de Amazon EFS.	Cree un grupo de seguridad en la VPC que esté configura do con un adjunto de VPN a la base de datos en las instalaciones a través de AWS Transit Gateway. Para obtener más información sobre los comandos y los pasos descritos en este y otros artículos, consulte la sección «Recursos relaciona dos» al final de este patrón.	DevOpsAWS/administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
Edite las reglas del grupo de seguridad.	Agregue una regla de entrada utilizando el tipo NFS, el puerto 2049 y el rango de IP del servidor de base de datos en las instalaciones como fuente. De forma predeterminada, la regla de salida permite salir a todo el tráfico. Si no es así, añada una regla de salida para abrir una conexión para el puerto NFS. Añada otras dos reglas de entrada: el puerto 2049 (origen: el ID del grupo de seguridad del mismo grupo de seguridad) y el puerto 22 (fuente: intervalo de direcciones IP desde el que se conectará a una instancia EC2).	DevOpsAWS/administrador de bases de datos
Cree un sistema de archivos.	En los objetivos de montaje, use la VPC y el grupo de seguridad que creó en la historia anterior. Elija el modo de rendimiento y el rendimien to en función de los requisitos de E/S de la base de datos en las instalaciones. De manera opcional, habilite el cifrado en reposo.	DevOpsAWS/administrador de bases de datos

Monte el sistema de archivos.

Tarea	Descripción	Habilidades requeridas
Crear un rol de perfil de instancia de IAM para asociarlo a una instancia de EC2	Cree un rol de IAM que tenga permisos para cargar y acceder a objetos en Amazon S3. Elija el bucket de S3 donde se almacenará la copia de seguridad como recurso de políticas.	AWS DevOps
Cree una instancia de EC2	Inicie una instancia EC2 basada en Linux y adjunte el rol de perfil de instancia de IAM que creó en el paso anterior y el grupo de seguridad que creó anteriorm ente.	AWS DevOps
Instale el cliente NFS.	Instale el cliente NFS en el servidor de base de datos en las instalaciones y en la instancia EC2. Para obtener instrucciones, consulte la sección «Información adicional ».	DevOps
Monte el sistema de archivos de EFS.	Monte un sistema de archivos EFS en su instancia de Amazon EC2 en las instalaci ones. En cada servidor, cree un directorio para almacenar la copia de seguridad y monte el sistema de archivos mediante el punto de conexión de destino de montaje. Para obtener ejemplos, consulte la	DevOps

Tarea	Descripción	Habilidades requeridas
	sección «Información adicional ».	

Crear una copia de seguridad de la base de datos de origen MySQL

Tarea	Descripción	Habilidades requeridas
Instale Percona XtraBackup.	Instale Percona XtraBackup 2.3 o 2.4 (según la versión de la base de datos MySQL) en el servidor de bases de datos local. Para obtener los enlaces de instalación, consulte la sección «Recursos relaciona dos».	Administrador de base de datos
Cuente los esquemas y las tablas de la base de datos de origen.	Recopile y anote el número de esquemas y objetos de la base de datos MySQL de origen. Utilizará estos recuentos para validar la base de datos Aurora MySQL después de la migración.	Administrador de base de datos
(Opcional) Anote la secuencia de registro binario más reciente de la base de datos de origen.	Realice este paso si desea establecer la replicación de registros binarios entre la base de datos de origen y Aurora MySQL para minimizar el tiempo de inactividad. log-bin debe estar habilitado y server_id debe ser único. Anote la secuencia de registros binarios actual de la base de datos de origen, justo	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	antes de iniciar una copia de seguridad. Realice este paso justo antes de la copia de seguridad completa si planea usar solo una copia de seguridad completa. Si planea realizar copias de seguridad incrementales después de una copia de seguridad completa, lleve a cabo este paso justo antes de la última copia de seguridad incremental que restaurará en la instancia de base de datos Aurora MySQL.	
Inicie una copia de seguridad completa de la base de datos MySQL de origen.	Realice una copia de seguridad completa de la base de datos fuente de MySQL con Percona XtraBacku p. Para ver ejemplos de comandos para copias de seguridad completas e incrementales, consulte la sección «Información adicional ».	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
(Opcional) Realice copias de seguridad incrementales con XtraBackup Percona.	Las copias de seguridad incrementales se pueden utilizar para reducir la cantidad de registros binarios que debe aplicar para sincronizar la base de datos de origen con Aurora MySQL. Las bases de datos de gran tamaño y con muchas transacciones pueden generar una gran cantidad de registros binarios durante las copias de seguridad. Al realizar copias de seguridad incrementales y almacenar las en un sistema de archivos Amazon EFS compartido, puede reducir considera blemente el tiempo de copia de seguridad y carga de la base de datos. Para obtener más información, consulte la sección «Información adicional ». Siga realizando copias de seguridad incrementales hasta que esté listo para iniciar el proceso de migración a Aurora.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Prepare copias de seguridad.	En este paso, los registros transaccionales se aplican a la copia de seguridad para las transacciones que estaban en curso durante la copia de seguridad. Siga aplicando registros transaccionales (--apply-log-only) a cada copia de seguridad increment al para fusionar las copias de seguridad, excepto la última copia de seguridad. Para obtener más ejemplos, consulte la sección «Informac ión adicional». Tras este paso, la copia de seguridad completa y combinada estará en ~/<efs_mount_name>/ fullbackup.	Administrador de base de datos
Comprima y divida la copia de seguridad final combinada.	Después de preparar la copia de seguridad final combinada , utilice los comandos tar, zip y split para crear archivos comprimidos más pequeños de la copia de seguridad. Para obtener más ejemplos, consulte la sección «Informac ión adicional».	Administrador de base de datos

Restauración de la copia de seguridad en un clúster de base de datos de Aurora MySQL

Tarea	Descripción	Habilidades requeridas
Cargue la copia de seguridad en Amazon S3.	El sistema de archivos Amazon EFS en el que se almacenan los archivos de copia de seguridad está montado tanto en la base de datos en las instalaciones como en una instancia de EC2, de modo que los archivos de copia de seguridad estén fácilmente disponibles para la instancia de EC2. Conéctese a la instancia EC2 mediante Secure Shell (SSH) y cargue los archivos de copia de seguridad comprimidos en un bucket de S3 nuevo o existente; por ejemplo: aws s3 sync ~/<efs_mount_name>/fullbackup s3://<bucket_name>/fullbackup. Para obtener más información, consulte los enlaces de la sección «Recursos relacionados».	AWS DevOps
Crear un rol de servicio para que Aurora pueda acceder a Amazon S3	Cree un rol de IAM con la confianza «rds.amazonaws.com» y una política que permita a Aurora acceder al bucket de S3 donde se almacenan los archivos de copia de seguridad. Los	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	permisos necesarios son ListBucket GetObject, y GetObjectVersion.	
Cree la configuración de red para Aurora.	Cree un grupo de subredes de base de datos de clúster con al menos dos zonas de disponibilidad y una configuración de tabla de enrutamiento de subred que permita la conectividad saliente a la base de datos de origen. Cree un grupo de seguridad que permita las conexiones salientes a la base de datos en las instalaciones y permita a los administradores conectarse al clúster de base de datos Aurora. Para obtener más información, consulte los enlaces de la sección «Recursos relacionados».	DevOpsAWS/administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
Restauración de la copia de seguridad en un clúster de base de datos de Aurora MySQL.	Restaure sus datos desde la copia de seguridad que cargó en Amazon S3. Especifique la versión MySQL de la base de datos de origen, proporcione el nombre del bucket de S3 y el prefijo de la ruta de la carpeta donde cargó el archivo de copia de seguridad (por ejemplo, «fullbackup» para los ejemplos de la sección «Información adicional») y proporcione el rol de IAM que creó para autorizar a Aurora a acceder a Amazon S3.	DevOpsAWS/administrador de bases de datos
Valide la base de datos de Aurora MySQL.	Valide el recuento de esquemas y objetos del clúster de base de datos Aurora restaurado con respecto al recuento obtenido de la base de datos de origen.	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Configure la replicación de binlog.	Utilice la secuencia de registro binario que indicó anteriorm ente antes de realizar la última copia de seguridad que se restauró en el clúster de base de datos Aurora. Cree un usuario de replicaci ón en la base de datos de origen y siga las instrucciones de la sección «Información adicional» para proporcio nar los privilegios adecuados , habilitar la replicación en Aurora y confirmar que la replicación está sincronizada.	DevOpsAWS/administrador de bases de datos

Recursos relacionados

Creación de un sistema de archivos de Amazon EFS

- Creación de un grupo de seguridad (documentación de Amazon VPC)
- Adjuntos de VPN de puerta de enlace de tránsito (documentación de Amazon VPC)
- Escalar el rendimiento de la VPN con AWS Transit Gateway (blog sobre redes y entrega de contenido)
- Creación de un sistema de archivos de Amazon EFS (documentación de Amazon EFS)
- Creación de objetivos de montaje (documentación de Amazon EFS)
- Cifrado de datos en reposo (documentación de Amazon EFS)

Montaje de sistemas de archivos

- Roles de IAM para Amazon EC2 (documentación de Amazon EC2)
- Lanzamiento de una instancia Linux de Amazon EC2 (documentación de Amazon EC2)
- Instalación del cliente NFS (documentación de Amazon EFS)

- Montaje del sistema de archivos Amazon EFS en el cliente en las instalaciones (documentación de Amazon EFS)
- Montaje de sistemas de archivos EFS (documentación de Amazon EFS)

Creación de un copia de seguridad completa de la base de datos MySQL de origen

- Instalación de Percona XtraBackup 2.3 (documentación de XtraBackup Percona)
- Instalación de Percona XtraBackup 2.4 (documentación de Percona) XtraBackup
- Establecer la configuración maestra de replicación (documentación de MySQL)
- Migración de datos desde una base de datos MySQL externa a un clúster de base de datos de Amazon Aurora MySQL (documentación de Aurora)
- Respaldo incremental (documentación de Percona XtraBackup)

Restauración de la copia de seguridad en Amazon Aurora MySQL

- Creación de un bucket (documentación de Amazon S3)
- Conexión a la instancia de Linux mediante SSH (documentación de Amazon EC2)
- Configuración de la CLI de AWS (documentación de la CLI de AWS)
- comando sync (referencia de comandos de la CLI de AWS)
- Creación de una política de IAM para acceder a los recursos de Amazon S3 (documentación de Aurora
- Requisitos previos del clúster de base de datos (documentación de Aurora)
- Uso de los grupos de subredes de base de datos (documentación de Aurora)
- Creación de un grupo de seguridad de VPC para una instancia de base de datos privada (documentación de Aurora)
- Restauración de un clúster de base de datos de Aurora MySQL desde un bucket de S3 (documentación de Aurora)
- Configuración de la replicación con MySQL o con otro clúster de base de datos de Aurora (documentación de Aurora)
- Procedimiento mysql.rds_set_external_master (referencia de SQL para MySQL en Amazon RDS)
- Procedimiento mysql.rds_start_replication (referencia de SQL sobre MySQL en Amazon RDS)

Referencias adicionales

- Migración de datos desde una base de datos MySQL externa a un clúster de base de datos de Amazon Aurora MySQL (documentación de Aurora)
- Descargas del servidor MySQL (sitio web de Oracle)

Tutoriales y videos

- Migración de datos de MySQL a un clúster de base de datos Aurora MySQL mediante Amazon S3 (Centro de conocimientos de AWS)
- Configuración y montaje de Amazon EFS (vídeo)

Información adicional

Instalación de un cliente NFS

- Si utiliza Red Hat o un sistema operativo Linux similar, utilice el comando:

```
$ sudo yum -y install nfs-utils
```

- Si utiliza Ubuntu o un sistema operativo Linux similar, utilice el comando:

```
$ sudo apt-get -y install nfs-common
```

Para obtener más información, consulte el tutorial en la documentación de Amazon EFS.

Montaje de un sistema de archivos de Amazon EFS

Utilice el comando:

```
mkdir ~/<efs_mount_name>
$ sudo mount -t nfs -o
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport mount-
target-IP:/ ~/<efs_mount_name>
```

Para obtener más información, consulte el tutorial y Montaje de un sistema de archivos en la documentación de Amazon EFS.

Hacer copias de seguridad de la base de datos fuente MySQL

Copias de seguridad completas

Use un comando como el siguiente, que toma la copia de seguridad, la comprime y la divide en fragmentos más pequeños de 1 GB cada uno:

```
xtrabackup --backup --user=dbuser --password=<password> --binlog-info=AUTO --stream=tar
 --target-dir=~/<efs_mount_name>/fullbackup | gzip - | split -d --bytes=1024MB - ~/
<efs_mount_name>/fullbackup/backup.tar.gz &
```

Si planea realizar copias de seguridad incrementales posteriores después de la copia de seguridad completa, no comprima ni divida la copia de seguridad. En su lugar, use un comando similar al siguiente:

```
xtrabackup --backup --user=dbuser --password=<password> --target-dir=~/
<efs_mount_name>/fullbackup/
```

Copias de seguridad incrementales

Utilice la ruta de copia de seguridad completa para el parámetro `--incremental-basedir`; por ejemplo:

```
xtrabackup --backup --user=dbuser --password=<password> --target-dir=~/
<efs_mount_name>/incremental/backupdate --incremental-basedir=~/<efs_mount_name>/
fullbackup
```

donde basedir es la ruta a la copia de seguridad completa y al archivo xtrabackup_checkpoints.

Para obtener más información sobre la creación de copias de seguridad, consulte Migración de datos desde una base de datos MySQL externa a un clúster de base de datos de MySQL de Amazon Aurora en la documentación de Aurora.

Preparar copias de seguridad

Para preparar una copia de seguridad completa:

```
xtrabackup --prepare --apply-log-only --target-dir=~/<efs_mount_name>/fullbackup
```

Para preparar una copia de seguridad incremental:

```
xtrabackup --prepare --apply-log-only --target-dir=~/<efs_mount_name>/fullbackup --
incremental-dir=~/<efs_mount_name>/incremental/06062020
```

Para preparar la copia de seguridad final:

```
xtrabackup --prepare --target-dir=~/<efs_mount_name>/fullbackup --incremental-dir=~/
<efs_mount_name>/incremental/06072020
```

Para obtener más información, consulte las copias de seguridad incrementales en la documentación de Percona XtraBackup .

Comprimir y dividir la copia de seguridad combinada

Para comprimir la copia de seguridad combinada en ~/<efs_mount_name>/fullbackup:

```
tar -zcvf <backupfilename.tar.gz> ~/<efs_mount_name>/fullbackup
```

Para dividir la copia de seguridad:

```
split -d -b1024M --verbose  <backupfilename.tar.gz> <backupfilename.tar.gz>
```

Configure la replicación de binlog

Para crear un usuario de replicación en la base de datos de origen y proporcionar los privilegios adecuados:

```
CREATE USER 'repl_user'@'' IDENTIFIED BY ''; GRANT REPLICATION CLIENT, REPLICATION
 SLAVE ON *.* TO 'repl_user'@'';
```

Para habilitar la replicación en Aurora mediante la conexión al clúster de base de datos Aurora, habilite los registros binarios en el grupo de parámetros del clúster de base de datos. Configure `binlog_format = mixed` (se prefiere el modo mixto). Este cambio requiere que reinicies la instancia para aplicar la actualización.

```
CALL mysql.rds_set_external_master ('sourcedbinstanceIP', sourcedbport, 'repl_user',
 '', 'binlog_file_name', binlog_file_position, 0); CALL mysql.rds_start_replication;
```

Para confirmar que la replicación está sincronizada:

```
SHOW Slave Status \G;
```

El campo Segundos detrás del maestro muestra qué tan lejos está Aurora de la base de datos en las instalaciones.

Migración de aplicaciones Java locales en las instalaciones a AWS mediante AWS App2Container

Origen: aplicaciones	Destino: aplicación conteneri zada implementada en Amazon ECS	Tipo R: redefinir la plataforma
Entorno: PoC o piloto	Tecnologías: migración; aplicaciones web y móviles	Carga de trabajo: código abierto
Servicios de AWS: Amazon EC2 Container Registry; Amazon ECS		

Resumen

AWS App2Container (A2C) es una herramienta de línea de comandos que le ayuda a transformar en contenedores las aplicaciones existentes que se ejecutan en máquinas virtuales sin necesidad de cambiar el código. A2C descubre aplicaciones en ejecución en un servidor, identifica las dependencias y genera artefactos relevantes para una implementación sin interrupciones en Amazon Elastic Container Service (Amazon ECS) y Amazon Elastic Kubernetes Service (Amazon EKS).

Este patrón proporciona los pasos para migrar de forma remota las aplicaciones Java en las instalaciones implementadas en un servidor de aplicaciones a AWS Fargate o Amazon EKS mediante App2Container a través de la máquina de trabajo.

La máquina de trabajo se puede utilizar en los siguientes casos de uso:

- La instalación de Docker no está permitida o no está disponible en los servidores de aplicaciones donde se ejecutan las aplicaciones Java.
- Debe gestionar la migración de varias aplicaciones implementadas en distintos servidores físicos o virtuales.

Requisitos previos y limitaciones

Requisitos previos

- Un servidor de aplicaciones con una aplicación Java que se ejecuta en un servidor Linux
- Una máquina de trabajo con un sistema operativo Linux
- Una máquina de trabajo con al menos 20 GB de espacio disponible en disco

Limitaciones

- No todas las aplicaciones son compatibles. Para más información, consulte Aplicaciones compatibles para Linux.

Arquitectura

Pila de tecnología de origen

- Aplicaciones Java que se ejecutan en un servidor Linux

Pila de tecnología de destino

- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- AWS CodePipeline
- Amazon Elastic Container Registry
- AWS Fargate

Arquitectura de destino

Herramientas

Herramientas

- AWS App2Container (A2C) es una herramienta de la línea de comandos que le ayuda a migrar mediante lift-and-shift las aplicaciones que se ejecutan en centros de datos en las instalaciones o en máquinas virtuales, de modo que se ejecuten en contenedores administrados por Amazon ECS o Amazon EKS.

- AWS CodeBuild: AWS CodeBuild es un servicio de compilación en la nube totalmente gestionado. CodeBuild compila su código fuente, ejecuta pruebas unitarias y produce artefactos listos para su implementación.
- AWS CodeCommit: AWS CodeCommit es un servicio de control de versiones alojado por Amazon Web Services que puede utilizar para almacenar y gestionar activos (como documentos, código fuente y archivos binarios) en la nube de forma privada.
- AWS CodePipeline: AWS CodePipeline es un servicio de entrega continua que puede utilizar para modelar, visualizar y automatizar los pasos necesarios para lanzar su software.
- Amazon ECS: Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores altamente escalable y rápido que facilita la tarea de ejecutar, detener y administrar contenedores en un clúster.
- Amazon ECR: Amazon Elastic Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado por AWS que es seguro, escalable y fiable.
- Amazon EKS: Amazon Elastic Kubernetes Service (Amazon EKS) es un servicio administrado que puede utilizar para ejecutar Kubernetes en AWS sin necesidad de instalar, operar ni mantener su propio plano de control o nodos de Kubernetes.
- AWS Fargate se puede utilizar en Amazon ECS para ejecutar contenedores sin tener que administrar servidores ni clústeres de instancias de Amazon Elastic Compute Cloud (Amazon EC2). Con Fargate, ya no tendrá que aprovisionar, configurar ni escalar clústeres de máquinas virtuales para ejecutar los contenedores.

Epics

Configuración de credenciales

Tarea	Descripción	Habilidades requeridas
Cree un secreto para acceder al servidor de aplicaciones.	Para acceder al servidor de aplicaciones de forma remota desde la máquina de trabajo, cree un secreto en AWS Secrets Manager. Como secreto, puede utilizar la clave privada de SSH o el certifica do y la clave privada de SSH.	DevOps, desarrollador

Tarea	Descripción	Habilidades requeridas
	Para obtener más información, consulte Administrar secretos para AWS App2Container.	

Configure la máquina de trabajo

Tarea	Descripción	Habilidades requeridas
Instalar el archivo tar.	Ejecute `sudo yum install -y tar`.	DevOps, Desarrollador
Instale la AWS CLI.	Para instalar la interfaz de la línea de comandos (CLI de AWS), ejecute `curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip" .` Descomprima `awscliv2.zip .` Ejecute `sudo ./aws/install .`	DevOps, Desarrollador
Instale App2Container.	Ejecute los comandos siguientes: `curl -o AWSApp2Container-installer-linux.tar.gz https://app2container-release-us-east-1.s3.us-east-1.amazonaws.com/lates`	DevOps, Desarrollador

Tarea	Descripción	Habilidades requeridas
	`t/linux/AWSApp2Container-installer-linux.tar.gz` `sudo tar xvf AWSApp2Container-installer-linux.tar.gz` `sudo ./install.sh`	
Configure los perfiles.	Para configurar el perfil predeterminado de AWS, ejecute `sudo aws configure` . Para configurar el perfil predeterminado de AWS con nombre, ejecute `sudo aws configure --profile <profile name>`.	DevOps, Desarrollador
Instalar Docker.	Ejecute los siguientes comandos. `sudo yum install -y docker` `sudo systemctl enable docker & sudo systemctl restart docker`	

Tarea	Descripción	Habilidades requeridas
Inicie App2Container.	Para inicializar App2Container, necesita la siguiente información: • `workspace` : para almacenar los artefactos de contenerización de aplicaciones. Recomendamos aportar una ruta de directorio que tenga al menos 20 GB de espacio libre en disco. • `awsProfile` : perfil de AWS configurado en el servidor. Esto es necesario para cargar artefactos en Amazon S3, ejecutar el comando `containerize` y generar artefactos de AWS para su implementación en Amazon ECS o Amazon EKS. • `s3Bucket`: para extraer y almacenar artefactos de AWS. • `metricsReportPermission` : para recopilar y almacenar las métricas reportadas. • `dockerContentTrust` : para firmar la imagen de Docker.	DevOps, Desarrollador

Tarea	Descripción	Habilidades requeridas
	Ejecute `sudo app2container init .`	

Configure la máquina de trabajo

Tarea	Descripción	Habilidades requeridas
Configure la máquina de trabajo para conectarse remotamente y ejecutar los comandos de App2Container en el servidor de aplicaciones.	Para configurar la máquina de trabajo, se requiere la siguiente información: • `Server FQDN`: el nombre completo del dominio del servidor de aplicaciones. • `Server IP address`: la dirección IP del servidor de aplicaciones. El FQDN o la dirección IP son suficientes. • `SecretARN` : el nombre de recurso de Amazon (ARN) del secreto que se utiliza para conectarse al servidor de aplicaciones y que se almacena en Secrets Manager. • `AuthMethod` : el método de autenticación `key` o `cert`. Ejecute `sudo app2container remote configure .`	DevOps, Desarrollador

Descubra, analice y extraiga aplicaciones en la máquina de trabajo

Tarea	Descripción	Habilidades requeridas
Descubra las aplicaciones Java en las instalaciones.	Para descubrir de forma remota todas las aplicaciones en ejecución en el servidor de aplicaciones, ejecute el siguiente comando. `sudo app2container remote inventory --target <FQDN/IP of App server>` Este comando genera una lista de las aplicaciones implementadas en `inventory.json` .	Desarrollador, DevOps
Analice las aplicaciones descubiertas.	Para analizar de forma remota cada aplicación mediante el identificador de aplicación obtenido en la fase de inventario, ejecute el siguiente comando. `sudo app2container remote analyze --application-id <java-app-id> --target <FQDN/IP of App Server>` Esto genera un archivo `analysis.json` en la ubicación del espacio de trabajo. Una vez generado	Desarrollador, DevOps

Tarea	Descripción	Habilidades requeridas
	este archivo, puede modificar los parámetros de conteneri zación en función de sus necesidades.	
Extraiga las aplicaciones analizadas.	Para generar un archivo de aplicaciones para la aplicació n analizada, ejecute de forma remota el siguiente comando, que generará el paquete tar en la ubicación del espacio de trabajo. `sudo app2container remote extract --application-id <application id> --target <FQDN/IP of App Server>` Los artefactos extraídos se pueden generar en la máquina de trabajo local.	Desarrollador, DevOps

Guarde en contenedores los artefactos extraídos en la máquina de trabajo

Tarea	Descripción	Habilidades requeridas
Coloque en contenedores los artefactos extraídos.	Guarde en contenedores los artefactos extraídos en el paso anterior ejecutando el siguiente comando. `sudo app2container containerize --input-`	Desarrollador, DevOps

Tarea	Descripción	Habilidades requeridas
	`archive <tar bundle location on worker machine>`	
Finalice el objetivo.	Para finalizar el objetivo, abra `deployment.json` , que se crea cuando se ejecuta el comando `containerize` . Para especificar AWS Fargate como objetivo, establezca `createEcsArtifacts` en `true`. Para establecer Amazon EKS como objetivo, establezca `createEksArtifacts` en true.	Desarrollador, DevOps

Genere y aprovisione artefactos de AWS

Tarea	Descripción	Habilidades requeridas
Genere artefactos de implementación de AWS en la máquina de trabajo.	Para generar artefactos de implementación, ejecute el siguiente comando. `sudo app2container generate app-deployment --application-id <application id>` Esto genera la CloudFormation plantilla de `ecs-master.yml` AWS en el espacio de trabajo.	DevOps

Tarea	Descripción	Habilidades requeridas
Aprovisione los artefactos.	Para aprovisionar aún más los artefactos generados, implemente la CloudFormation plantilla de AWS ejecutando el siguiente comando. `aws cloudformation deploy --template-file <path to ecs-master.yml> --capabilities CAPABILITY_NAMED_IAM --stack-name <application id>-ECS`	DevOps
Genere la canalización.	Modifique `pipeline.json` , que se creó en la historia anterior, en función de sus necesidades. A continuación, ejecute el comando `generate pipeline` para generar los artefactos de implementación de la canalización.	DevOps

Recursos relacionados

- ¿Qué es App2Container?
- Entrada de blog sobre AWS App2Container
- Conceptos básicos de configuración de la CLI de AWS
- Conceptos básicos de Docker para Amazon ECS
- Comandos de Docker

Migración de sistemas de archivos compartidos en una gran migración de AWS

Creado por Amit Rudraraju (AWS), Sam Apa (AWS), Bheemeswararao Balla (AWS), Wally Lu (AWS) y Sanjeev Prakasam (AWS)

Entorno: producción	Origen: sistema de archivos compartidos en las instalaciones	Destino: Amazon EFS o Amazon FSx
Tipo R: redefinir la plataforma	Carga de trabajo: todas las demás cargas de trabajo	Tecnologías: migración; almacenamiento y copia de seguridad
Servicios de AWS: AWS DataSync; Amazon EFS; Amazon FSx para Windows File Server; Amazon FSx para ONTAP NetApp		

Resumen

La migración de 300 o más servidores se considera una migración grande. El objetivo de una migración grande es migrar las cargas de trabajo de sus centros de datos en las instalaciones existentes a la nube de AWS, y estos proyectos suelen centrarse en las cargas de trabajo de aplicaciones y bases de datos. Sin embargo, los sistemas de archivos compartidos requieren una atención específica y un plan de migración independiente. Este patrón describe el proceso de migración de los sistemas de archivos compartidos y proporciona las prácticas recomendadas para migrarlos correctamente como parte de un gran proyecto de migración.

Un sistema de archivos compartidos (SFS), también conocido como sistema de archivos de red o agrupado, es un recurso compartido de archivos que se monta en varios servidores. Se accede a los sistemas de archivos compartidos mediante protocolos como el Sistema de archivos de red (NFS), el Sistema de archivos común de Internet (CIFS) o el Bloque de mensajes del servidor (SMB).

Estos sistemas no se migran con herramientas de migración estándar, como AWS Application Migration Service, porque no están dedicados al host que se está migrando ni se representan como

un dispositivo de bloques. Si bien la mayoría de las dependencias del host se migran de forma transparente, la coordinación y la administración de los sistemas de archivos dependientes deben gestionarse por separado.

Los sistemas de archivos compartidos se migran en las siguientes fases: descubrir, planificar, preparar, recortar y validar. Con este patrón y los libros de trabajo adjuntos, migra el sistema de archivos compartidos a un servicio de almacenamiento de AWS, como Amazon Elastic File System (Amazon EFS), Amazon FSx NetApp para ONTAP o Amazon FSx for Windows File Server. Para transferir el sistema de archivos, puede utilizar AWS DataSync o una herramienta de terceros, como NetApp SnapMirror.

Nota: Este patrón forma parte de una serie de Recomendaciones de AWS sobre grandes migraciones a la nube de AWS. Este patrón incluye las prácticas recomendadas e instrucci ones para incorporar los SFS en sus planes de onda para servidores. Si va a migrar uno o más sistemas de archivos compartidos fuera de un gran proyecto de migración, consulte las instrucci ones de transferencia de datos en la documentación de AWS para Amazon EFS, Amazon FSx for Windows File Server y Amazon FSx para ONTAP. NetApp

Requisitos previos y limitaciones

Requisitos previos

Los requisitos previos pueden variar en función de los sistemas de archivos compartidos de origen y destino y del caso de uso. Los problemas más coqmunes son los siguientes:

- Una cuenta de AWS activa.
- Ha completado la búsqueda de la cartera de aplicaciones para su gran proyecto de migración y ha empezado a desarrollar planes de onda. Para obtener más información, consulte Manual de estrategias de portafolio para grandes migraciones de AWS.
- Nubes privadas virtuales (VPC) y grupos de seguridad que permiten el tráfico de entrada y salida entre el centro de datos en las instalaciones y su entorno de AWS. Para obtener más información, consulte las opciones de conectividad de red a Amazon VPC y los requisitos de red de AWS. DataSync
- Permisos para crear CloudFormation pilas de AWS o permisos para crear recursos de Amazon EFS o Amazon FSx. Para obtener más información, consulte la CloudFormation documentación, la documentación de Amazon EFS o la documentación de Amazon FSx.

- Si utiliza AWS DataSync para realizar la migración, necesitará los siguientes permisos:
  - Permisos para DataSync que AWS envíe registros a un grupo de CloudWatch registros de AWS Logs. Para obtener más información, consulte DataSync Permitir cargar registros a grupos de CloudWatch registros.
  - Permisos para acceder al grupo de CloudWatch registros. Para obtener más información, consulte Descripción general de la administración de los permisos de acceso a los recursos de CloudWatch Logs.
  - Permisos para crear agentes y tareas en DataSync. Para obtener más información, consulte Permisos de IAM necesarios para usar AWS DataSync.

Limitaciones

- Este patrón está diseñado para migrar los archivos SFS como parte de un gran proyecto de migración. Incluye las prácticas recomendadas e instrucciones para incorporar los SFS en sus planes de migración de aplicaciones. Si va a migrar uno o más sistemas de archivos compartidos fuera de un gran proyecto de migración, consulte las instrucciones de transferencia de datos en la documentación de AWS para Amazon EFS, Amazon FSx for Windows File Server y Amazon FSx para ONTAP. NetApp
- Este patrón se basa en las arquitecturas, los servicios y los patrones de migración más utilizados. Sin embargo, los grandes proyectos y estrategias de migración pueden variar de una organización a otra. Es posible que necesite personalizar esta solución o los libros de trabajo proporcionados en función de sus necesidades.

Arquitectura

Pila de tecnología de origen

Una o varias de las siguientes:

- Servidor de archivos Linux (NFS)
- Servidor de archivos Windows (SMB)
- NetApp arreglo de almacenamiento
- Cabina de almacenamiento Dell EMC Isilon

Pila de tecnología de destino

Una o varias de las siguientes:

- Amazon Elastic File System
- Amazon FSx para ONTAP NetApp
- Amazon FSx para Windows File Server

Arquitectura de destino

El diagrama muestra el proceso siguiente:

1. Establece una conexión entre el centro de datos en las instalaciones y la nube de AWS mediante un servicio de AWS, como AWS Direct Connect o AWS Site-to-Site VPN.
2. El DataSync agente se instala en el centro de datos local.
3. Según su plan de oleada, solía DataSync replicar los datos del sistema de archivos compartidos de origen al recurso compartido de archivos de AWS de destino.

Fases de migración

La siguiente imagen muestra las fases y los pasos de alto nivel para migrar un SFS en un proyecto de migración de gran tamaño.

La sección Epics de este patrón contiene instrucciones detalladas sobre cómo completar la migración y utilizar los libros de trabajo adjuntos. A continuación, se brinda información general de alto nivel de los pasos de este enfoque por etapas.

Fase	Pasos
Descubra	1. Con una herramienta de detección, se recopilan datos sobre el sistema de archivos compartido, incluidos los servidores, los puntos de montaje y las direcciones IP. 2. Mediante una base de datos de gestión de la configuración (CMDB) o una herramienta

	de migración, se recopilan detalles sobre el servidor, incluida información sobre la onda de migraciones, el entorno, el propietario de la aplicación, el nombre del servicio de gestión de servicios de TI (ITSM), la unidad organizativa y el identificador de la aplicación.
Planifique	3. Con la información recopilada sobre los SFS y los servidores, cree el plan de onda del SFS. 4. Con la información de la hoja de trabajo de creación, para cada SFS, elija un servicio de AWS de destino y una herramienta de migración.
Preparación	5. Configure la infraestructura de destino en Amazon EFS, Amazon FSx para NetApp ONTAP o Amazon FSx for Windows File Server. 6. Configure el servicio de transferencia de datos, por ejemplo, y DataSync, a continuac ión, inicie la sincronización de datos inicial. Cuando se complete la sincronización inicial, puede configurar las sincronizaciones recurrent es para que se ejecuten según una programac ión, 7. Actualice el plan de ondas del SFS con información sobre el recurso compartido de archivos de destino, como la dirección IP o la ruta.

Realizar la transición	8. Detenga las aplicaciones que acceden activamente al SFS de origen. 9. En el servicio de transferencia de datos, realice una sincronización de datos final. 10. Cuando se complete la sincronización, compruebe que se ha realizado correctamente revisando los datos de registro en CloudWatch Registros.
Valide	11. En los servidores, cambie el punto de montaje por la nueva ruta SFS. 12. Reinicie y valide las aplicaciones.

Herramientas

Servicios de AWS

- Amazon CloudWatch Logs le ayuda a centralizar los registros de todos sus sistemas, aplicaciones y servicios de AWS para que pueda supervisarlos y archivarlos de forma segura.
- AWS DataSync es un servicio de transferencia y descubrimiento de datos en línea que le ayuda a mover archivos o datos de objetos hacia, desde y entre los servicios de almacenamiento de AWS.
- Amazon Elastic File System (Amazon EFS) le ayuda a crear y configurar sistemas de archivos compartidos en la nube de AWS.
- Amazon FSx proporciona sistemas de archivos que admiten los protocolos de conectividad estándares del sector y ofrecen alta disponibilidad y replicación en todas las regiones de AWS.

Otras herramientas

- SnapMirrores una herramienta de replicación de NetApp datos que replica datos de volúmenes de origen específicos o qtrees a volúmenes o qtrees de destino, respectivamente. Puede utilizar esta herramienta para migrar un sistema de archivos NetApp fuente a Amazon FSx para ONTAP.
- Robocopy, abreviatura de Robust File Copy, es un directorio de línea de comandos y comandos para Windows. Puede utilizar esta herramienta para migrar un sistema de archivos fuente de Windows a Amazon FSx para Windows File Server.

Prácticas recomendadas

Enfoques de planificación de olas

Al planificar las ondas para su gran proyecto de migración, tenga en cuenta la latencia y el rendimiento de las aplicaciones. Cuando el SFS y las aplicaciones dependientes funcionan en ubicaciones diferentes, como una en la nube y otra en el centro de datos en las instalaciones, esto puede aumentar la latencia y afectar al rendimiento de las aplicaciones. A continuación, se muestran las siguientes opciones al crear planes de onda:

1. Migre el SFS y todos los servidores dependientes en la misma oleada: este enfoque evita problemas de rendimiento y minimiza las tareas de retrabajo, como la reconfiguración de los puntos de montaje varias veces. Se recomienda cuando se requiere una latencia muy baja entre la aplicación y el SFS. Sin embargo, la planificación de ondas es compleja y, por lo general, el objetivo es eliminar las variables de las agrupaciones de dependencias, no añadirlas. Además, este enfoque no se recomienda si muchos servidores acceden al mismo SFS, ya que esto hace que la onda sea demasiado grande.
2. Migre el SFS una vez que se haya migrado el último servidor dependiente: por ejemplo, si varios servidores acceden a un SFS y dichos servidores tienen previsto migrar en las oleadas 4, 6 y 7, programe la migración del SFS en la oleada 7.

   Este enfoque suele ser el más lógico para migraciones grandes y se recomienda para aplicaciones sensibles a la latencia. Reduce los costos asociados a la transferencia de datos. También minimiza el período de latencia entre el SFS y las aplicaciones de nivel superior (como las de producción), ya que las aplicaciones de nivel superior suelen estar programadas para migrar en último lugar, después de las aplicaciones de desarrollo y control de calidad.

   Sin embargo, este enfoque aún requiere detección, planificación y agilidad. Es posible que tenga que migrar el SFS en una onda anterior. Confirme que las aplicaciones puedan soportar la latencia adicional durante el período de tiempo entre la primera onda dependiente y la onda que contiene el SFS. Realice una sesión de descubrimiento con los propietarios de las aplicaciones y migre la aplicación en la misma fase, es decir, la aplicación más sensible a la latencia. Si se descubren problemas de rendimiento después de migrar una aplicación dependiente, prepárese para migrar rápidamente el SFS lo más rápido posible.
3. Migre el SFS al final de un gran proyecto de migración: este enfoque se recomienda si la latencia no es un factor, por ejemplo, cuando se accede con poca frecuencia a los datos del SFS o no son críticos para el rendimiento de la aplicación. Este enfoque agiliza la migración y simplifica las tareas de transición.

Puede combinar estos enfoques en función de la sensibilidad a la latencia de la aplicación. Por ejemplo, puede migrar los SFS sensibles a la latencia utilizando los enfoques 1 o 2 y, a continuación, migrar el resto de los SFS utilizando el enfoque 3.

Elegir un servicio de sistema de archivos de AWS

AWS ofrece varios servicios en la nube para el almacenamiento de archivos. Cada uno ofrece diferentes ventajas y limitaciones en cuanto al rendimiento, la escala, la accesibilidad, la integración, la conformidad y la optimización de costos. Hay algunas opciones lógicas predeterminadas. Por ejemplo, si su sistema de archivos en las instalaciones actual utiliza Windows Server, Amazon FSx para Windows File Server es la opción predeterminada. O bien, si el sistema de archivos local utiliza NetApp ONTAP, Amazon FSx for NetApp ONTAP es la opción predeterminada. Sin embargo, puede elegir un servicio específico en función de los requisitos de su aplicación o para aprovechar otras ventajas operativas en la nube. Para obtener más información, consulte Elegir el servicio de almacenamiento de archivos de AWS adecuado para su implementación (presentación en la Cumbre de AWS).

Elección de una herramienta de migración

Amazon EFS y Amazon FSx admiten el uso de AWS DataSync para migrar sistemas de archivos compartidos a la nube de AWS. Para obtener más información sobre los sistemas y servicios de almacenamiento compatibles, las ventajas y los casos de uso, consulte Qué es AWS DataSync. Para obtener información general sobre el proceso de transferencia de archivos, consulte Cómo funcionan las DataSync transferencias de AWS. DataSync

También hay varias herramientas de terceros disponibles, entre las que se incluyen las siguientes:

- Si elige Amazon FSx para NetApp ONTAP, puede usarlo para NetApp SnapMirror migrar los archivos del centro de datos local a la nube. SnapMirror utiliza la replicación a nivel de bloques, que puede ser más rápida DataSync y reducir la duración del proceso de transferencia de datos. Para obtener más información, consulte Migración a FSx para usar ONTAP. NetApp SnapMirror
- Si elige Amazon FSx para Windows File Server, puede utilizar Robocopy para migrar archivos a la nube. Para obtener más información, consulte Migración de archivos existentes a FSx for Windows File Server mediante Robocopy.

Epics

Descubra

Tarea	Descripción	Habilidades requeridas
Prepare el libro de trabajo de descubrimiento del SFS.	1. Descargue los libros de trabajo de la sección Adjuntos de este patrón. Contiene dos archivos, SFS-Discovery-Workbook.xlsx y SFS-Wave-Plan-Workbook.xlsx. 2. Abra el archivo SFS-Discovery-Workbook en Microsoft Excel. 3. En la hoja de trabajo del Panel, haga lo siguiente: • En la columna A, actualice el nombre del entorno. • En la columna B, actualice el orden de los entornos para colocarlos en orden desde la prioridad más baja (1) hasta la prioridad más alta. • En las columnas D a E, actualice el horario de oleaje. • En las columnas C y K, actualice los nombres de las cuentas de AWS.	Ingeniero de migraciones, líder de migración

Tarea	Descripción	Habilidades requeridas
	• En la columna L, actualice los identific adores de VPC. • En las columnas M a O, actualice los identific adores de subred. 4. Revise el resto de la plantilla del libro de trabajo y actualice cualquier otro valor necesario para su organización o caso de uso. 5. Guarde el cuaderno de trabajo.	

Tarea	Descripción	Habilidades requeridas
Recopile información sobre el SFS de origen.	1. Con la herramienta de detección que prefiera, identifique todos los montajes del SFS en todos los dispositivos de almacenamiento, servidores Linux y servidores Windows aplicables. En términos generales, necesitará recopilar la siguiente información: • Dispositivos cliente • Direcciones IP de clientes • Detalles de SFS • Punto de montaje Nota: Puede añadir los detalles del punto de montaje al manual de procedimientos de migración para volver a montar el SFS después de la migración. 2. Abra el archivo SFS-Discovery-Workbook. 3. En la hoja de trabajo Wave-Sheet, haga lo siguiente: • En la columna Ubicación del servidor (D), en la fórmula, confirme que el formato del rango CIDR de la fuente en las instalaci	Ingeniero de migraciones, líder de migración

Tarea	Descripción	Habilidades requeridas
	ones funciona para su rango. Por ejemplo, si su rango de CIDR es `10.0.0.0/8` , introduzca `10.*.*.*`. • En la columna Ubicación SFS (E), en la fórmula, confirme que el formato del rango CIDR de la VPC de destino funciona para su rango. Por ejemplo, si su rango de CIDR es `176.16.0.0/16` , introduzca `176.16.*.*` . 4. En la hoja de trabajo SFS-Data, haga lo siguiente: • En la columna Nombre del servidor (A), introduzca el nombre del servidor en el que está montado el SFS. • En la columna Ruta del SFS (B), introduzca el nombre del SFS. • En la columna Dirección IP (C), introduzca la dirección IP del servidor. • Agregue cualquier otra información relevante que haya recopilado durante	

Tarea	Descripción	Habilidades requeridas
	la detección, como el punto de montaje y el tamaño del SFS. Puede utilizar estos datos más adelante para modificar los cálculos de planificación de las olas. 5. Guarde el cuaderno de trabajo.	

Tarea	Descripción	Habilidades requeridas
Recopile información sobre los servidores.	1. Con la CMDB o los datos registrados en la herramienta de migración, identifique toda la siguiente información sobre los servidores que tienen soportes SFS: • Nombre del servidor • Dirección IP • Onda • Unidad organizativa (OU) • Entorno de servidor, como `DEV`, `QA` o `PROD` • Nombre de la aplicación • Propietario de la aplicación e información de contacto 2. Abra el archivo SFS-Discovery-Workbook. 3. En la hoja de trabajo Server-Data, en las columnas A a H, introduzca la información que recopiló sobre los servidores de origen. Tenga en cuenta lo siguiente: • En la columna Wave # (C), introduzca el nombre de la onda (por ejemplo`Wave1`), out-of-scope (`OOS`) o. `Retire` • Si aparece en la columna de Contacto del propietar	Ingeniero de migraciones, líder de migración

Tarea	Descripción	Habilidades requeridas
	io de la aplicación (H), compruebe que la dirección de correo electrónico sea correcta. Esta dirección de correo electrónico se genera automáticamente en función del nombre que proporcionó en la columna del Propietario de la aplicación (G). Si es necesario, actualice manualmente el valor para que refleje la dirección de correo electrónico correcta. • No modifique las columnas I a J, que contienen fórmulas. 4. Guarde el cuaderno de trabajo.	

Planifique

Tarea	Descripción	Habilidades requeridas
Cree el plan de olas del SFS.	1. Abra el archivo SFS-Discovery-Workbook. 2. Compruebe que toda la información recopilada en la fase de descubrimiento sea precisa y esté actualizada.	Responsable de compilación, líder de transición, ingeniero de migraciones, líder de migraciones

Tarea	Descripción	Habilidades requeridas
	3. En la hoja de trabajo Wave-Sheet, filtre la columna de onda SFS (K) según el valor 1. Esta es una lista de todos los SFS de la primera onda. Nota: Un valor de `0` en esta columna indica que el SFS está fuera del ámbito de la migración. Esto puede deberse a que el SFS ya está alojado en AWS o a que los servidores que acceden al recurso compartido están fuera del ámbito de la migración. 4. Compruebe que desea migrar estos SFS en esta onda. Para obtener más información sobre cómo asignar los SFS a las olas, consulte Enfoques de planificación de las ondas en la sección Prácticas recomendadas. 5. Seleccione y copie las celdas que contienen los valores filtrados. No copie la fila de encabezado que contiene los títulos de las columnas.	

Tarea	Descripción	Habilidades requeridas
	6. Abra el archivo SFS-Wave-Plan-Workbook que descargó anteriormente. 7. En la hoja de trabajo Export-from-Discovery, seleccione la celda A2. 8. Pegue los datos copiados. 9. Guarde los archivos SFS-Discovery-Workbook y SFS-Wave-Plan-Workbook.	

Tarea	Descripción	Habilidades requeridas
Elija el servicio de AWS y la herramienta de migración de destino.	1. En el archivo SFS-Wave-Plan-Workbook, en la hoja de trabajo Exported-from-Discovery, seleccione y copie los valores de la columna Ruta anterior (C). 2. En la hoja de trabajo Build-Wave, seleccione la celda A2. 3. Pegue los datos copiados. Las columnas B a M de esta hoja de trabajo se actualizan automáticamente para reflejar otros datos asociados a esta ruta. 4. Elimine los valores duplicados de la columna A. Para obtener instrucciones, consulte Eliminar valores duplicados (sitio web de soporte de Microsoft). 5. En la columna Patrón o servicio de destino (F), revise el servicio de AWS de destino recomenda do y actualícelo según sea necesario. Para obtener más información, consulte Elegir un servicio de sistema de archivos de AWS en la sección Prácticas recomendadas de este patrón.	Ingeniero de migraciones, líder de migración

Tarea	Descripción	Habilidades requeridas
	6. En la columna Método de migración (G), revise la herramienta de migración recomendada y actualíce la según sea necesario. Para obtener más información, consulte Elegir una herramienta de migración en la sección de Prácticas recomendadas de este patrón. 7. Guarde el archivo SFS-Discovery-Workbook. Ha terminado de crear un plan de onda para esta ola. 8. Repita estas instrucciones para preparar un plan de onda para cada ola. Como los planes de onda están sujetos a cambios durante la migración, le recomendamos que planifique con no más de 5 ondas de antelación.	

Preparación

Tarea	Descripción	Habilidades requeridas
Configure el sistema de archivos de destino.	De acuerdo con los detalles registrados en su plan de onda, configure los sistemas de archivos de destino en la cuenta de AWS, la VPC	Ingeniero de migraciones, líder de migración, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	y las subredes de destino. Para obtener instrucciones, consulte la siguiente documentación de AWS: • Amazon EFS • Amazon FSx para ONTAP NetApp • Amazon FSx para Windows File Server	

Tarea	Descripción	Habilidades requeridas
Configure la herramienta de migración y transfiera los datos.	1. Si utiliza AWS DataSync, configure el registro de las DataSync tareas. Para obtener instrucciones, consulte Registrar las actividades de las DataSync tareas de AWS. 2. Configure la herramienta de migración y realice una transferencia de datos inicial según las instrucciones de la herramienta que haya seleccionado: • Para Amazon EFS, consulte lo siguiente: • Transfiera archivos a Amazon EFS mediante AWS DataSync • Para Amazon FSx para ONTAP, consulte lo siguiente: • Migración a FSx para ONTAP mediante NetApp SnapMirror • Migración a FSx para ONTAP mediante AWS DataSync • Para Amazon FSx para Windows File Server, consulte lo siguiente: • Migración de archivos existentes a FSx for Windows File	Administrador de AWS, administrador de la nube, ingeniero de migraciones, líder de migración

Tarea	Descripción	Habilidades requeridas
	Server mediante AWS DataSync • Migración de archivos existentes a FSx for Windows File Server mediante Robocopy 3. Los cambios en el SFS de origen pueden producirse durante o después de la transferencia inicial. Configure transferencias de datos recurrentes entre los sistemas de archivos de origen y destino para mantener los datos sincronizados: • Si lo está utilizando DataSync, consulte Programar DataSync una tarea de AWS. DataSync transfiere solo los archivos nuevos o modificados del SFS de origen. • Si utiliza una herramienta de terceros, consulte la documentación de la herramienta que hayas seleccionado.	

Tarea	Descripción	Habilidades requeridas
Actualice el plan de onda.	1. Abra el archivo SFS-Wave-Plan-Workbook para la oleada actual. 2. En la hoja de trabajo Build-Wave, en la columna Nueva dirección IP de ruta (N), introduzca la dirección IP del sistema de archivos de destino. Aplique alguna de las siguientes acciones para localizar la dirección IP: • Para FSx for Windows File Server, en la consola de Amazon FSx, elija Sistemas de archivos, elija su sistema de archivos y, a continuación, consulte la sección Red y seguridad. • Para FSx para ONTAP, consulte Montaje de volúmenes. • Para Amazon EFS, consulte Montaje con una dirección IP. 3. En la columna Nueva ruta (O), introduzca la nueva ruta de montaje. La ruta de montaje es el nombre de DNS del sistema de archivos. Aplique alguna de las siguientes acciones	Ingeniero de migraciones, líder de migración

Tarea	Descripción	Habilidades requeridas
	para localizar la ruta de montaje: • Para FSx for Windows File Server, en la consola de Amazon FSx, elija Sistemas de archivos, elija su sistema de archivos y, a continuac ión, seleccione Adjuntar. • Para FSx para ONTAP, consulte la página de detalles del Sistema de archivos. Para obtener instrucciones, consulte Montaje de volúmenes. • Para Amazon EFS, consulte Obtener información. 4. En la hoja de trabajo Remount-Summary, confirme que las columnas Nueva ruta (C) y Nueva dirección IP de ruta (D) reflejan los valores actualizados. 5. Confirme que su organizac ión haya preparado manuales de procedimi entos para volver a montar los sistemas de archivos de Linux y Windows tras la transición. Para obtener instrucciones, consulte lo siguiente:	

Tarea	Descripción	Habilidades requeridas
	• Montaje de sistemas de archivos de EFS • Acceso a recursos compartidos de archivos de FSx para Windows File Server • Montaje de FSx para volúmenes ONTAP 6. Si algún servidor dependiente no está incluido en esta onda, regístrelo en la hoja de trabajo App-Team-Communication. Informe a los propietarios de las aplicaciones o servidores correspondientes, ya que es posible que no estén incluidos en las comunicaciones estándar. 7. Si los SFS se eliminan de la onda después de completar el plan de oleada, haga un seguimiento de los mismos en la hoja de trabajo Descoped.	

Realizar la transición

Tarea	Descripción	Habilidades requeridas
Detener la aplicación.	Si las aplicaciones o los clientes están realizando operaciones de lectura y	Propietario de la aplicación, desarrollador de la aplicación

Tarea	Descripción	Habilidades requeridas
	escritura de forma activa en el SFS de origen, deténgalos antes de realizar la sincroniz ación de datos final. Para obtener instrucciones, consulte la documenta ción de la aplicación o sus procesos internos para detener las actividades de lectura y escritura. Por ejemplo, consulte Iniciar o detener el servidor web (IIS 8) (documentación de Microsoft) o Administrar los servicios del sistema con systemctl (documentación de Red Hat).	

Tarea	Descripción	Habilidades requeridas
Realice la transferencia de datos final.	1. En la herramienta de migración, ejecute manualmente una tarea o trabajo final de transfere ncia de datos para sincronizar el sistema de archivos de destino con el SFS de origen. Para obtener instrucciones, consulte Cómo iniciar la DataSync tarea o consulte la documentación de la herramienta de migración de terceros que haya seleccionado. 2. Esperar a que se complete una transferencia. Para obtener más información, consulte Supervisión de la DataSync actividad de AWS con Amazon CloudWatch y Supervisión de la DataSync tarea desde la línea de comandos.	Ingeniero de migraciones, líder de migración

Tarea	Descripción	Habilidades requeridas
Valide la transferencia de datos.	Si utiliza AWS DataSync, haga lo siguiente para validar que la transferencia de datos final se haya realizado correctamente: 1. En la DataSync consola de AWS, anote el ID de la tarea y la ejecución, por ejemplo `task-0000-exec-1111` . 2. Navegue hasta la sección de registro de tareas de la DataSync tarea. 3. Elija el enlace al grupo de CloudWatch registros. 4. En los registros, busque la tarea y el ID de ejecución. 5. Tome nota de cualquier error de transferencia. Para obtener más información, consulte Errores comunes en la DataSync documentación. 6. Valide lo siguiente: • Compare las listas de archivos de los SFS de origen y destino para confirmar que se han transferido todos los datos • Compare los permisos de acceso a los archivos	Ingeniero de migraciones, líder de migración

Tarea	Descripción	Habilidades requeridas
	entre los SFS de origen y destino. Si utiliza una herramienta de terceros, consulte las instrucciones de validación de la transferencia de datos en la documentación de la herramienta de migración seleccionada.	

Valide

Tarea	Descripción	Habilidades requeridas
Vuelva a montar el sistema de archivos y valide la función y el rendimiento de la aplicación.	1. Si los servidores dependientes se migraron en esta oleada, en el archivo SFS-Wave-Plan-Workbook, en la hoja de trabajo Remount-Summary, introduzca la nueva dirección IP del servidor en la columna Nueva dirección IP del servidor (F). 2. En todos los servidores, actualice el punto de montaje del sistema de archivos desde la ruta anterior a la nueva. Utilice el manual de instrucciones de su organización para volver a montarlo, tal como	Administrador de sistemas de AWS, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	se describió anteriormente en la fase de Preparación. 3. Confirme que el sistema de archivos está montado correctamente y que es accesible comprobando los montajes y verificando que los archivos estén presentes. El equipo de infraestructura suele realizar estas actividades. 4. Reinicie las aplicaciones y pida a sus propietarios o al equipo de control de calidad que realicen las pruebas funcionales y de rendimiento de la aplicación, según sea necesario.	

Solución de problemas

Problema	Solución
Los valores de celda de Microsoft Excel no se actualizan.	Copie las fórmulas de las filas de muestra arrastrando el controlador de relleno. Para obtener más información, consulte las instrucciones para Windows o Mac (sitio web de soporte de Microsoft).

Recursos relacionados

Documentación de AWS

- DataSync Documentación de AWS

- Documentación de Amazon EFS
- Documentación de Amazon FSx
- Grandes migraciones a la nube de AWS
  - Guía para grandes migraciones de AWS
  - Guía de portafolio para grandes migraciones a AWS

Solución de problemas

- Solución de DataSync problemas de AWS
- Solución de problemas de Amazon EFS
- Solución de problemas de Amazon FSx para Windows File Server
- Solución de problemas de Amazon FSx para ONTAP NetApp

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Migre una base de datos Oracle a Amazon RDS for Oracle mediante adaptadores de archivos planos de GoldenGate Oracle

Creado por Dhairya Jindani (AWS) y Baji Shaik (AWS)

Entorno: PoC o piloto	Origen: una base de datos Oracle (en las instalaciones o en una instancia de EC2)	Destino: Amazon RDS para Oracle
Tipo R: redefinir la plataforma	Carga de trabajo: Oracle	Tecnologías: Migración; Análisis; Bases de datos
Servicios de AWS: Amazon RDS		

Resumen

Oracle GoldenGate es un servicio de captura y replicación de datos en tiempo real para bases de datos y entornos de TI heterogéneos. Sin embargo, este servicio no admite actualmente Amazon Relational Database Service (Amazon RDS) para Oracle. Para obtener una lista de las bases de datos compatibles, consulte Oracle GoldenGate para bases de datos heterogéneas (documentación de Oracle). Este patrón describe cómo utilizar Oracle GoldenGate y los adaptadores de archivos GoldenGate planos de Oracle para generar archivos planos a partir de la base de datos Oracle de origen, que puede estar en las instalaciones o en una instancia de Amazon Elastic Compute Cloud (Amazon EC2). A continuación, puede importar esos archivos planos a una instancia de base de datos de Amazon RDS para Oracle.

En este patrón, se utiliza Oracle GoldenGate para extraer los archivos de seguimiento de la base de datos Oracle de origen. La bomba de datos copia los archivos de seguimiento en un servidor de integración, que es una instancia de EC2. En el servidor de integración, Oracle GoldenGate utiliza el adaptador de archivos planos para generar una serie de archivos planos secuenciales basados en la captura de datos transacionales de los archivos de seguimiento. Oracle GoldenGate formatea los datos como valores separados por delimitadores o valores delimitados por longitud. A continuación, utilice Oracle SQL*Loader para importar los archivos planos a la instancia de base de datos Amazon RDS para Oracle de destino.

Público objetivo

Este patrón está destinado a quienes tienen experiencia y conocimiento de los componentes fundamentales de un Oracle. GoldenGate Para obtener más información, consulte Descripción general de la GoldenGate arquitectura de Oracle (documentación de Oracle).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de Amazon Web Services (AWS) activa.
- Una GoldenGate licencia de Oracle.
- Una licencia independiente para un GoldenGate adaptador de Oracle.
- Una base de datos de Oracle de origen, que se ejecute en las instalaciones o en una instancia de EC2.
- Una instancia de EC2 de Linux que se utiliza como servidor de integración. Para obtener más información, consulte Introducción a las instancias de Linux de Amazon EC2 (documentación de Amazon EC2).
- Una instancia de base de datos de Amazon RDS para Oracle. Para obtener más información, consulte Creación de una instancia de base de datos de Oracle (documentación de Amazon RDS).

Versiones de producto

- Oracle Database Enterprise Edition, versión 10g, 11g, 12c o posterior
- Oracle GoldenGate versión 12.2.0.1.1 o posterior

Arquitectura

Pila de tecnología de origen

Una base de datos Oracle (local o en una instancia de EC2)

Pila de tecnología de destino

Amazon RDS para Oracle

Arquitectura de origen y destino

1. Oracle GoldenGate extrae las pistas de los registros de la base de datos de origen.
2. La bomba de datos extrae los rastros y los migra a un servidor de integración.
3. El adaptador de archivos GoldenGate planos de Oracle lee los registros, las definiciones de las fuentes y los parámetros de extracción.
4. Se sale de la extracción, que genera un archivo de control y archivos de datos planos.
5. Los archivos de datos planos se migran a una instancia de base de datos de Amazon RDS para Oracle en la nube de AWS.

Herramientas

Servicios de AWS

- Amazon Elastic Compute Cloud (Amazon EC2) brinda capacidad de computación escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon Relational Database Service (Amazon RDS) para Oracle ayuda a configurar, utilizar y escalar una base de datos relacional en la nube de AWS.

Otros servicios

- Oracle GoldenGate es un servicio que le ayuda a replicar, filtrar y transformar datos de una base de datos a otra base de datos heterogénea o a otra topología de destino, como archivos planos.
- Los adaptadores de GoldenGate aplicaciones de Oracle permiten GoldenGate a Oracle producir una serie de archivos planos secuenciales y archivos de control a partir de los datos transaccionales capturados en los archivos de seguimiento de una base de datos de origen. Estos adaptadores se utilizan ampliamente para operaciones de extracción, transformación y carga (ETL) en aplicaciones de data warehouse y en aplicaciones de propiedad o heredadas. Oracle GoldenGate realiza esta captura y la aplica prácticamente en tiempo real en bases de datos, plataformas y sistemas operativos heterogéneos. Los adaptadores admiten diferentes formatos para los archivos de salida, como CSV o Apache Parquet. Puede cargar estos archivos generados para cargar los datos en diferentes bases de datos heterogéneas.

Epics

Configure Oracle GoldenGate en el servidor de base de datos de origen

Tarea	Descripción	Habilidades requeridas
Descargue Oracle GoldenGate.	En el servidor de base de datos de origen, descargue la GoldenGate versión 12.2.0.1.1 o posterior de Oracle. Para obtener instrucciones, consulte Descarga de Oracle GoldenGate (documentación de Oracle).	Administrador de base de datos
Instale Oracle GoldenGate.	Para obtener instrucciones, consulte Instalación de Oracle GoldenGate (documentación de Oracle).	Administrador de base de datos
Configure Oracle GoldenGate.	Para obtener instrucciones, consulte Preparación de la base de datos para Oracle GoldenGate (documentación de Oracle).	Administrador de base de datos

Configure Oracle GoldenGate en el servidor de integración

Tarea	Descripción	Habilidades requeridas
Descargue Oracle GoldenGate.	En el servidor de integración, descargue la GoldenGate versión 12.2.0.1.1 o posterior de Oracle. Para obtener instrucciones, consulte Descarga de Oracle	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	GoldenGate (documentación de Oracle).	
Instale Oracle GoldenGate.	Cree directorios, configure el proceso de administración y cree el archivo `defgen` para un entorno heterogéneo. Para obtener instrucciones, consulte Instalación de Oracle GoldenGate (documentación de Oracle).	Administrador de base de datos

Cambie la configuración de captura GoldenGate de datos de Oracle

Tarea	Descripción	Habilidades requeridas
Prepare los GoldenGate adaptadores de Oracle.	En el servidor de integración, configure el software del GoldenGate adaptador de Oracle. Haga lo siguiente: 1. Desde Oracle Software Delivery Cloud, descargue ggs_Adapters_Linux_x64.zip. 2. Descomprima ggs_Adapters_Linux_x64.zip. 3. Ejecute el siguiente comando para instalar los adaptadores. `tar -xvf ggs_Adapters_Linux_x64.tar`	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Configure la bomba de datos.	En el servidor de origen, configure la bomba de datos para transferir el archivo de seguimiento del servidor de origen al servidor de integración. Cree el archivo de parámetros de la bomba de datos y el directorio de archivos de senderos. Para obtener instrucciones, consulte Configuración del adaptador de archivos planos (documentación de Oracle).	Administrador de base de datos

Generar y migrar los archivos planos

Tarea	Descripción	Habilidades requeridas
Genere los archivos planos.	Cree el archivo de extracción y el archivo de control y, a continuación, inicie el proceso de extracción en el servidor de integración. Esto extrae los cambios de la base de datos y graba la base de datos de origen en los archivos planos. Para obtener instrucciones, consulte Uso del adaptador de archivos planos (documentación de Oracle).	Administrador de base de datos
Cargue los archivos planos en la base de datos de destino.	Cargue los archivos planos en la instancia de base de datos de Amazon RDS para Oracle	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	de destino. Para obtener más información, consulte Importación mediante Oracle SQL*Loader (documentación de Amazon RDS).	

Solución de problemas

Problema	Solución
El adaptador de archivos GoldenGate planos de Oracle genera un error.	Para obtener una descripción de los errores del adaptador, consulte Localización de mensajes de error (documentación de Oracle). Para obtener instrucciones de solución de problemas , consulte Solución de problemas del adaptador de archivos planos (documentación de Oracle).

Recursos relacionados

- Instalación de Oracle GoldenGate (documentación de Oracle)
- Configuración de Oracle GoldenGate (documentación de Oracle)
- Descripción de los GoldenGate adaptadores Oracle (documentación de Oracle)
- Configuración del adaptador de archivos planos (documentación de Oracle)

Cambie las aplicaciones de Python y Perl para que admitan la migración de bases de datos de Microsoft SQL Server a una edición compatible con PostgreSQL de Amazon Aurora

Creado por Dwarika Patra (AWS) y Deepesh Jayaprakash (AWS)

Entorno: PoC o piloto	Origen: SQL Server	Destino: Aurora compatible con PostgreSQL
Tipo R: redefinir la plataforma	Carga de trabajo: Microsoft; código abierto	Tecnologías: migración; bases de datos
Servicios de AWS: Amazon Aurora		

Resumen

Este patrón describe los cambios en los repositorios de aplicaciones que pueden ser necesarios al migrar bases de datos de Microsoft SQL Server a una edición compatible con Amazon Aurora PostgreSQL. El patrón asume que estas aplicaciones están basadas en Python o en Perl, y proporciona instrucciones independientes para estos lenguajes de secuencias de comandos.

La migración de bases de datos de SQL Server a una versión compatible con Aurora PostgreSQL implica la conversión de esquemas, la conversión de objetos de base de datos, la migración de datos y la carga de datos. Debido a las diferencias entre PostgreSQL y SQL Server (en relación con los tipos de datos, los objetos de conexión, la sintaxis y la lógica), la tarea de migración más difícil consiste en realizar los cambios necesarios en la base de código para que funcione correctamente con PostgreSQL.

Para una aplicación basada en Python, los objetos y clases de conexión están dispersos por todo el sistema. Además, la base de código de Python puede usar varias bibliotecas para conectarse a la base de datos. Si la interfaz de conexión a la base de datos cambia, los objetos que ejecutan las consultas en línea de la aplicación también requieren cambios.

En el caso de una aplicación basada en Perl, los cambios se refieren a los objetos de conexión, los controladores de conexión a la base de datos, las sentencias SQL integradas estáticas y dinámicas

y la forma en que la aplicación gestiona las consultas DML dinámicas y complejas y los conjuntos de resultados.

Al migrar la aplicación, también puede considerar posibles mejoras en AWS, como reemplazar el servidor FTP por el acceso a Amazon Simple Storage Service (Amazon S3).

El proceso de migración de la aplicación implica los siguientes desafíos:

- Objetos de conexión. Si los objetos de conexión están dispersos en el código con varias bibliotecas y llamadas a funciones, es posible que tenga que encontrar una forma generalizada de cambiarlos para que sean compatibles con PostgreSQL.
- Gestión de errores o excepciones durante la recuperación o actualización de registros. Si tiene operaciones condicionales de creación, lectura, actualización y eliminación (CRUD) en la base de datos que devuelven variables, conjuntos de resultados o marcos de datos, cualquier error o excepción puede provocar errores de aplicación con efectos en cascada. Estas deben gestionarse con cuidado, con las validaciones adecuadas y ahorrándose puntos. Uno de estos puntos de ahorro es llamar a consultas SQL integradas de gran tamaño o a objetos de bases de datos dentro de bloques `BEGIN...EXCEPTION...END`.
- Controlar las transacciones y su validación. Esto incluye las confirmaciones y anulaciones manuales y automáticas. El controlador PostgreSQL para Perl requiere que siempre se establezca de forma explícita el atributo autocommit.
- Manejo de consultas SQL dinámicas. Esto requiere una sólida comprensión de la lógica de consultas y pruebas iterativas para garantizar que las consultas funcionen según lo esperado.
- Desempeño. Debe asegurarse de que los cambios en el código no reduzcan el rendimiento de la aplicación.

Este patrón explica el proceso de conversión en detalle.

Requisitos previos y limitaciones

Requisitos previos

- Conocimientos prácticos de la sintaxis de Python y Perl.
- Conocimientos básicos de SQL Server y PostgreSQL.
- Comprensión de la arquitectura de aplicaciones existente.
- Acceda al código de su aplicación, a la base de datos de SQL Server y a la base de datos PostgreSQL.

- Acceda al entorno de desarrollo Windows o Linux (u otro tipo de Unix) con credenciales para desarrollar, probar y validar los cambios en las aplicaciones.
- En el caso de una aplicación basada en Python, las bibliotecas de Python estándar que pueda necesitar la aplicación, como Pandas para gestionar marcos de datos, y psycopg2 o SQLAlchemy para las conexiones a bases de datos.
- Para una aplicación basada en Perl, se requieren paquetes de Perl con bibliotecas o módulos dependientes. El módulo Comprehensive Perl Archive Network (CPAN) es compatible con la mayoría de los requisitos de las aplicaciones.
- Todas las bibliotecas o módulos personalizados dependientes necesarios.
- Credenciales de bases de datos para acceso de lectura a SQL Server y acceso de lectura y escritura a Aurora.
- PostgreSQL para validar y depurar los cambios en las aplicaciones con los servicios y los usuarios.
- Acceso a herramientas de desarrollo durante la migración de aplicaciones, como Visual Studio Code, Sublime Text o pgAdmin.

Limitaciones

- Algunas versiones, módulos, bibliotecas y paquetes de Python o Perl no son compatibles con el entorno de nube.
- Algunas bibliotecas y marcos de terceros utilizados para SQL Server no se pueden reemplazar para admitir la migración a PostgreSQL.
- Las variaciones de rendimiento pueden requerir cambios en la aplicación, en las consultas de Transact-SQL (T-SQL) integradas, en las funciones de las bases de datos y en los procedimientos almacenados.
- PostgreSQL admite nombres en minúsculas para nombres de tablas, nombres de columnas y otros objetos de bases de datos.
- Algunos tipos de datos, como las columnas UUID, se almacenan únicamente en minúsculas. Las aplicaciones Python y Perl deben gestionar estas diferencias entre mayúsculas y minúsculas.
- Las diferencias de codificación de caracteres deben gestionarse con el tipo de datos correcto para las columnas de texto correspondientes de la base de datos PostgreSQL.

Versiones de producto

- Python 3.6 o posterior (usa la versión compatible con tu sistema operativo)

- Perl 5.8.3 o posterior (utilice la versión compatible con su sistema operativo)
- Aurora, compatible con PostgreSQL, edición 4.2 o posterior (consulte los detalles)

Arquitectura

Pila de tecnología de origen

- Lenguaje de secuencias de comandos (programación de aplicaciones): Python 2.7 o posterior, o Perl 5.8
- Base de datos: Microsoft SQL Server versión 13
- Sistema operativo: Red Hat Enterprise Linux (RHEL) 7

Pila de tecnología de destino

- Lenguaje de secuencias de comandos (programación de aplicaciones): Python 3.6 o posterior de Perl
- Base de datos: Compatible con Aurora PostgreSQL
- Sistema operativo: RHEL 7

Arquitectura de migración

Herramientas

Herramientas y servicios de AWS

- La edición de Amazon Aurora compatible con PostgreSQL es un motor de bases de datos relacionales, completamente administrado, compatible con PostgreSQL y conforme a ACID, que combina la velocidad y la fiabilidad de las bases de datos comerciales de tecnología avanzada con la sencillez y la rentabilidad de las bases de datos de código abierto. Aurora PostgreSQL es un reemplazo instántaneo para PostgreSQL que simplifica y hace más rentable configurar, usar y escalar las implementaciones de PostgreSQL nuevas y existentes.
- La Interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.

Otras herramientas

- Bibliotecas de conexión a bases de datos de Python y PostgresSQL, como psycopg2 y SQLAlchemy
- Perl y sus módulos de DBI
- Terminal interactiva PostgreSQL (psql)

Epics

Migre su repositorio de aplicaciones a PostgreSQL: pasos de alto nivel

Tarea	Descripción	Habilidades requeridas
Siga estos pasos de conversión de código para migrar su aplicación a PostgreSQL.	1. Configure bibliotecas y controladores ODBC específicos de la base de datos para PostgreSQL. Por ejemplo, puede usar uno de los módulos CPAN para Perl y pyodbc, psycopg2 o SQLAlchemy para Python. 2. Convierta los objetos de la base de datos mediante estas bibliotecas para conectarse a Aurora compatible con PostgreSQL. 3. Aplique los cambios de código en los módulos de aplicación existentes para obtener sentencias T-SQL compatibles. 4. Reescriba las llamadas a funciones específicas de la base de datos y los	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	procedimientos almacenados en el código de la aplicación. 5. Controle los cambios en las variables de la aplicación y sus tipos de datos que se utilizan para las consultas SQL en línea. 6. Gestione funciones específicas de bases de datos incompatibles. 7. end-to-end Prueba completa del código de aplicación convertido para la migración de bases de datos. 8. Compare los resultados de Microsoft SQL Server con los de la aplicación que migró a PostgreSQL. 9. Realice una evaluación comparativa del rendimiento de las aplicaciones entre Microsoft SQL Server y PostgreSQL. 10. Revise los procedimientos almacenados o las sentencias T-SQL en línea solicitadas por la aplicación para mejorar el rendimiento. Las siguientes epics proporcionan instrucciones detalladas	

Tarea	Descripción	Habilidades requeridas
	para algunas de estas tareas de conversión para aplicaciones de Python y Perl.	

Tarea	Descripción	Habilidades requeridas
Use una lista de verificación para cada paso de la migración.	Añada lo siguiente a la lista de verificación para cada paso de la migración de la aplicación, incluido el paso final: • Revise la documentación de PostgreSQL para asegurarse de que todos los cambios son compatibles con el estándar PostgreSQL. • Compruebe si hay valores enteros y flotantes en las columnas. • Identifique el número de filas insertadas, actualizadas y extraídas, junto con los nombres de las columnas y las marcas de fecha y hora. Puede utilizar una utilidad de diferencias o escribir un script para automatizar estas comprobaciones. • Realice las comprobaciones de rendimiento de las sentencias SQL integradas de gran tamaño y compruebe el rendimiento general de la aplicación. • Compruebe la correcta gestión de los errores en las operaciones de la base de datos y la correcta salida del	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	programa mediante el uso de varios bloques try/catch. • Asegúrese de que se hayan implementado los procesos de registro adecuados.	

Analice y actualice su aplicación: Base de código Python

Tarea	Descripción	Habilidades requeridas
Analice su base de código Python existente.	Su análisis debe incluir lo siguiente para facilitar el proceso de migración de la aplicación: • Identifique todos los objetos de conexión en el código. • Identifique todas las consultas SQL en línea incompatibles (como las sentencias T-SQL y los procedimientos almacenados) y analice los cambios necesarios. • Revise la documentación del código y realice un seguimiento del flujo de control para comprender la funcionalidad del código. Esto será útil más adelante, cuando pruebes la aplicación para comparar el rendimiento o la carga.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	• Comprenda el propósito de la aplicación para poder probarla eficazmente después de la conversió n de la base de datos. La mayoría de las aplicacio nes de Python que son aptas para la conversión con migraciones de bases de datos son fuentes que cargan datos de otras fuentes en tablas de bases de datos o extractores que recuperan datos de las tablas y los transform an en diferentes formatos de salida (como CSV, JSON o archivos planos) que son adecuados para crear informes o realizar llamadas a la API para realizar validaciones.	

Tarea	Descripción	Habilidades requeridas
Convierta sus conexiones de bases de datos para que sean compatibles con PostgreSQL.	La mayoría de las aplicaciones de Python utilizan la biblioteca pyodbc para conectarse con las bases de datos de SQL Server de la siguiente manera. `import pyodbc` `....` `try:` `conn_string = "Driver=ODBC Driver 17 for SQL Server;UID={};PWD={};Server={};Database={}".format (conn_user, conn_password, conn_server, conn_database)` `conn = pyodbc.connect(conn_string)` `cur = conn.cursor()` `result = cur.execute(query_string)` `for row in result:` `print (row)` `except Exception as e:` `print(str(e))` Convierta la conexión de base de datos para que sea compatible con PostgreSQL de la siguiente manera. `import pyodbc` `import psycopg2` `....` `try:`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	<pre> conn_string = 'postgresql+psycop g2://'+ conn_user+':'+conn _password+'@'+conn _server+'/'+conn_d atabase conn = pyodbc.co nnect(conn_string, connect_args={'opt ions':'-csearch_pa th=dbo'}) cur = conn.cursor() result = cur.execu te(query_string) for row in result: print (row) except Exception as e: print(str(e))</pre>	

Tarea	Descripción	Habilidades requeridas
Cambie las consultas SQL en línea a PostgreSQL.	Convierta sus consultas SQL en línea a un formato compatible con PostgreSQL. Por ejemplo, la siguiente consulta de SQL Server recupera una cadena de una tabla. `dtype = “type1”` `stm = ‘“SELECT TOP 1 searchcode FROM TypesTable (NOLOCK) WHERE code=”’ + “’” + str(dtype) + “’”` `# For Microsoft SQL Server Database Connection` `engine = create_engine(‘mssql+pyodbc:///?odbc_connect=%s’ % urllib.parse.quote_plus(conn_string), connect_args={‘connect_timeout’:login_timeout})` `conn = engine_connect()` `rs = conn.execute(stm)` `for row in rs:` `  print(row)` Tras la conversión, la consulta SQL en línea compatible con PostgreSQL tiene el siguiente aspecto. `dtype = “type1”`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`stm = '"SELECT searchcode FROM TypesTable WHERE code="' + "'" + str(dtype) + "' LIMIT 1"` `# For PostgreSQL Database Connection` `engine = create_engine('postgres+psycopg2://%s' %conn_string, connect_args={'connect_timeout':login_timeout})` `conn = engine.connect()` `rs = conn.execute(stm)` `for row in rs:` `  print(row)`	

Tarea	Descripción	Habilidades requeridas
Gestione consultas SQL dinámicas.	El SQL dinámico puede estar presente en un script o en varios scripts de Python. Los ejemplos anteriores mostraron cómo utilizar la función de reemplazo de cadenas de Python para insertar variables con el fin de crear consultas SQL dinámicas. Un enfoque alternativo consiste en añadir variables a la cadena de consulta siempre que sea aplicable. En el ejemplo siguiente, la cadena de consulta se construye sobre la marcha en función de los valores devueltos por una función. `query = '"SELECT id from equity e join issues i on e.permId=i.permId where e.id'"` `query += get_id_filter(ids) + " e.id is NOT NULL` Estos tipos de consultas dinámicas son muy comunes durante la migración de aplicaciones. Siga estos pasos para gestionar consultas dinámicas:	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	• Compruebe la sintaxis general (por ejemplo, la sintaxis de la sentencia `SELECT` con una cláusula `JOIN`). • Compruebe todos los nombres de variables o columnas utilizados en la consulta, como `i` y `id`. • Compruebe las funciones, los argumentos y los valores devueltos utilizados en la consulta (por ejemplo, `get_id_filter` y su argumento `ids`).	

Tarea	Descripción	Habilidades requeridas
Gestione los conjuntos de resultados, las variables y los marcos de datos.	Para Microsoft SQL Server, se utilizan métodos de Python como `fetchone()` o `fetchall()` para recuperar el conjunto de resultados de la base de datos. También puede usar `fetchmany(size)` y especificar el número de registros que se van a devolver del conjunto de resultados. Para ello, puede utilizar el objeto de conexión pyodbc como se muestra en el siguiente ejemplo. pyodbc (Microsoft SQL Server) `import pyodbc` `server = 'tcp:myse` `rver.database.wind` `ows.net'` `database = 'exampledb'` `username = 'exampleu` `sername'` `password = 'examplep` `assword'` `conn = pyodbc.co` `nnect('DRIVER={ODB` `C Driver 17 for SQL` ` Server};SERVER='+s` `erver+';DATABASE='` `+database+';UID='+` `username+';PWD='+` ` password)` `cursor = conn.cursor()` `cursor.execute("SELECT` ` * FROM ITEMS")`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`row = cursor.fe tchone() while row: print(row[0]) row = cursor.fe tchone()` En Aurora, para realizar tareas similares, como conectars e a PostgreSQL y obtener conjuntos de resultados, puede usar psycopg2 o SQLAlchemy. Estas bibliotec as de Python proporcionan el módulo de conexión y el objeto de cursor para recorrer los registros de la base de datos PostgreSQL, como se muestra en el siguiente ejemplo. psycopg2 (Aurora compatible con PostgreSQL) `import psycopg2 query = "SELECT * FROM ITEMS;" //Initialize variables host=dbname=user= password=port=sslm ode=connect_timeou t="" connstring = "host='{h ost}' dbname='{ dbname}' user='{user}' \`	

Tarea	Descripción	Habilidades requeridas
	password='{passw ord}'port='{port}' ".format(host=host ,dbname=dbname,\ user=user,password= password,port=port) conn = psycopg2. connect(connstring) cursor = conn.cursor() cursor.execute(query) column_names = [column[0] for column in cursor.description] print("Column Names: ", column_names) print("Column values: " for row in cursor: print("itemid :", row[0]) print("itemdescrpt ion :", row[1]) print("it emprice :", row[3]))	
	SQLAlchemy (compatible con Aurora PostgreSQL) from sqlalchemy import create_engine from pandas import DataFrame conn_string = 'postgres ql://core:database @localhost:5432/ex ampledatabase' engine = create_en gine(conn_string) conn = engine.co nnect() dataid = 1001	

Tarea	Descripción	Habilidades requeridas
	`result = conn.exec ute("SELECT * FROM ITEMS") df = DataFrame (result.fetchall()) df.columns = result.ke ys() df = pd.DataFrame() engine.connect() df = pd.read_sql_query( sql_query, engine, coerce_float=False) print(“df=”, df)`	

Tarea	Descripción	Habilidades requeridas
Pruebe la aplicación durante y después de la migración.	La prueba de la aplicació n Python migrada es un proceso continuo. Como la migración incluye cambios en los objetos de conexión (psycopg2 o SQLAlchemy), la gestión de errores, nuevas funciones (marcos de datos), cambios en el SQL en línea, funcionalidades de copia masiva (`bcp` en lugar de `COPY`) y cambios similares , debe probarse detenidam ente durante y después de la migración de la aplicación. Consultar si: • Condiciones y manejo del error • Algún desajuste en los registros tras la migración • Actualizaciones o eliminaci ones de registros • Tiempo necesario para poder ejecutar la aplicación	Desarrollador de aplicaciones

Analice y actualice su aplicación: base de código Perl

Tarea	Descripción	Habilidades requeridas
Analice su base de código Perl existente.	Su análisis debe incluir lo siguiente para facilitar el proceso de migración de la aplicación. Debe identificar:	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	• Cualquier código INI o basado en la configuración • Controladores Perl de Open Database Connectivity (ODBC) estándar para bases de datos específicos de bases de datos o cualquier controlador personalizado • Se requieren cambios de código para las consultas en línea y T-SQL • Interacciones entre varios módulos de Perl (por ejemplo, un único objeto de conexión ODBC de Perl al que varios componentes funcionales llaman o utilizan) • Manejo de conjuntos de datos y conjuntos de resultados • Bibliotecas de Perl externas y dependientes • Cualquier API que se utilice en la aplicación • Compatibilidad de versiones de Perl y compatibilidad de controladores con Aurora compatible con PostgreSQL	

Tarea	Descripción	Habilidades requeridas
Convierta las conexiones de la aplicación Perl y el módulo DBI para que sean compatibl es con PostgreSQL.	Las aplicaciones basadas en Perl suelen utilizar el módulo DBI de Perl, que es un módulo de acceso a bases de datos estándar para el lenguaje de programación Perl. Puede usar el mismo módulo DBI con controladores diferentes para SQL Server y PostgreSQL. Para obtener más informaci ón sobre los módulos de Perl necesarios, las instalaci ones y otras instrucciones, consulte la documentación de DBD::Pg. El siguiente ejemplo se conecta a Aurora compatible con PostgreSQL en `exampletest-aurora pg-database.cluste r-sampleclusture.u s-east-.rds.amazon aws.com` . `#!/usr/bin/perl` `use DBI;` `use strict;` `my $driver = "Pg";` `my $hostname = “examplet` `est-aurorapg-datab` `ase-sampleclusture` `.us-east.rds.amazo` `naws.com”` `my $dsn = "DBI:$driver:` ` dbname = $hostname` `;host = 127.0.0.1;port` ` = 5432";`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`my $username = "postgres";` `my $password = "pass123";` `$dbh = DBI->connect("dbi:Pg:dbname=$hostname;host=$host;port=$port;options=$options",` `$username,` `$password,` `{AutoCommit => 0, RaiseError => 1, PrintError => 0}` `);`	

Tarea	Descripción	Habilidades requeridas
Cambie las consultas SQL en línea a PostgreSQL.	Es posible que su aplicación tenga consultas SQL en línea con `SELECT`, `DELETE`, `UPDATE` y sentencias similares que incluyan cláusulas de consulta que PostgreSQL no admite. Por ejemplo, consulte palabras clave como `TOP` y `NOLOCK` no se admiten en PostgreSQL. En los siguientes ejemplos, se muestra cómo se pueden gestionar `TOP`, `NOLOCK` y variables booleanas. En SQL Server: `$sqlStr = $sqlStr . "WHERE a.student_id in (SELECT TOP $numofRecords c_student_id \ FROM active_student_record b WITH (NOLOCK) \ INNER JOIN student_contributor c WITH (NOLOCK) on c.contributor_id = b.c_st)` Para PostgreSQL, conviértalo a: `$sqlStr = $sqlStr . "WHERE a.student_id in (SELECT TOP $numofRecords c_student_id \`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	FROM active_student_rec ord b INNER JOIN student_contributor c \ on c.contributor_id = b.c_student_contr_id WHERE b_current_1 is true \ LIMIT $numofRecords)"	

Tarea	Descripción	Habilidades requeridas
Gestione consultas SQL dinámicas y variables de Perl.	Las consultas SQL dinámicas son sentencias SQL que se crean durante el tiempo de ejecución de la aplicación. Estas consultas se crean de forma dinámica cuando la aplicación está en ejecución , en función de determinadas condiciones, por lo que el texto completo de la consulta no se conoce hasta el tiempo de ejecución. Un ejemplo es una aplicación de análisis financiero que analiza las 10 principales acciones a diario, y estas acciones cambian todos los días. Las tablas SQL se crean en función de los mejores resultados y los valores no se conocen hasta el tiempo de ejecución. Supongamos que las consultas SQL en línea de este ejemplo se pasan a una función contenedora para obtener los resultados establecidos en una variable y, a continuación, una variable utiliza una condición para determinar si la tabla existe: • Si la tabla existe, no la cree; procésela.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	• Si la tabla no existe, créela y, a continuación, procésela. A continuación, se muestra un ejemplo de gestión de variables, seguido de las consultas de SQL Server y PostgreSQL para este caso de uso. `my $tableexists = db_read( arg 1, $sql_qry, undef, 'writer'); my $table_already_exists = $tableexists->[0]{table_exists}; if ($table_already_exists){ # do some thing } else { # do something else }` SQL Server: `my $sql_qry = “SELECT OBJECT_ID('$backendTable', 'U') table_exists", undef, 'writer') ";` PostgreSQL: `my $sql_qry = “SELECT TO_REGCLASS('$backendTable', 'U')`	

Tarea	Descripción	Habilidades requeridas
	table_exists", undef, 'writer')"; En el siguiente ejemplo, se utiliza una variable de Perl en SQL en línea, que ejecuta una sentencia `SELECT` con un `JOIN` para obtener la clave principal de la tabla y la posición de la columna clave. SQL Server: `my $sql_qry = "SELECT column_name', character_maxi mum_length \ FROM INFORMATION_SCHEMA .COLUMNS \ WHERE TABLE_SCH EMA='$example_sche maInfo' \ AND TABLE_NAME='$examp le_table' \ AND DATA_TYPE IN ('varchar','nvarch ar');";` PostgreSQL: `my $sql_qry = "SELECT c1.column_name, c1.ordinal_position \ FROM information_schema .key_column_usage AS c LEFT \ JOIN information_schema .table_constraints AS t1 \`	

Tarea	Descripción	Habilidades requeridas
	`ON t1.constraint_name = c1.constraint_name \ WHERE t1.table_name = $example_schemaInfo'.'$example_table' \ AND t1.constraint_type = 'PRIMARY KEY' ;";`	

Realice cambios adicionales en su aplicación basada en Perl o Python para admitir PostgreSQL

Tarea	Descripción	Habilidades requeridas
Convierta construcciones adicionales de SQL Server a PostgreSQL.	Los siguientes cambios se aplican a todas las aplicaciones, independientemente del lenguaje de programación. • Califique los objetos de base de datos que utiliza su aplicación con nombres de esquema nuevos y adecuados. • Gestione los operadores LIKE para hacer coincidir mayúsculas de minúsculas con la característica de intercalación de PostgreSQL. • Gestione funciones específicas de bases de datos no compatibles, como `DATEDIFF`, `DATEADD`, `GETDATE`, `CONVERT` y los operadores `CAST`. Para ver funciones equivalentes	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	compatibles con PostgreSQL, consulte Funciones SQL nativas o integradas en la sección Información adicional. • Maneje los valores booleanos en las declaraciones comparativas. • Maneje los valores de retorno de las funciones. Pueden ser conjuntos de registros, marcos de datos, variables y valores booleanos. Gestiónelos de acuerdo con los requisitos de su aplicación y para admitir PostgreSQL. • Gestione bloques anónimos (por ejemplo, `BEGIN TRAN`) con nuevas funciones de PostgreSQL definidas por el usuario. • Convierta inserciones masivas en filas. El equivalente en PostgreSQL de la utilidad Copia masiva (`bcp`) de SQL Server, a la que se llama desde dentro de la aplicación, es `COPY`. • Convierta los operadores de concatenación de columnas. SQL Server usa + para la	

Tarea	Descripción	Habilidades requeridas
	concatenación de cadenas, pero PostgreSQL usa ||.	

Mejoró el desempeño

Tarea	Descripción	Habilidades requeridas
Aproveche los servicios de AWS para mejorar el rendimiento.	Al migrar a la nube de AWS, puede refinar el diseño de sus aplicaciones y bases de datos para aprovechar los servicios de AWS. Por ejemplo, si las consultas de su aplicación Python, que está conectada a un servidor de bases de datos compatible con Aurora PostgreSQL, tardan más que las consultas originales de Microsoft SQL Server, podría considerar la posibilidad de crear una fuente de datos históricos directamente a un bucket de Amazon Simple Storage Service (Amazon S3) desde el servidor Aurora y utilizar consultas SQL basadas en Amazon Athena para generar informes y consultas de datos analíticos para sus usuarios. cuadros de mando.	Desarrollador de aplicaciones, arquitecto de la nube

Recursos relacionados

- Perl
- Módulo Perl DBI
- Python
- psycopg2
- SQLAlchemy
- Copia masiva - PostgreSQL
- Copia masiva - Microsoft SQL Server
- PostgreSQL
- Uso de Amazon Aurora PostgreSQL

Información adicional

Tanto Microsoft SQL Server como Aurora PostgreSQL son compatibles con ANSI SQL. Sin embargo, debe tener en cuenta cualquier incompatibilidad en la sintaxis, los tipos de datos de columnas, las funciones nativas específicas de las bases de datos, las inserciones masivas y la distinción entre mayúsculas y minúsculas cuando migre su aplicación de Python o Perl de SQL Server a PostgreSQL.

Las siguientes secciones brindan más información sobre posibles inconsistencias.

Comparación de tipos de datos

Los cambios en el tipo de datos de SQL Server a PostgreSQL pueden provocar diferencias significativas en los datos resultantes en los que funcionan las aplicaciones. Para ver una comparación de los tipos de datos, consulte la tabla del sitio web de Sqlines.

Funciones SQL nativas o integradas

El comportamiento de algunas funciones difiere entre las bases de datos de SQL Server y PostgreSQL. La siguiente tabla muestra una comparación.

Microsoft SQL Server	Descripción	PostgreSQL
`CAST`	Convierte un valor de un tipo de datos a otro tipo.	PostgreSQL `type :: operator`

`GETDATE()`	Devuelve la fecha y la hora del sistema de base de datos actual, en un formato `YYYY-MM-DD hh:mm:ss.mmm` .	`CLOCK_TIMESTAMP`
`DATEADD`	Añade un intervalo de fecha y hora a una fecha.	`INTERVAL` expression
`CONVERT`	Convierte un valor en un formato de datos específico.	`TO_CHAR`
`DATEDIFF`	Devuelve la diferencia entre dos campos de fecha.	`DATE_PART`
`TOP`	Limita el número de filas de un conjunto de resultados de `SELECT`.	`LIMIT/FETCH`

Bloques anónimos

Una consulta SQL estructurada se organiza en secciones como la declaración, los ejecutables y el manejo de excepciones. En la siguiente tabla se comparan las versiones Microsoft SQL Server y PostgreSQL de un bloque anónimo simple. En el caso de bloques anónimos complejos, le recomendamos que llame una función de base de datos personalizada en su aplicación.

Microsoft SQL Server

```
my $sql_qry1=
my $sql_qry2 =
my $sqlqry = "BEGIN TRAN
$sql_qry1 $sql_qry2
if @\@error !=0 ROLLBACK
TRAN
else COMIT TRAN";
```

PostgreSQL

```
my $sql_qry1=
my $sql_qry2 =
my $sql_qry = " DO \$\$
BEGIN
$header_sql $content_sql
END
\$\$";
```

Otras diferencias

- Inserciones masivas de filas: el equivalente en PostgreSQL de la utilidad bcp de Microsoft SQL Server es COPY.
- Distinción entre mayúsculas y minúsculas: los nombres de las columnas distinguen entre mayúsculas y minúsculas en PostgreSQL, por lo que debe convertir los nombres de las columnas de SQL Server a minúsculas o mayúsculas. Esto se convierte en un factor al extraer o comparar datos, o al colocar los nombres de las columnas en los conjuntos de resultados o las variables. El siguiente ejemplo identifica las columnas en las que los valores se pueden almacenar en mayúsculas o minúsculas.

```
my $sql_qry = "SELECT $record_id FROM $exampleTable WHERE LOWER($record_name) =
 \'failed transaction\'";
```

- Concatenación: SQL Server usa + como operador para la concatenación de cadenas, mientras que PostgreSQL usa `||`.
- Validación: debe probar y validar las consultas y funciones de SQL en línea antes de usarlas en el código de la aplicación para PostgreSQL.
- Inclusión de la biblioteca ORM: también puede buscar incluir o reemplazar la biblioteca de conexiones de bases de datos existente con bibliotecas ORM de Python, como SQLAlchemy yPynomoDB. Esto ayudará a consultar y manipular fácilmente los datos de una base de datos utilizando un paradigma orientado a objetos.

Patrones de migración por carga de trabajo

Temas

IBM

- Migrar una base de datos de Db2 de Amazon EC2 a Aurora compatible con MySQL mediante AWS DMS
- Migre Db2 para LUW a Amazon EC2 mediante envío de registros para reducir el tiempo de interrupción
- Migración de Db2 para LUW a Amazon EC2 con recuperación de desastres de alta disponibilidad
- Migrar de IBM Db2 en Amazon EC2 a compatible con Aurora PostgreSQL mediante AWS DMS y AWS SCT
- Migre de IBM WebSphere Application Server a Apache Tomcat en Amazon EC2

Microsoft

- Acelere el descubrimiento y la migración de las cargas de trabajo de Microsoft a AWS
- Cambie las aplicaciones de Python y Perl para que admitan la migración de bases de datos de Microsoft SQL Server a una edición compatible con PostgreSQL de Amazon Aurora
- Cree CloudFormation plantillas de AWS para las tareas de AWS DMS con Microsoft Excel y Python
- Exportación de una base de datos de Microsoft SQL Server a Amazon S3 mediante AWS DMS
- Incorporar y migrar instancias de Windows de EC2 a una cuenta de AWS Managed Services
- Migración de una cola de mensajes de Microsoft Azure Service Bus a Amazon SQS
- Migración de una base de datos de Microsoft SQL Server de Amazon EC2 a Amazon DocumentDB mediante AWS DMS
- Migración de una base de datos de Microsoft SQL Server a Aurora MySQL mediante AWS DMS y AWS SCT
- Migración de una aplicación .NET de Microsoft Azure App Service a AWS Elastic Beanstalk
- Migración de una base de datos de Microsoft SQL Server en las instalaciones a Amazon EC2
- Migración de una base de datos de Microsoft SQL Server en las instalaciones a Amazon RDS para SQL Server
- Migración de bases de datos en las instalaciones de Microsoft SQL Server a Amazon RDS para SQL Server mediante servidores vinculados
- Migre una base de datos de Microsoft SQL Server en las instalaciones a Amazon RDS para SQL Server mediante métodos nativos de copia de seguridad y restauración
- Migre una base de datos de Microsoft SQL Server en las instalaciones a Amazon Redshift mediante AWS DMS
- Migre una base de datos en las instalaciones de Microsoft SQL Server a Amazon Redshift mediante agentes de extracción de datos de AWS SCT
- ???
- Migre datos de Microsoft Azure Blob a Amazon S3 mediante Rclone
- Migración de los certificados SSL de Windows a un equilibrador de carga de aplicación mediante ACM
- ???
- Configure una infraestructura Multi-AZ para una FCI Always On de SQL Server mediante Amazon FSx

N/A

- Crear un proceso de aprobación para las solicitudes de firewall durante una migración para volver a alojar a AWS

Código abierto

- Crear usuarios y roles de aplicaciones en Aurora compatible con PostgreSQL
- ???
- Migración de una base de datos MySQL en las instalaciones a Amazon EC2
- Migrar una base de datos MySQL en las instalaciones a Amazon RDS para MySQL
- Migrar de una base de datos de MySQL en las instalaciones a Aurora MySQL
- Migrar una base de datos PostgreSQL en las instalaciones a Aurora PostgreSQL
- Migre de IBM WebSphere Application Server a Apache Tomcat en Amazon EC2 con Auto Scaling
- Migre de Oracle GlassFish a AWS Elastic Beanstalk
- Migre de PostgreSQL en Amazon EC2 a Amazon RDS para PostgreSQL mediante pglogical
- Migración de aplicaciones Java locales en las instalaciones a AWS mediante AWS App2Container
- Migre bases de datos MySQL locales a Aurora MySQL mediante Percona, XtraBackup Amazon EFS y Amazon S3
- Migre tablas externas de Oracle a Amazon Aurora compatible con PostgreSQL
- Migración de las cargas de trabajo de Redis a Redis Enterprise Cloud en AWS
- Reinicie el agente de replicación de AWS automáticamente sin deshabilitar SELinux después de reiniciar un servidor fuente de RHEL
- Transportar bases de datos PostgreSQL entre dos instancias de base de datos de Amazon RDS utilizando pg_transport

Oracle

- Configurar enlaces entre la base de datos de Oracle y Aurora compatible con PostgreSQL
- Convierta el tipo de datos VARCHAR2 (1) para Oracle en un tipo de datos booleano para Amazon Aurora PostgreSQL
- Emule Oracle DR mediante una base de datos global de Aurora compatible con PostgreSQL
- Migre gradualmente de Amazon RDS para Oracle a Amazon RDS para PostgreSQL con Oracle SQL Developer y AWS SCT
- ???
- Migrar Amazon RDS para Oracle a Amazon RDS para PostgreSQL en modo SSL mediante AWS DMS
- Migre Amazon RDS para Oracle a Amazon RDS para PostgreSQL con AWS SCT y AWS DMS mediante AWS CLI y AWS CloudFormation
- ???
- Migre una instancia de base de datos de Amazon RDS para Oracle a otra VPC
- Migre una base de datos de Oracle en las instalaciones a Amazon EC2 mediante Oracle Data Pump
- Migre una base de datos Oracle local a Amazon OpenSearch Service mediante Logstash
- Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para MySQL con AWS DMS y AWS SCT
- Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle
- Migración de una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle mediante Oracle Data Pump
- Migrar una base de datos de Oracle en las instalaciones a Amazon RDS para Oracle mediante Oracle Data Pump
- Migre una base de datos Oracle en las instalaciones a Amazon RDS para PostgreSQL mediante Oracle Bystander y AWS DMS
- Migre una base de datos de Oracle en las instalaciones a Amazon EC2
- Migrar una base de datos Oracle de Amazon EC2 a Amazon RDS para MariaDB mediante AWS DMS y AWS SCT
- Migración de una base de datos de Oracle de Amazon EC2 a Amazon RDS para Oracle mediante AWS DMS
- Migrar una base de datos de Oracle a Amazon DynamoDB mediante AWS DMS

- Migre una base de datos Oracle a Amazon RDS for Oracle mediante adaptadores de archivos planos de GoldenGate Oracle
- Migración de una base de datos de Oracle a Amazon Redshift con AWS DMS y AWS SCT
- Migrar una base de datos de Oracle a Aurora PostgreSQL con AWS DMS y AWS SCT
- Migre una EnterpriseOne base de datos de Oracle JD Edwards a AWS mediante Oracle Data Pump y AWS DMS
- Migre una tabla particionada de Oracle a PostgreSQL mediante AWS DMS
- Migre una PeopleSoft base de datos de Oracle a AWS mediante AWS DMS
- Migre datos de una base de datos Oracle en las instalaciones a Aurora PostgreSQL
- Migrar de Amazon RDS para Oracle a Amazon RDS para MySQL
- Migre de Oracle 8i o 9i a Amazon RDS para PostgreSQL mediante la vista materializada y AWS DMS
- Migre de Oracle 8i o 9i a Amazon RDS para PostgreSQL mediante AWS DMS SharePlex
- Migre de Oracle Database a Amazon RDS for PostgreSQL mediante Oracle GoldenGate
- ???
- Migración de Oracle a Amazon DocumentDB con AWS DMS
- Migre de Oracle WebLogic a Apache Tomcat (ToMEE) en Amazon ECS
- Migre índices basados en funciones de Oracle a PostgreSQL
- Migre aplicaciones heredadas de Oracle Pro*C a ECPG
- Migre valores CLOB de Oracle a filas individuales en PostgreSQL en AWS
- Migre los códigos de error de Oracle Database a una base de datos Amazon Aurora compatible con PostgreSQL
- Migre Oracle E-Business Suite a Amazon RDS Custom
- Migrar las funciones nativas de Oracle a PostgreSQL mediante extensiones
- Migre Oracle PeopleSoft a Amazon RDS Custom
- Migre la funcionalidad ROWIdentificador de Oracle a PostgreSQL en AWS
- Migre los paquetes pragma SERIALLY_REUTILIZABLE de Oracle a PostgreSQL
- Migre columnas generadas de forma virtual de Oracle a PostgreSQL
- Configure la funcionalidad UTL_FILE de Oracle en Aurora compatible con PostgreSQL
- Validar los objetos de la base de datos después de migrar de Oracle a Amazon Aurora PostgreSQL

SAP

- Migración de una base de datos de SAP ASE en las instalaciones a Amazon EC2
- Migración de SAP ASE a Amazon RDS para SQL Server utilizando AWS DMS
- Migre SAP ASE de Amazon EC2 a Amazon Aurora compatible con PostgreSQL mediante AWS SCT y AWS DMS
- Reduzca el tiempo de transición de la migración homogénea de SAP mediante el servicio de migración de aplicaciones

Más patrones

- Evaluar la preparación de las aplicaciones para la migración a la nube de AWS mediante CAST Highlight
- Evaluar el rendimiento de las consultas para migrar bases de datos de SQL Server a MongoDB Atlas en AWS
- Automatice la conmutación por error y la conmutación por recuperación entre regiones mediante DR Orchestrator Framework
- Cree un visor de archivos de unidad central avanzada en la nube de AWS
- Configure una extensión de centro de datos para VMware Cloud en AWS mediante el modo Hybrid Linked Mode
- Conéctese a los planos de datos y control del Servicio de Migración de Aplicaciones a través de una red privada
- Almacenamiento en contenedores de las cargas de trabajo de mainframe que Blu Age ha modernizado
- Convertir consultas JSON de Oracle en SQL de bases de datos PostgreSQL
- Convierta la característica temporal NORMALIZE de Teradata en Amazon Redshift SQL
- Convierta la característica RESET WHEN de Teradata en Amazon Redshift SQL
- Copiar tablas de Amazon DynamoDB entre cuentas mediante AWS Backup
- Implementar un clúster de Cassandra en Amazon EC2 con IP estáticas privadas para evitar el reequilibrio
- Implemente aplicaciones de varias pilas mediante AWS CDK con TypeScript
- Emule cargas de trabajo de Oracle RAC mediante puntos de conexión personalizados en Aurora PostgreSQL
- Calcule el tamaño del motor de Amazon RDS para una base de datos de Oracle mediante informes de AWR
- Genere información de datos mediante AWS Mainframe Modernization y Amazon Q en QuickSight
- Gestionar bloques anónimos en instrucciones SQL dinámicas en Aurora PostgreSQL
- Gestionar las sobrecargadas funciones de Oracle en Aurora PostgreSQL
- Integre VMware vRealize Network Insight con VMware Cloud on AWS
- Migrar las instancias de base de datos de Amazon RDS para Oracle a otras cuentas que usen AMS

- Migre un clúster de Apache Kafka local a Amazon MSK mediante MirrorMaker
- Migre las cargas de trabajo de Apache Cassandra a Amazon Keyspaces con AWS Glue
- Migre de Oracle 8i o 9i a Amazon RDS para Oracle con AWS DMS SharePlex
- Migre los datos de Hadoop a Amazon S3 mediante WanDisco Migrator LiveData
- Migre funciones y procedimientos de Oracle con más de 100 argumentos a PostgreSQL
- Migrar las variables de enlace OUT de Oracle a una base de datos PostgreSQL
- Migración de los sistemas BYOL de RHEL a instancias con licencia incluida de AWS mediante AWS MGN
- ???
- Migrar SQL Server a AWS mediante grupos de disponibilidad distribuidos
- ???
- ???
- Modernice la administración de la producción de mainframe en AWS mediante OpenText Micro Focus Enterprise Server y LRS X PageCenter
- Modificar los encabezados HTTP al migrar de F5 a un equilibrador de carga de aplicación en AWS
- Resolver los errores de conexión después de migrar Microsoft SQL Server a la nube de AWS
- Envíe registros desde VMware Cloud on AWS a Splunk mediante VMware Aria Operations for Logs
- Configure la recuperación ante desastres para Oracle JD Edwards EnterpriseOne con AWS Elastic Disaster Recovery
- Simplifique la administración de certificados privados mediante AWS Private CA y AWS RAM
- Transfiera datos de Db2 z/OS a gran escala a Amazon S3 en archivos CSV

Modernización

Temas

Analizar y visualizar la arquitectura del software en CAST Imaging

Creado por Arpita Sinha (Cast Software) y James Hurrell (Cast Software)

Entorno: Producción	Tecnologías: Modernización	Carga de trabajo: todas las demás cargas de trabajo

Resumen

Este patrón muestra cómo se puede utilizar CAST Imaging para navegar visualmente por un sistema de software complejo y realizar un análisis preciso de la estructura del software. Esta manera de utilizar CAST Imaging ayuda a tomar decisiones más informadas sobre la arquitectura de la aplicación, especialmente con fines de modernización.

Para ver la arquitectura de una aplicación en CAST Imaging, primero debe incorporar el código fuente de la aplicación a través de la consola CAST. A continuación, la consola publica los datos de la aplicación en CAST Imaging, donde se puede visualizar la arquitectura de la aplicación y navegar por ella capa por capa.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- La Imagen de máquina de Amazon (AMI) para CAST Imaging
- Una instancia de Amazon Elastic Compute Cloud (Amazon EC2) que incluya lo siguiente (se recomienda una instancia de Amazon EC2 r5.xlarge optimizada para la memoria):
  - 4 vCPU
  - 32 GB de RAM
  - Volumen mínimo de 500 GB de unidad de estado sólido (SSD) (gp3) de uso general
- Claves de licencia de CAST Console y CAST Imaging (para obtener las claves de licencia necesarias, póngase en contacto con CAST en aws.contact-me@castsoftware.com)
- El código fuente completo de la aplicación que desea analizar en formato comprimido (.zip)
- Microsoft Edge, Mozilla Firefox o Google Chrome

Arquitectura

El diagrama siguiente muestra un ejemplo de flujo de trabajo para incorporar el código fuente de una aplicación a través de la consola CAST y, a continuación, visualizarlo en CAST Imaging:

En el diagrama, se muestra el siguiente flujo de trabajo:

1. CAST genera metadatos del código fuente de la aplicación mediante ingeniería inversa del código de front-end, middleware y back-end.
2. Los datos de la aplicación que genera CAST se importan automáticamente a CAST Imaging, donde se pueden visualizar y analizar.

A continuación, se muestra un resumen de cómo funciona este proceso:

Herramientas

- CAST Imaging es una aplicación basada en un navegador que facilita poder ver y navegar visualmente por un sistema de software, para tomar decisiones informadas sobre su arquitectura.
- CAST Console es una aplicación basada en un navegador que facilita poder configurar, ejecutar y gestionar los análisis de CAST AIP.

Nota: Las CAST Imaging y CAST Console se incluyen en la AMI de CAST Imaging.

Epics

Configurar el entorno de CAST Imaging

Tarea	Descripción	Habilidades requeridas
Ejecute la configuración inicial de CAST Console.	1. Abra su navegador web y conéctese a CAST Console; para ello ingrese la URL: http://localhost:8081	Arquitectos de software, desarrolladores y responsables técnicos

Tarea	Descripción	Habilidades requeridas
	2. Especifique la clave de licencia de CAST Console cuando se solicite. A continuación, elija Siguiente . 3. Revise los ajustes de configuración. Si no es necesario realizar ningún cambio, selecciona Save and Finish (Guardar y finalizar).	
Ejecute la configuración inicial de CAST Imaging.	1. Abra su navegador web y conéctese a CAST Imaging; para ello ingrese la URL: http://localhost:8083 2. Cuando se solicite, inicie sesión especificando admin tanto para el nombre de usuario como para la contraseña. 3. Especifique la clave de licencia de CAST Imaging cuando se solicite. A continuación, seleccione Update (Actualizar) para guardar la clave.	Arquitectos de software, desarrolladores y responsab les técnicos

Tarea	Descripción	Habilidades requeridas
Configure el servidor local CAST Extend.	(Opcional) De forma predeterminada, el servidor local CAST Extend está configurado para funcionar en modo fuera de línea. Si esto es aceptable, no se requiere ninguna configura ción adicional. Sin embargo, si prefiere configurar el servidor local CAST Extend en modo en línea o proxy con una conexión directa a CAST Extend, siga estos pasos. Nota: Para obtener las credenciales de CAST Extend, consulte la página de registro de CAST Extend. 1. Utilice el acceso directo del CAST Extend Admin Center (Centro de administr ación de CAST Extend) en el escritorio para cargar su navegador web y conectars e al servidor local de CAST Extend. 2. Elija la opción Online. 3. Especifique sus credencia les de CAST Extend (correo electrónico y contraseña) y seleccione Save (Guardar) para completar el proceso.	Arquitectos de software, desarrolladores y responsab les técnicos

Incorporar su aplicación a CAST Imaging

Tarea	Descripción	Habilidades requeridas
Prepare el código fuente para su aplicación.	Guarde el código fuente de la aplicación en un único archivo .zip comprimido.	Arquitectos de software, desarrolladores y responsables técnicos
Agregue su aplicación a CAST Console.	1. Abra su navegador web y conéctese a CAST Console; para ello ingrese la URL: http://localhost:8081 2. Cuando se solicite, inicie sesión especificando admin tanto para el nombre de usuario como para la contraseña. 3. Seleccione Add application (Agregar aplicación). A continuación, especifique el nombre de la aplicación y seleccione Add.	Arquitectos de software, desarrolladores y responsables técnicos
Abra el asistente de entrega de código fuente.	Busque la aplicación que creó en CAST Console. Después, seleccione Add version (Añadir versión).	Arquitectos de software, desarrolladores y responsables técnicos
Cargue el código fuente para su aplicación.	Realice una de las acciones siguientes: • Arrastre y suelte el archivo .zip que contiene el código fuente de la aplicación en el asistente de entrega de código fuente. – O bien –	Arquitectos de software, desarrolladores y responsables técnicos

Tarea	Descripción	Habilidades requeridas
	• Seleccione el icono de cargar en la nube. A continuación, abra el archivo .zip que contiene el código fuente de la aplicación.	
Inicie el proceso de análisis.	1. En el asistente de entrega, proporcione los detalles de la versión y especifique las opciones de configuración. Para obtener más información, consulte Standard onboarding for CAST Imaging (Incorporación estándar para CAST Imaging) en la documentación de CAST Imaging. 2. Asegúrese de que la opción Publish to CAST Imaging (Publicar en CAST Imaging) esté seleccionada. A continuación, seleccione Proceed (Continuar). Nota: Si selecciona Proceed, se inicia el proceso de análisis del código fuente. La ventana de progreso de CAST Console muestra cada paso del proceso de análisis y visualiza una notificación cuando se completa el análisis.	Arquitectos de software, desarrolladores y responsables técnicos

Verifique los resultados del análisis y los datos publicados en CAST Imaging

Tarea	Descripción	Habilidades requeridas
Compruebe el estado y los registros.	Una vez completadas todas las acciones de análisis, compruebe que aparezca un mensaje de éxito en la ventana de progreso. Nota: Puede comprobar los registros individuales de cada acción de análisis inmediata mente después de completar la. Para revisar los registros de una acción específica, seleccione View log (Ver registro) en la ventana Progress.	Arquitectos de software, desarrolladores y responsab les técnicos
Compruebe los detalles de la aplicación.	En el Application details panel (Panel de detalles de la aplicación), revise los detalles de los resultados del análisis. Asegúrese de analizar las tecnologías detectadas y la organización del código fuente.	Arquitectos de software, desarrolladores y responsab les técnicos
Verifique y acceda a CAST Imaging.	1. En el panel Application Management (Administ ración de la aplicació n) de CAST Console, compruebe que el estado de la versión de la aplicació n sea Imaging processed. Aparece un icono de CAST Imaging.	Arquitectos de software, desarrolladores y responsab les técnicos

Tarea	Descripción	Habilidades requeridas
	2. Seleccione el icono de CAST Imaging para navegar directamente a los datos de su aplicación en CAST Imaging. Nota: El estado Imaging processed significa que el código fuente se analizó y se cargó en su instancia de CAST Imaging.	

Comenzar a analizar la aplicación con CAST Imaging

Tarea	Descripción	Habilidades requeridas
Inicie sesión en CAST Imaging.	Abra CAST Imaging y especifique las credenciales de administrador predeterminadas (admin/admin). Aparecerán los datos de su aplicación.	Arquitectos de software, desarrolladores y responsables técnicos
Explore los datos de su aplicación en CAST Imaging.	Comience a ver la arquitectura de su software mediante las funciones de CAST Imaging. Para ver un tutorial rápido sobre cómo utilizar las funciones de CAST Imaging, seleccione el icono de ayuda para mostrar el asistente de CAST Imaging.	Arquitectos de software, desarrolladores y responsables técnicos

Tarea	Descripción	Habilidades requeridas
	Para obtener más información, consulte la guía del usuario CAST Imaging User Guide.	

Recursos relacionados

Documentación de CAST Console

- Login (Iniciar sesión)
- Configuring options via CAST Console (Configurar opciones a través de CAST Console)

Documentación de CAST Imaging

- Application onboarding for CAST Imaging - prerequisites (Incorporar la aplicación CAST Imaging: requisitos previos)
- Cómo añadir una nueva aplicación para CAST Imaging
- Standard onboarding for CAST Imaging – check results (Incorporación estándar de CAST Imaging: comprobar los resultados)
- Login (Iniciar sesión)
- Configuration options – Admin Center GUI (Opciones de configuración: GUI del Centro de administración)

Más recursos sobre CAST Imaging en AWS

- Modernización de aplicaciones a AWS acelerada por CAST: técnica (PartnerCast seminario web sobre AWS, requiere una cuenta gratuita)
- Using CAST and AWS Migration Hub Refactor Spaces to Modernize Legacy Applications (Usar CAST y AWS Migration Hub Refactor Spaces para modernizar las aplicaciones antiguas) (entrada de blog de AWS)
- Modernize Applications to AWS Architectures with CAST Imaging (Modernizar las aplicaciones para las arquitecturas de AWS mediante CAST Imaging) (taller de AWS)
- AWS Marketplace: CAST Imaging
- Todos los recursos de CAST en AWS

Evaluar la preparación de las aplicaciones para la migración a la nube de AWS mediante CAST Highlight

Documento creado por Greg Rivera (Cast Software)

Entorno: Producción	Origen: Código fuente heredado de una aplicación	Destino: Código de aplicación refactorizado en AWS
Tipo R: renovar arquitectura	Carga de trabajo: IBM; Microsoft; código abierto; Oracle	Tecnologías: Modernización; migración; contenedores y microservicios
Servicios de AWS: Amazon RDS; Amazon S3		

Resumen

CAST Highlight es una solución de software como servicio (SaaS) para analizar rápidamente el catálogo de aplicaciones. Este patrón muestra cómo configurar y utilizar CAST Highlight para evaluar si las aplicaciones de software personalizadas del catálogo de TI de una organización están preparadas para la nube y planificar la modernización o la migración a la nube de Amazon Web Services (AWS).

CAST Highlight genera información acerca de lo preparada que está una aplicación para la nube, identifica los bloqueadores de código que deben eliminarse antes de la migración, estima el esfuerzo necesario para eliminarlos y recomienda qué servicios de AWS podrían usar las aplicaciones individuales después de la migración.

Este patrón describe el procedimiento de configuración y uso de CAST Highlight, que consta de cinco pasos: configuración de nuevos usuarios, administración de aplicaciones, administración de campañas, análisis del código fuente y análisis de los resultados. Es necesario completar todos los pasos de la sección Epics de este patrón para garantizar la revisión y el análisis correctos de las aplicaciones.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta CAST Highlight activa con permisos de Portfolio Manager (Administrador de portfolio).
- Al menos 300 MB de espacio libre en disco y 4 GB de memoria en su ordenador local para instalar el agente local CAST Highlight.
- Microsoft Windows 8 o posterior.
- El código fuente de la aplicación debe almacenarse en archivos de texto a los que se pueda acceder desde la máquina en la que está instalado el agente local. Ningún código fuente sale de las instalaciones y todo el código se escanea localmente.

Arquitectura

El diagrama siguiente ilustra el flujo de trabajo para utilizar CAST Highlight.

El flujo de trabajo consta de los pasos siguientes:

1. Inicie sesión en el portal CAST Highlight, descargue el agente local e instálelo en su ordenador local. Amazon Simple Storage Service (Amazon S3) almacena el paquete de instalación del agente local.
2. Escanee los archivos del código fuente y cree un archivo de resultados.
3. Cargue el archivo de resultados en el portal CAST Highlight. Importante: No se incluye ningún código fuente en el archivo de resultados.
4. Responda a las preguntas de la encuesta para cada aplicación escaneada.
5. Vea los paneles e informes disponibles en el portal CAST Highlight. Amazon Relational Database Service (Amazon RDS) almacena el código escaneado, los resultados del análisis y los datos del software CAST Highlight.

Pila de tecnología

CAST Highlight admite las siguientes tecnologías para analizar si las aplicaciones están preparadas para la nube:

- Java
- COBOL
- C#

- C++
- Clojure
- PHP
- JavaScript
- TypeScript
- Python
- Microsoft Transact-SQL
- VB.Net
- Kotlin
- Scala
- Swift

Automatizar y escalar

- Se puede utilizar un analizador CLI analyzer para automatizar el proceso de análisis de CAST Highlight.

Herramientas

No se necesitan herramientas para este patrón si se cumplen todos los requisitos previos. Sin embargo, puede utilizar herramientas opcionales, como utilidades de administración de código fuente (SCM), extractores de código u otras herramientas, para administrar sus archivos de código fuente.

Epics

Configurar nuevo usuario

Tarea	Descripción	Habilidades requeridas
Active su cuenta CAST Highlight y cree una contraseña.	Todos los usuarios nuevos de CAST Highlight reciben un correo electrónico de activación de la cuenta. Siga el enlace de activación para activar su cuenta CAST Highlight	N/A

Tarea	Descripción	Habilidades requeridas
	y escriba una contraseña para completar el proceso de activación.	
Inicie sesión en el portal CAST Highlight.	Después de especificar la nueva contraseña, se muestra la página de inicio de CAST Highlight. Inicie sesión en el portal CAST Highlight con sus credenciales de usuario.	N/A

Application Management (Administración de aplicaciones)

Tarea	Descripción	Habilidades requeridas
Cree un registro de aplicaciones.	En el portal CAST Highlight , vaya a la pestaña Manage Application (Administrar aplicación) en la sección Manage Portfolio (Administrar portfolio). En el mosaico Applications (Aplicaciones) de la parte superior de la pantalla, seleccione Add (Agregar).	N/A
Seleccione el nombre de una aplicación.	Escriba un nombre para la aplicación y seleccione Save (Guardar). Este nombre se utiliza para el registro de su aplicación en CAST Highlight.	N/A
Repita los pasos para todas las aplicaciones.	Repita estos pasos para cada aplicación que desee escanear.	N/A

Administración de campañas

Tarea	Descripción	Habilidades requeridas
Cree una campaña.	CAST Highlight utiliza el término «campaña» para describir un conjunto de aplicaciones que se analizará n en un momento específico. En el portal CAST Highlight , vaya a la pestaña Manage Campaigns (Administrar campañas) en la sección Manage Portfolio (Administrar portfolio). Seleccione Create Campaign (Crear campaña) para abrir la pantalla de creación de campañas.	N/A
Escriba un nombre y seleccion e una fecha de cierre para la campaña.	Escriba un nombre para su campaña y seleccione una fecha de cierre. Importante: Los colaboradores no pueden enviar los resultado s del análisis de las aplicacio nes después de la fecha de cierre de la campaña.	N/A
Decida incluir el escaneo del código fuente, las respuesta s a las encuestas y el alcance del dominio y de la aplicación.	Seleccione una o más de las encuestas estándar utilizada s para mejorar los datos de análisis del código fuente con información cualitativa. Las categorías de la encuesta son Impacto empresarial, Esfuerzo de mantenimiento del software CloudReady, Propiedades de	N/A

Tarea	Descripción	Habilidades requeridas
	las aplicaciones e Impacto ecológico. Seleccione el dominio y las aplicaciones que se analizarán durante la campaña. Importante: Asegúrese de añadir todas las aplicacio nes que quiera escanear en la sección Manage Applicati ons (Gestión de aplicacio nes) antes de empezar la campaña.	
Personalizar el mensaje de lanzamiento.	Personalice el mensaje de lanzamiento que se enviará por correo electrónico a todos los colaboradores asociados a las aplicaciones de la campaña.	N/A
Lanzar la campaña.	Seleccione Complete (Completar) para lanzar la campaña.	N/A

Análisis del código fuente

Tarea	Descripción	Habilidades requeridas
Descargue el agente local de CAST Highlight.	En el portal CAST Highlight, seleccione Application Scans (Escaneos de aplicaciones) y descargue el agente local en su ordenador local.	N/A

Tarea	Descripción	Habilidades requeridas
Instalar el agente local.	Inicie el programa de instalación HighlightSetup CAST.exe y siga las instrucciones de configuración que aparecen. Una vez instalado el agente local, estará todo listo para analizar las aplicaciones.	N/A
Defina el alcance del escaneo del código del agente local.	El análisis del código se realiza en el nivel de archivos y no tiene en cuenta los vínculos lógicos ni las dependencias entre archivos. Todos los archivos se consideran iguales y forman parte de la aplicación. Para obtener resultados precisos y uniformes, defina el alcance de escaneado del código mediante las características de exclusión de archivos o carpetas disponibles en el agente local.	N/A

Tarea	Descripción	Habilidades requeridas
Incluir paquetes de código abierto o COTS.	(Opcional) Si desea incluir paquetes de código abierto o comerciales off-the-shelf (COTS), asegúrese de que estén incluidos en las carpetas que planea escanear. Por lo general, las bibliotecas externas se agrupan en una subcarpeta denominada «de terceros» o similar, y el código principal suele encontrarse en la carpeta de archivos «src/main».	N/A
Excluir las clases de prueba.	Las clases de prueba suelen excluirse del análisis del código fuente porque, por lo general, no forman parte de la aplicación compilada. Sin embargo, puede optar por incluirlas en el escaneo si es necesario.	N/A
Excluir las carpetas de SCM, compilación e implementación.	Para obtener resultados más coherentes, evite incluir carpetas de SCM, compilación o implementación (por ejemplo, archivos .git o .svn) en el escaneo.	N/A

Tarea	Descripción	Habilidades requeridas
Incluir los archivos de dependencias.	Si desea obtener información sobre las estructuras y las dependencias cuyos archivos físicos no forman parte de la carpeta que está escaneando, asegúrese de incluir los archivos de dependencias (como los archivos pom.xml, build.gradle, package.json o .vcsproj).	N/A
Invocar el agente local.	Ejecute el agente local en su máquina Windows local.	N/A
Seleccione la carpeta que contiene el código fuente.	Seleccione la carpeta que contiene el código fuente. Puede añadir varias carpetas para la detección del agente local. Si bien el agente local admite la detección de código fuente a través de rutas de red, debe asegurarse de que las carpetas estén ubicadas en su máquina local. Importante: Se recomienda realizar varios escaneos si hay más de 10 000 archivos en las carpetas de origen.	N/A

Tarea	Descripción	Habilidades requeridas
Iniciar la detección de archivos.	En el panel de control del agente local, seleccione Discover Files (Detectar archivos). El agente local detecta los archivos de sus carpetas y subcarpetas, así como sus tecnologías. Puede pulsar el botón Cancel para cancelar la detección en cualquier momento. Una vez finalizada la detección de archivos, el agente local muestra una lista de las carpetas y los archivos encontrados. La columna Technologies muestra las tecnologías asociadas y el recuento de archivos. La columna Path (Ruta) muestra la ubicación de las carpetas y los archivos.	N/A

Tarea	Descripción	Habilidades requeridas
Ajustar la configuración de escaneo del código fuente.	(Opcional) Para ajustar el escaneo del agente local, puede desactivar una o varias tecnologías para una carpeta o un archivo específicos. Si todas las tecnologías están desactivadas, la carpeta o el archivo se excluirán del análisis. Para desactivar las tecnologí as, seleccione la etiqueta amarilla de la tecnología que desee desactivar. También puede elegir el icono del filtro al pasar el ratón sobre un archivo o una carpeta para asociar una tecnología a un archivo o carpeta específic os. Estos ajustes se guardan y aceleran el proceso de detección de la carpeta o del archivo.	N/A
Iniciar el escaneo de código fuente.	Después de configurar el escaneo, seleccione «Scan Files» (Escanear archivos) para comenzar el proceso de escaneo.	N/A

Tarea	Descripción	Habilidades requeridas
Compruebe si hay etiquetas verdes o grises.	Una vez finalizado el escaneo del código fuente, se muestra una etiqueta de estado en los niveles de carpetas y de archivos. Una etiqueta verde significa que los archivos se escanearon correctamente con la tecnología asociada. Una etiqueta gris significa que los archivos no se escanearon y se han excluido. El motivo de su exclusión se muestra al pasar el ratón sobre la etiqueta de cada archivo. Algunos motivos posibles de exclusión de archivos son: archivos binarios, archivos ilegibles, archivos que no están, biblioteca externa, archivos codificados, archivos generados, errores de sintaxis, contenido que no está en el idioma esperado, código que no cumple con suficientes criterios de análisis, archivos que superan el límite de tamaño (10 MB), problemas de tiempo de espera o falta de disponibilidad del analizador.	N/A

Tarea	Descripción	Habilidades requeridas
Modificar la configuración de escaneo y volver a escanear el código.	(Opcional) Puede modificar los ajustes de la configura ción de escaneo y elegir Scan Files (Escanear archivos) para volver a escanear los archivos.	N/A
Confirmar los resultados del escaneo.	Seleccione Confirm Results (Confirmar resultados) si los resultados del escaneo cumplen sus requisitos.	N/A
Vea las estructuras y las bibliotecas de software que ha encontrado el agente local.	Vea las estructuras y las bibliotecas de software utilizadas o a las que hacen referencia las aplicaciones y que el agente local detectó durante el escaneo del código. Para conservar o ignorar los elementos de estas listas, active o desactive el botón individual. Seleccione Confirm dependencies (Confirmar dependencias) para continuar. Importante: Si una estructura está desactivada, no aparece en el portal CAST Highlight ni se vincula a su aplicación.	N/A

Tarea	Descripción	Habilidades requeridas
Guardar los resultados de escanear el código.	El agente local muestra un resumen de los resultado s de escanear el código, agrupados por tecnologí a. Elija Save (Guardar) y especifique la carpeta en la que desea guardar los resultados. El agente local genera un archivo .zip por escaneo, que contiene todos los resultados del análisis. En función del número de tecnologías distintas y de las carpetas fuente raíz, el agente local genera automáticamente uno o varios archivos.csv con la estructura de nombres FolderName.Technology.Date. csv.	N/A
Cargar el archivo de resultado s de escanear el código en el portal CAST Highlight.	En el portal CAST Highlight , seleccione las aplicacio nes que analizó en la sección Application Scans (Escaneos de aplicaciones). Seleccione Upload Results (Cargar resultados) y elija los archivos .csv. También puede cargar los archivos .csv de forma individual. Después de cargar cada archivo, aparecerá un registro de la carga en la pantalla.	N/A

Tarea	Descripción	Habilidades requeridas
Eliminar archivos de resultados del análisis, si es necesario.	(Opcional) Para eliminar un archivo de resultados de análisis en cualquier momento del proceso de carga, seleccione el icono de la papelera. Importante: Solo los usuarios con privilegios de administrador de portfolio o el colaborador que cargó los resultados pueden eliminarlos.	N/A
Responder a la encuesta sobre la aplicación.	En las aplicaciones para las que se requiere una encuesta aparece el botón Survey (Encuesta). Seleccione Survey (Encuesta), responda a las preguntas de cada sección de la encuesta y pulse Submit (Enviar) cuando termine. El progreso de la encuesta se muestra en la parte superior de la pantalla. Puede enviar los resultados después de enviar toda la información obligatoria. Sin embargo, para mejorar los datos de la instancia CAST Highlight de su organización responda a todas las preguntas.	N/A

Tarea	Descripción	Habilidades requeridas
Enviar los resultados de escanear el código.	Después de cargar todos los archivos de resultados en formato .csv de la aplicación y responder a las preguntas de la encuesta, seleccione Submit (Enviar) en la sección Application Scans (Escaneos de aplicaciones). Este paso es necesario para completar el proceso y garantizar que los resultados estén disponibles en el portal CAST Highlight.	N/A

Análisis de los resultados

Tarea	Descripción	Habilidades requeridas
Ver la página de inicio del portal CAST Highlight.	La página de inicio del portal CAST Highlight incluye mosaicos con información de alto nivel sobre su cartera de aplicaciones, como el estado del software y las puntuacio nes de seguridad del código abierto para toda su cartera. CloudReady La página de inicio también incluye el número de aplicaciones incorporadas. Para obtener más información sobre las definiciones de métricas y la metodología de medición de CAST Highlight, consulte CAST Highlight: métricas y	N/A

Tarea	Descripción	Habilidades requeridas
	metodología (PowerPoint presentación de Microsoft).	
Vea el CloudReady panel de control.	Elija el CloudReady mosaico para abrir el CloudRead y tablero. Este es el panel principal en el nivel del portfolio para evaluar si las aplicaciones están preparada s para la nube. Le ayuda a planificar y desarrollar una hoja de ruta del portfolio para migración a la nube	N/A

Tarea	Descripción	Habilidades requeridas
Ver el panel de control de Portfolio Advisor for Cloud.	El panel de control de Portfolio Advisor for Cloud segmenta automáticamente las aplicaciones en las categorías de migración recomendadas. La segmentación se basa en las características técnicas de cada aplicación. Los factores incluyen el análisis del código fuente (preparación para la nube, la resiliencia del software, etc.) y el impacto empresarial, que se desprende de la encuesta. En la esquina superior derecha, seleccione Compute (Computar) para generar las recomendaciones de segmentación iniciales. Las burbujas de los gráficos de la parte superior del panel representan cada aplicación del catálogo, organizadas según la segmentación recomendada. Cada aplicación también aparece en una tabla de datos situada debajo de los gráficos, que incluye las métricas pertinentes de cada aplicación. Los posibles segmentos que se recomiendan incluyen:	N/A

Tarea	Descripción	Habilidades requeridas
	• Rehost (Volver a alojar): se recomienda cambiar la configuración de la infraestructura de la aplicación y migrar mediante lift-and-shift a la nube mediante una solución de infraestructura como servicio (IaaS). • Refactor (Refactorizar): se recomienda realizar modificaciones menores en el código de la aplicación sin cambiar la arquitectura ni la funcionalidad, de modo que se pueda migrar mediante una solución de contenedor como servicio (CaaS) o plataforma como servicio (PaaS). • Rearchitect (Rediseñar): se recomienda modificar drásticamente el código de la aplicación con el fin de mejorar el estado de la aplicación y prepararla para la migración mediante una solución PaaS o implementarla como una aplicación sin servidor mediante una solución de función como servicio (FaaS). • Rebuild (Reconstruir): se recomienda descartar el código de la aplicación y	

Tarea	Descripción	Habilidades requeridas
	volver a desarrollarla en la nube mediante una solución PaaS o volver a desarroll arla como una aplicación sin servidor mediante una solución FaaS. • Retire (Retirar): se recomienda descartar la aplicación por completo o, posiblemente, sustituirla por una alternativa comercial de software como servicio (SaaS).	
Modificar las recomenda ciones de segmentación.	En algunos casos, puede optar por cambiar el segmento recomendado por CAST Highlight. Para ello, vaya a la aplicación en la tabla de datos y seleccione un segmento diferente de la lista desplegab le situada junto al nombre de la aplicación. Seleccione Save (Guardar) en la esquina superior derecha para guardar los cambios. También puede exportar estos datos en cualquier momento. Para ello, seleccione Export (Exportar) en la esquina superior derecha.	N/A

Tarea	Descripción	Habilidades requeridas
Elegir una aplicación para analizarla.	En el panel de control de Portfolio Advisor for Cloud, elija la burbuja de una aplicación para analizarl a. Seleccione el nombre de la aplicación en la tabla situada después del gráfico de burbujas para iniciar un análisis más profundo. Están disponibles diferente s paneles para analizar aplicaciones individuales, como Code Insights (Informac ión del código) (patrones de salud del software), Trends (Tendencias) y Software Composition (Composición del software) (riesgos del código abierto).	N/A

Tarea	Descripción	Habilidades requeridas
Analice los CloudReady resultados de una aplicación individual.	Seleccione la CloudRead ypestaña, que muestra la CloudReady puntuación general de la aplicación. Esta puntuación es un promedio ponderado basado en una combinación de las respuesta s de la CloudReady encuesta y el escaneo del CloudReady código. Las respuestas a las preguntas de la encuesta se muestran en la tabla situada debajo de los mosaicos. Selecciona CloudReady Code Scan para ver los resultado s del escaneo de código. Hay una lista de CloudRead y patrones para los que se escaneó el código de la aplicación. La lista incluye las columnas siguientes: • Cloud Requirement (requisit o de la nube) es el patrón de código específico. • Technology (tecnolog ía) es el lenguaje de programación del patrón. «Impact» (impacto) es el impacto del patrón en la aplicación (C = código, F = estructura, A = arquitect ura).	N/A

Tarea	Descripción	Habilidades requeridas
	• Criticality (criticidad) es el nivel de importancia que tiene abordar este patrón antes de migrar. • La contribución es la forma en que este patrón contribuye a la CloudRead y puntuación general. Si el patrón es verde, es un refuerzo y aumenta la CloudReady puntuación. Si el patrón es rojo, es un bloqueador y reduce la CloudReady puntuación. Si el patrón no tiene color, es un bloqueador que no se detectó y aumenta la CloudReady puntuación. • Roadblocks (obstáculos) son el número de aparicion es individuales de un patrón bloqueador. Seleccione el número de obstáculos para mostrar una lista de los archivos de código fuente en los que se detectó el patrón. • Est. Effort (Esfuerzo estimado) es una estimació n del número de días que se necesitarán para eliminar los obstáculos de cada fila.	

Tarea	Descripción	Habilidades requeridas
Exportar los datos a Microsoft Excel.	(Opcional) Seleccione Export to Excel para exportar los datos para su posterior análisis. Los datos de los resultados del análisis de la aplicación se pueden utilizar para analizar con más detalle si una aplicació n está preparada para la nube y determinar qué código debe actualizarse antes de la migración.	N/A
Ver recomendaciones.	Selecciona Recomendaciones junto a CloudReady Code Scan para ver la pantalla de recomendaciones de servicios en la nube. Esto identifica los servicios de AWS que la aplicación podría adoptar en función de sus características. Repita este paso para ver recomendaciones para todas las aplicaciones que analizó.	N/A

Recursos relacionados

Administración de campañas

- Formación para certificación básica de CAST Highlight - Sección 3: Configuración de portfolio (vídeo)

Análisis del código fuente

- Formación para certificación básica de CAST Highlight - Sección 4: Análisis de aplicaciones (vídeo)

Otros recursos

- CAST Highlight en AWS Marketplace
- AWS y CAST: Acelere la modernización de las aplicaciones
- CAST Highlight: Documentación, tutoriales de productos y herramientas de terceros
- CAST Highlight: Demostración sobre preparación de un producto para la nube (vídeo)
- Modernización de la cartera de aplicaciones con CAST Highlight (seminario de AWS)

Archivar automáticamente los elementos en Amazon S3 con DynamoDB TTL

Creado por Tabby Ward (AWS)

Repositorio de código: archiva elementos en S3 mediante DynamoDB TLL	Entorno: PoC o piloto	Tecnologías: Modernización; bases de datos; modelo sin servidor; almacenamiento y copia de seguridad; administración de costos
Carga de trabajo: código abierto	Servicios de AWS: Amazon S3; Amazon DynamoDB; Amazon Kinesis; AWS Lambda	

Resumen

Este patrón proporciona los pasos para eliminar datos antiguos de una tabla de Amazon DynamoDB y archivarlos en un bucket de Amazon Simple Storage Service (Amazon S3) en Amazon Web Services (AWS) sin tener que gestionar una flota de servidores.

Este patrón utiliza el Tiempo de vida (TTL) de Amazon DynamoDB para eliminar automáticamente los elementos antiguos y Amazon DynamoDB Streams para capturar los elementos de TTL que han vencido. A continuación, conecta DynamoDB Streams a AWS Lambda, que ejecuta el código sin aprovisionar ni administrar ningún servidor.

Cuando se añaden nuevos elementos a la transmisión de DynamoDB, se inicia la función Lambda y escribe los datos en una transmisión de entrega de Amazon Data Firehose. Firehose proporciona una solución sencilla y totalmente gestionada para cargar los datos como un archivo en Amazon S3.

DynamoDB se utiliza a menudo para almacenar datos de serie temporal, como datos de secuencias de clics de páginas web o datos de Internet de las cosas (IoT) procedentes de sensores y dispositivos conectados. En lugar de eliminar los elementos a los que se accede con menos frecuencia, muchos clientes prefieren archivarlos con fines de auditoría. TTL simplifica este

archivado, ya que elimina automáticamente los elementos en función del atributo de marca de tiempo.

Los elementos que TTL ha eliminado pueden identificarse en DynamoDB Streams, que captura una secuencia en orden cronológico de las modificaciones de los elementos y almacena la secuencia en un registro durante 24 horas como máximo. Una función de Lambda puede consumir estos datos y archivarlos en un bucket de Amazon S3 para reducir el costo de almacenamiento. Para reducir aun más los costos, se pueden crear Reglas del ciclo de vida de Amazon S3 para realizar la transición automática de los datos (tan pronto como se creen) a las clases de almacenamiento de menor costo, como S3 Glacier Instant Retrieval o S3 Glacier Flexible Retrieval, o Amazon S3 Glacier Deep Archive para el almacenamiento a largo plazo.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Interfaz de la línea de comandos de AWS (AWS CLI) 1.7 o posterior, instalada y configurada en macOS, Linux o Windows.
- Python 3.7 o versiones posteriores.
- Boto3, instalado y configurado. Si Boto3 no está instalado, ejecute el comando `python -m pip install boto3` para instalarlo.

Arquitectura

Pila de tecnología

- Amazon DynamoDB
- Amazon DynamoDB Streams
- Amazon Data Firehose
- AWS Lambda
- Amazon S3

1. TTL elimina los elementos.

2. El activador de flujos de DynamoDB invoca la función de procesador de flujos Lambda.
3. La función Lambda coloca los registros en el flujo de entrega de Firehose en formato de lote.
4. Los registros de datos se archivan en el bucket de S3.

Herramientas

- AWS CLI: la interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta unificada para administrar los servicios de AWS.
- Amazon DynamoDB: Amazon DynamoDB es una base de datos de documentos y valores clave que ofrece un rendimiento de milisegundos de un solo dígito a cualquier escala.
- Tiempo de vida (TTL) de Amazon DynamoDB: TTL de Amazon DynamoDB le permite definir una marca temporal por elemento para determinar cuándo ya no se necesita un elemento.
- Amazon DynamoDB Streams: Amazon DynamoDB Streams captura una secuencia en orden cronológico de las modificaciones de los elementos en una tabla de DynamoDB y almacena esta información en un registro durante 24 horas como máximo.
- Amazon Data Firehose: Amazon Data Firehose es la forma más sencilla de cargar de forma fiable datos de streaming en lagos de datos, almacenes de datos y servicios de análisis.
- AWS Lambda: AWS Lambda ejecuta código sin necesidad de aprovisionar ni administrar servidores. Solo paga por el tiempo de computación que consume.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos que ofrece escalabilidad, disponibilidad de datos, seguridad y rendimiento líderes del sector.

Código

El código de este patrón está disponible en los elementos de GitHub Archivar en S3 mediante el repositorio TTL de DynamoDB.

Epics

Configurar una tabla de DynamoDB, un TTL y una transmisión de DynamoDB

Tarea	Descripción	Habilidades requeridas
Crear una tabla de DynamoDB.	Utilice la CLI de AWS para crear una tabla en DynamoDB llamada `Reservation` . Seleccione una unidad de capacidad de lectura (RCU) y una unidad de capacidad de escritura (WCU) al azar, y asigne a su tabla dos atributos: `ReservationID` y `ReservationDate` . `aws dynamodb create-table \` `--table-name Reservation \` `--attribute-definitions AttributeName=ReservationID,AttributeType=S AttributeName=ReservationDate,AttributeType=N \` `--key-schema AttributeName=ReservationID,KeyType=HASH AttributeName=ReservationDate,KeyType=RANGE \` `--provisioned-throughput ReadCapacityUnits=100,WriteCapacityUnits=100`	Arquitecto de la nube, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`ReservationDate` es una marca de tiempo epoch que se utilizará para activar el TTL.	
Active el TTL de DynamoDB.	Utilice la CLI de AWS para activar el TTL de DynamoDB para el atributo `ReservationDate` . `aws dynamodb update-time-to-live \` `--table-name Reservation\` `  --time-to-live-specification Enabled=true,AttributeName=ReservationDate`	Arquitecto de la nube, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Active un flujo de DynamoDB.	Utilice la CLI de AWS para activar un flujo de DynamoDB para la tabla `Reservation` mediante el tipo de flujo `NEW_AND_OLD_IMAGES`. `aws dynamodb update-table \` `--table-name Reservation \` `  --stream-specification StreamEnabled=true,StreamViewType=NEW_AND_OLD_IMAGES` Este flujo contendrá registros de los elementos nuevos, los elementos actualizados, los elementos eliminados y los elementos eliminados por TTL. Los registros de los elementos que se eliminan mediante TTL incluyen un atributo de metadatos adicional para distinguirlos de los elementos que se eliminaron manualmente. El campo `userIdentity` para eliminaciones de TTL indica que el servicio DynamoDB realizó la acción de eliminación. En este patrón, solo se archivan los elementos	Arquitecto de la nube, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	eliminados por TTL, pero solo puede archivar los registros donde `eventName` sea `REMOVE` y `userIdentity` incluya `principalId` igual a `dynamodb.amazonaws.com`.	

Crear y configurar un bucket de S3

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3.	Utilice la CLI de AWS para crear un bucket de S3 de destino en su región de AWS y sustituya `us-east-1` por su región. `aws s3api create-bucket \ --bucket reservationfirehosedestinationbucket \ --region us-east-1` Asegúrese de que el nombre del bucket de S3 sea único a nivel mundial, ya que todas las cuentas de AWS comparten el espacio de nombres.	Arquitecto de la nube, desarrollador de aplicaciones
Cree una política de ciclo de vida de 30 días para el bucket de S3.	1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3.	Arquitecto de la nube, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	2. Elige el depósito S3 que contiene los datos de Firehose. 3. En el bucket de S3, seleccione la pestaña Administración y, luego,Agregar regla de ciclo de vida. 4. Escriba un nombre para la regla en el cuadro de diálogo Regla de ciclo de vida y configure una regla del ciclo de vida de 30 días para su bucket.	

Crea un flujo de entrega de Firehose

Tarea	Descripción	Habilidades requeridas
Cree y configure un flujo de entrega de Firehose.	Descarga y edita el ejemplo de `CreateFireHoseToS3.py` código del GitHub repositorio. Este código está escrito en Python y muestra cómo crear una transmisión de entrega de Firehose y un rol de AWS Identity and Access Management (IAM). El rol de IAM tendrá una política que Firehose podrá usar para escribir en el bucket S3 de destino.	Arquitecto de la nube, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	Para ejecutar el script, utilice los siguientes comandos y argumentos de línea de comando: Argumento 1 = <Your_S3_bucket_ARN> , que es el nombre de recurso de Amazon (ARN) del bucket que creó con anterioridad. Argumento 2= Tu nombre de Firehose (lo está firehose_to_s3_stream usando este piloto) Argumento 3 = su nombre de rol de IAM (Este piloto utiliza firehose_to_s3). `python CreateFirehoseToS3.py <Your_S3_Bucket_ARN> firehose_to_s3_stream firehose_to_s3` Si el rol de IAM especificado no existe, el script creará un rol de asunción con una política de relaciones de confianza, así como una política que conceda suficientes permisos de Amazon S3. Para ver ejemplos de estas políticas, consulte la sección Información adicional.	

Tarea	Descripción	Habilidades requeridas
Verifica el flujo de entrega de Firehose.	Describa la transmisión de entrega de Firehose mediante la AWS CLI para comprobar que la transmisión de entrega se creó correctamente. `aws firehose describe-delivery-stream --delivery-stream-name firehose_to_s3_stream`	Arquitecto de la nube, desarrollador de aplicaciones

Cree una función Lambda para procesar el flujo de entrega de Firehose

Tarea	Descripción	Habilidades requeridas
Cree una política de confianza para la función de Lambda.	Cree un archivo de política de confianza con la siguiente información. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "lambda.amazonaws.com" }, "Action": "sts:AssumeRole" } ]`	Arquitecto de la nube, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	} Esto le concederá a su función permiso para acceder a los recursos de AWS.	
Cree un rol de ejecución para la función de Lambda.	Para crear el rol de ejecución, ejecute el siguiente código. `aws iam create-role --role-name lambda-ex --assume-role-policy-document file://TrustPolicy.json`	Arquitecto de la nube, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Agregue permisos al rol.	Para agregar permisos al rol, use el comando `attach-policy-to-role` . `aws iam attach-role-policy --role-name lambda-ex --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole` `aws iam attach-role-policy --role-name lambda-ex --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaDynamoDBExecutionRole` `aws iam attach-role-policy --role-name lambda-ex --policy-arn arn:aws:iam::aws:policy/AmazonKinesisFirehoseFullAccess` `aws iam attach-role-policy --role-name lambda-ex --policy-arn arn:aws:iam::aws:policy/IAMFullAccess`	Arquitecto de la nube, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Creación de una función de Lambda.	Ejecute el siguiente comando para comprimir el archivo `LambdaStreamProcessor.py` del repositorio de código. `zip function.zip LambdaStreamProcessor.py` Cuando cree la función de Lambda, necesitará el ARN del rol de ejecución de Lambda. Para obtener el ARN, ejecute el siguiente código. `aws iam get-role \ --role-name lambda-ex` Para crear la función de Lambda, ejecute el siguiente código. `aws lambda create-function --function-name LambdaStreamProcessor \ --zip-file fileb://function.zip --handler LambdaStreamProcessor.handler --runtime python3.8 \ --role {Your Lamda Execution Role ARN}\ --environment Variables="{firehose_name=firehose_t`	Arquitecto de la nube, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`o_s3_stream,bucket_arn = arn:aws:s3:::reservationfirehosedestinationbucket,iam_role_name = firehose_to_s3, batch_size=400}"`	
Configure el desencadenador de la función de Lambda.	Utilice la CLI de AWS para configurar el desencadenador (DynamoDB Streams), que invoca la función de Lambda. El tamaño del lote de 400 es para evitar problemas de simultaneidad de Lambda. `aws lambda create-event-source-mapping --function-name LambdaStreamProcessor \ --batch-size 400 --starting-position LATEST \ --event-source-arn <Your Latest Stream ARN From DynamoDB Console>`	Arquitecto de la nube, desarrollador de aplicaciones

Probar la funcionalidad

Tarea	Descripción	Habilidades requeridas
Añada elementos con marcas de tiempo vencidas a la tabla de Reserva.	Para probar la funcionalidad, añada a la tabla `Reservation` los elementos con marcas de tiempo epoch vencidos. El TTL eliminará automátic	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	amente los elementos en función de la marca de tiempo. La función de Lambda se inicia con las actividades de DynamoDB Stream y filtra el evento para identificar la actividad `REMOVE` o los elementos eliminados. A continuación, coloca los registros en el flujo de entrega de Firehose en formato de lote. El flujo de entrega de Firehose transfiere los artículos a un depósito S3 de destino con el `firehosetos3example/year=current year/month=current month/day=current day/hour=current hour/` prefijo. Importante: Para optimizar la recuperación de datos, configure Amazon S3 con `Prefix` y `ErrorOutputPrefix` que se detallan en la sección Información adicional.	

Limpiar los recursos

Tarea	Descripción	Habilidades requeridas
Elimine todos los recursos.	Elimine todos los recursos para asegurarse de que no se le cobre por ningún servicio que no utilice.	Arquitecto de la nube, desarrollador de aplicaciones

Recursos relacionados

- Administración del ciclo de vida del almacenamiento
- Clases de almacenamiento de Amazon S3
- Documentación de AWS SDK para Python (Boto3)

Información adicional

Creación y configuración de un flujo de entrega de Firehose: ejemplos de políticas

Documento de ejemplo de política de relaciones de confianza de Firehose

```
firehose_assume_role = {
        'Version': '2012-10-17',
        'Statement': [
            {
                'Sid': '',
                'Effect': 'Allow',
                'Principal': {
                    'Service': 'firehose.amazonaws.com'
                },
                'Action': 'sts:AssumeRole'
            }
        ]
    }
```

Ejemplos de políticas de permisos de S3

```
s3_access = {
```

```
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "",
                "Effect": "Allow",
                "Action": [
                    "s3:AbortMultipartUpload",
                    "s3:GetBucketLocation",
                    "s3:GetObject",
                    "s3:ListBucket",
                    "s3:ListBucketMultipartUploads",
                    "s3:PutObject"
                ],
                "Resource": [
                    "{your s3_bucket ARN}/*",
                    "{Your s3 bucket ARN}"
                ]
            }
        ]
    }
```

Probar la funcionalidad: configuración de Amazon S3

Se elige la configuración de Amazon S3 con el siguiente `Prefix` y `ErrorOutputPrefix` para optimizar la recuperación de datos.

prefix

```
firehosetos3example/year=! {timestamp: yyyy}/month=! {timestamp:MM}/day=!
 {timestamp:dd}/hour=!{timestamp:HH}/
```

Firehose crea primero una carpeta base llamada `firehosetos3example` directamente debajo del depósito S3. A continuación, evalúa las expresiones`!{timestamp:yyyy}`, `!{timestamp:MM}`!`{timestamp:dd}`, y `!{timestamp:HH}` para año, mes, día y hora utilizando el formato Java DateTimeFormatter.

Por ejemplo, una marca de tiempo de llegada aproximada de 1604683577 en tiempo de época de Unix se evalúa como `year=2020`, `month=11`, `day=06` y `hour=05`. Por lo tanto, se evalúa en `firehosetos3example/year=2020/month=11/day=06/hour=05/` la ubicación de Amazon S3 en la que se entregan los registros de datos.

ErrorOutputPrefix

```
firehosetos3erroroutputbase/!{firehose:random-string}/!{firehose:error-output-type}/!
{timestamp:yyyy/MM/dd}/
```

Los `ErrorOutputPrefix` generan una carpeta base llamada `firehosetos3erroroutputbase` directamente debajo del bucket de S3. La expresión `!{firehose:random-string}` se evalúa como una cadena aleatoria de 11 caracteres, como `ztWxkdg3Thg`. Se podría evaluar como `firehosetos3erroroutputbase/ztWxkdg3Thg/processing-failed/2020/11/06/` la ubicación de un objeto de Amazon S3 en la que se entregan los registros fallidos.

Creación de un PAC de Micro Focus Enterprise Server con Amazon EC2 Auto Scaling y Systems Manager

Creado por Kevin Yung (AWS), Peter Woods (Micro Focus), Abraham Rondon (Micro Focus) y Krithika Palani Selvam (AWS)

Entorno: producción	Tecnologías: modernización; nativa de la nube; infraestr uctura DevOps

Resumen

Este patrón presenta una arquitectura escalable para aplicaciones de mainframe que usan Micro Focus Enterprise Server en un clúster de rendimiento y disponibilidad (PAC) escalable horizontalmente y un grupo de escalado automático Amazon Elastic Compute Cloud (Amazon EC2) en Amazon Web Services (AWS). La solución está totalmente automatizada con enlaces de ciclo de vida de AWS Systems Manager y Amazon EC2 Auto Scaling. Al usar este patrón, puede configurar sus aplicaciones de mainframe en línea y por lotes para lograr una alta resiliencia escalando vertical y horizontalmente de forma automática en función de sus demandas de capacidad.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Software y licencia de Micro Focus Enterprise Server. Para obtener más información, contacte con el departamento de ventas de Micro Focus.
- Comprender el concepto de reconstrucción y entrega de una aplicación de mainframe a ejecutar en Micro Focus Enterprise Server. Para obtener información general, consulte Hoja de datos de Micro Focus Enterprise Server.
- Comprender los conceptos de clúster de rendimiento y disponibilidad escalable horizontalmente de Micro Focus Enterprise Server. Para más información, consulte la documentación de Micro Focus Enterprise Server.

- Comprensión del concepto general de aplicación de mainframe DevOps con integración continua (CI). Para ver un patrón de AWS Prescriptive Guidance desarrollado por AWS y Micro Focus, consulte Modernización de mainframe: DevOps en AWS con Micro Focus.

Limitaciones

- Para obtener una lista de las plataformas compatibles con Micro Focus Enterprise Server, consulte la hoja de datos de Micro Focus Enterprise Server.
- Los scripts y pruebas usados en este patrón se basan en Amazon EC2 Windows Server 2019; no se han probado otras versiones y sistemas operativos de Windows Server con este patrón.
- El patrón se basa en Micro Focus Enterprise Server 6.0 para Windows; no se han probado versiones anteriores o posteriores para desarrollar este patrón.

Versiones de producto

- Micro Focus Enterprise Server 6.0
- Windows Server 2019

Arquitectura

En un entorno de mainframe convencional, debe aprovisionar el hardware para alojar las aplicaciones y los datos corporativos. Para hacer frente a los picos de demanda estacionales, mensuales, trimestrales o incluso imprevistos o sin precedentes, los usuarios de mainframe deben escalar horizontalmente sus capacidades adquiriendo capacidad de almacenamiento y procesamiento adicionales. El aumento de la cantidad de recursos de almacenamiento y capacidad de cómputo mejora el rendimiento general, pero el escalado no es lineal.

Este no es el caso cuando comienza a adoptar un modelo de consumo bajo demanda en AWS mediante servidores Amazon EC2 Auto Scaling y Micro Focus Enterprise. En las siguientes secciones se explica en detalle cómo crear una arquitectura de aplicaciones de mainframe escalable y totalmente automatizada mediante el clúster de rendimiento y disponibilidad (PAC) escalable horizontalmente de Micro Focus Enterprise Server con un grupo de escalado automático de Amazon EC2.

Arquitectura de escalado automático de Micro Focus Enterprise Server

En primer lugar, es importante conocer los conceptos básicos de Micro Focus Enterprise Server. Este entorno proporciona un entorno de implementación x86 compatible con mainframe para aplicaciones que tradicionalmente se ejecutaban en el mainframe de IBM. Ofrece ejecuciones en línea y por lotes, así como un entorno de transacciones compatible con:

- IBM COBOL
- IBM PL/I
- Trabajos por lotes en IBM JCL
- Transacciones de IBM CICS e IMS TM
- Servicios web
- Utilidades de procesamiento por lotes comunes, incluida SORT

Micro Focus Enterprise Server permite la ejecución de aplicaciones de mainframe con cambios mínimos. Las cargas de trabajo de mainframe existentes se pueden trasladar a plataformas x86 y modernizarse para aprovechar las extensiones nativas en la nube de AWS y así expandirse rápidamente a nuevos mercados o geografías.

El patrón AWS Prescriptive Guidance Modernization: DevOps on AWS with Micro Focus introdujo la arquitectura para acelerar el desarrollo y las pruebas de aplicaciones de mainframe en AWS mediante Micro Focus Enterprise Developer y Enterprise Test Server con AWS y AWS CodePipeline . CodeBuild Este patrón se centra en la implementación de aplicaciones de mainframe en el entorno de producción de AWS para lograr una alta disponibilidad y resiliencia.

En un entorno de producción de mainframe, es posible que haya configurado IBM Parallel Sysplex en el mainframe para lograr un alto rendimiento y una alta disponibilidad. Para crear una arquitectura escalable horizontalmente similar a Sysplex, Micro Focus presentó el clúster de rendimiento y disponibilidad (PAC) en Enterprise Server. Los PAC permiten la implementación de aplicaciones de mainframe en varias regiones de Enterprise Server administradas como una sola imagen y escaladas horizontalmente en instancias de Amazon EC2. Los PAC también ofrecen un rendimiento predecible de las aplicaciones y del sistema bajo demanda.

En un PAC, varias instancias de Enterprise Server funcionan juntas como una sola entidad lógica. Por lo tanto, el fallo de una instancia de Enterprise Server no interrumpirá la continuidad del negocio, ya que la capacidad se comparte con otras regiones. Las nuevas instancias se inician automáticamente con una funcionalidad estándar del sector, como un grupo de Amazon EC2 Auto Scaling. Esto elimina los puntos únicos de fallo y mejora la resiliencia ante problemas de hardware,

red y aplicaciones. Las instancias de Enterprise Server escalables horizontalmente se pueden operar y administrar mediante las API de Enterprise Server Common Web Administration (ESCWA), lo que simplifica el mantenimiento operativo y la facilidad de servicio de los Enterprise Server.

Nota: Micro Focus recomienda que el clúster de rendimiento y disponibilidad (PAC) esté formado por, al menos, tres regiones de Enterprise Server. Así, la disponibilidad no se verá comprometida en caso de que una región de Enterprise Server falle o requiera mantenimiento.

La configuración del PAC requiere un servicio de administración de base de datos relacional (RDBMS) compatible para administrar la base de datos regional, una base de datos interregional y las bases de datos de almacenes de datos opcionales. Es necesario usar una base de datos de almacén de datos para gestionar los archivos de Virtual Storage Access Method (VSAM). La compatibilidad con el gestor de archivos de base de datos de Micro Focus mejora la disponibilidad y la escalabilidad. Entre los RDBMS compatibles se incluyen:

- Microsoft SQL Server 2009 o posterior
- PostgreSQL 10.x, incluida la edición compatible con PostgreSQL de Amazon Aurora
- DB2 10.4 o posterior

Para obtener más información sobre los requisitos de RDBMS y PAC compatibles, consulte Micro Focus Enterprise Server: requisitos previos y Micro Focus Enterprise Server: configuración de PAC recomendada.

El siguiente diagrama muestra una configuración de arquitectura de AWS típica para un PAC de Micro Focus.

	Componente	Descripción
1	Grupo de escalado automático de instancias de Enterprise Server	Configure un grupo de escalado automático implementado con las instancias de Enterprise Server en un PAC. Las CloudWatch alarmas de Amazon pueden aumentar o activar el número de instancia

		s mediante CloudWatch métricas.
2	Grupo de escalado automático de instancias ESCWA de Enterprise Server	Configure un grupo de escalado automático implementado con Enterprise Server Common Web Administration (ESCWA). ESCWA proporciona API de gestión de clústeres. Los servidores de ESCWA actúan como plano de control para añadir o eliminar Enterprise Server e iniciar o detener las regiones de Enterprise Server en el PAC durante los eventos de escalado automático de la instancia de Enterprise Server. Como la instancia de ESCWA se usa únicamente para la gestión del PAC, su patrón de tráfico es predecible. y su escalado. automático (el requisito de capacidad deseado se puede establecer en 1).
3	Instancia de Amazon Aurora en una configuración Multi-AZ	Configure un sistema de administración de base de datos relacional (RDBMS) para alojar los archivos de datos de los usuarios y del sistema y compartirlos entre las instancias de Enterprise Server.

4	Instancia y réplica de Amazon ElastiCache for Redis	Configure una instancia principal de ElastiCache Redis y al menos una réplica para alojar los datos de los usuarios y actuar como un repositor io escalable (SOR) para las instancias de Enterpris e Server. Puede configura r uno o más repositorios escalables horizontalmente para almacenar tipos específic os de datos de usuario. Enterprise Server emplea una base de datos NoSQL de Redis como SOR, requisito fundamental para mantener la integridad del PAC.
5	Equilibrador de carga de red	Configure un equilibrador de carga que proporcione un nombre de host para que las aplicaciones se conecten a los servicios proporcionados por las instancias de Enterprise Server (por ejemplo, acceder a la aplicación a través de un emulador 3270).

Estos componentes conforman el requisito mínimo para un clúster PAC de Micro Focus Enterprise Server. La siguiente sección trata sobre la automatización de la administración de clústeres.

Uso de Automatización de AWS Systems Manager para escalar

Una vez implementado el clúster PAC en AWS, el PAC se administra mediante las API de Enterprise Server Common Web Administration (ESCWA).

Para automatizar las tareas de administración de clústeres durante los eventos de escalado automático, puede utilizar los manuales de automatización de Systems Manager y Auto Scaling with Amazon EC2. EventBridge La arquitectura de estas automatizaciones se muestra en el siguiente diagrama.

	Componente	Descripción
1	Enlace de ciclo de vida de escalado automático	Configura enlaces de ciclo de vida de escalado automático y envía notificaciones a Amazon EventBridge cuando se lancen nuevas instancias y las instancias existentes finalicen en el grupo de escalado automático.
2	Amazon EventBridge	Configure una EventBridge regla de Amazon para enrutar los eventos de escalado automático a los objetivos del runbook de Systems Manager Automation.
3	Manuales de procedimientos de Automation	Configure los manuales de automatización de Systems Manager para ejecutar PowerShell scripts de Windows e invoque las API de la CESPAO para administrar el PAC. Para ver más ejemplos, consulte la sección Información adicional.
4	Instancia ESCWA de Enterprise Server en un grupo de escalado automático	Configurar una instancia ESCWA de Enterprise Server en un grupo de escalado

automático. La instancia de ESCWA proporciona API para gestionar el PAC.

Herramientas

- Micro Focus Enterprise Server: Micro Focus Enterprise Server proporciona el entorno de ejecución para aplicaciones creadas con cualquier variante de entorno de desarrollo integrado (IDE) de Enterprise Developer.
- Amazon EC2 Auto Scaling: Amazon EC2 Auto Scaling le ayuda a garantizar que cuenta con la cantidad correcta de instancias de Amazon EC2 disponibles para gestionar la carga de su aplicación. Crea colecciones de instancias de EC2, denominadas grupos de escalado automático, y especifica un número mínimo y máximo de instancias.
- Amazon ElastiCache for Redis: Amazon ElastiCache es un servicio web para configurar, administrar y escalar un almacén de datos en memoria distribuido o un entorno de caché en la nube. Proporciona una capacidad de almacenamiento en caché de alto rendimiento, escalable y rentable.
- Amazon RDS: Amazon Relational Database Service (Amazon RDS) es un servicio web que facilita la configuración, el funcionamiento y el escalado de una base de datos relacional en la nube de AWS. Proporciona una capacidad rentable y de tamaño ajustable para una base de datos relacional y se ocupa de las tareas comunes de administración de bases de datos.
- AWS Systems Manager: AWS Systems Manager es un servicio que puede utilizar para ver y controlar su infraestructura en AWS. Mediante la consola de Systems Manager, puede ver los datos operativos de varios servicios de AWS y automatizar las tareas operativas en sus recursos de AWS. Systems Manager lo ayuda a mantener la seguridad y la conformidad mediante el análisis de sus instancias administradas y el informe sobre las infracciones de las políticas que detecte o la toma de medidas correctivas con respecto a estas.

Epics

Crear una instancia de Amazon Aurora

Tarea	Descripción	Habilidades requeridas
Cree una CloudFormation plantilla de AWS para una instancia de Amazon Aurora.	Utilice el fragmento de código de ejemplo de AWS para crear una CloudFormation plantilla que cree una instancia de Amazon Aurora compatible con PostgreSQL Edition.	Arquitecto de la nube
Implemente una CloudFormation pila para crear la instancia de Amazon Aurora.	Use la CloudFormation plantilla para crear una instancia compatible con Aurora PostgreSQL que tenga habilitada la replicación Multi-AZ para las cargas de trabajo de producción.	Arquitecto de la nube
Configure los ajustes de conexión a la base de datos para Enterprise Server.	Siga las instrucciones de la documentación de Micro Focus para preparar las cadenas de conexión y la configuración de la base de datos para Micro Focus Enterprise Server.	DevOps Ingeniero de datos, ingeniero

Crear un ElastiCache clúster de Amazon para la instancia de Redis

Tarea	Descripción	Habilidades requeridas
Crea una CloudFormation plantilla para el ElastiCache clúster de Amazon para la instancia de Redis.	Utilice el fragmento de código de ejemplo de AWS para crear una CloudFormation plantilla que cree un ElastiCac	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	he clúster de Amazon para la instancia de Redis.	
Implemente la CloudFormation pila para crear un ElastiCac he clúster de Amazon para la instancia de Redis.	Cree el ElastiCache clúster de Amazon para la instancia de Redis que tiene habilitad a la replicación Multi-AZ para las cargas de trabajo de producción.	Arquitecto de la nube
Configure los ajustes de conexión de Enterprise Server PSOR.	Siga las instrucciones de la documentación de Micro Focus para preparar la configuración de la conexión del repositorio Scale-Out PAC (PSOR) para Micro Focus Enterprise Server PAC.	DevOps ingeniero

Cree un grupo de escalado automático de ESCWA para Micro Focus Enterprise Server

Tarea	Descripción	Habilidades requeridas
Cree una AMI de Micro Focus Enterprise Server.	Cree una instancia de Amazon EC2 de Windows Server e instale el binario de Micro Focus Enterprise Server en la instancia de EC2. Crear una imagen de máquina de Amazon (AMI) de una instancia EC2. Para más información, consulte la documentación de instalación de Enterprise Server.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Cree una CloudFormation plantilla para Enterprise Server ESCWA.	Use el fragmento de código de ejemplo de AWS para crear una plantilla de una pila personalizada de Enterprise Server ESCWA en un grupo de escalado automático.	Arquitecto de la nube
Implemente la CloudFormation pila para crear un grupo de escalado de Amazon EC2 para Enterprise Server ESCWA.	Utilice la CloudFormation plantilla para implementar el grupo de escalado automático con la AMI de la CESPAO de Micro Focus Enterprise Server creada en la historia anterior.	Arquitecto de la nube

Cree de un manual de procedimientos de Automatización de AWS Systems Manager

Tarea	Descripción	Habilidades requeridas
Cree una CloudFormation plantilla para un manual de automatización de Systems Manager.	Utilice los fragmentos de código de ejemplo de la sección de información adicional para crear una CloudFormation plantilla que cree un manual de automatización de Systems Manager para automatizar la creación de PAC, la ampliación de Enterprise Server y la ampliación horizontal de Enterprise Server.	Arquitecto de la nube
Implemente la CloudFormation pila que contiene el manual de automatización de Systems Manager.	Utilice la CloudFormation plantilla para implementar una pila que contenga el manual de automatización	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	para la creación de PAC, el escalado de Enterprise Server y el escalado de Enterprise Server.	

Cree un grupo de escalado automático para Micro Focus Enterprise Server

Tarea	Descripción	Habilidades requeridas
Cree una CloudFormation plantilla para configurar un grupo de escalado automátic o para Micro Focus Enterprise Server.	Utilice el fragmento de código de ejemplo de AWS para crear una CloudFormation plantilla que cree un grupo de escalado automático. Esta plantilla reutilizará la misma AMI que se creó para la instancia de Micro Focus Enterprise Server ESCWA. A continuación, utilice un fragmento de código de ejemplo de AWS para crear el evento del ciclo de vida de escalado automático y configure Amazon EventBrid ge para filtrar los eventos de escalado horizontal y horizontal en la misma plantilla . CloudFormation	Arquitecto de la nube
Implemente la CloudFormation pila para el grupo de escalado automático de los servidores empresariales Micro Focus.	Implemente la CloudFormation pila que contiene el grupo de escalado automático para los servidores Micro Focus Enterprise.	Arquitecto de la nube

Recursos relacionados

- Clúster de rendimiento y disponibilidad (PAC) de Micro Focus Enterprise Server
- Enlaces de ciclo de vida de Amazon EC2 Auto Scaling
- Ejecute automatizaciones con activadores mediante EventBridge

Información adicional

Los siguientes escenarios deben automatizarse para reducir o escalar horizontalmente los clústeres de PAC.

Automatización para iniciar o recrear un PAC

Al inicio de un clúster de PAC, Enterprise Server requiere que ESCWA invoque las API para crear una configuración de PAC. Esta acción inicia y agrega regiones de Enterprise Server al PAC. Para crear o volver a crear un PAC, siga estos pasos:

1. Configure un repositorio escalable horizontalmente de PAC (PSOR) en ESCWA con un nombre determinado.

```
POST /server/v1/config/groups/sors
```

2. Cree un PAC con un nombre determinado y adjúntele el PSOR.

```
POST /server/v1/config/groups/pacs
```

3. Configure la base de datos regional y la base de datos interregional si es la primera vez que configura un PAC.

   Nota: en este paso se usan consultas SQL y la herramienta dbhfhadmin de la línea de comandos de Micro Focus Enterprise Suite para crear la base de datos e importar los datos iniciales.

4. Instale la definición de PAC en las regiones de Enterprise Server.

```
POST /server/v1/config/mfds
POST /native/v1/config/groups/pacs/${pac_uid}/install
```

5. Inicie las regiones de Enterprise Server en el PAC.

```
POST /native/v1/regions/${host_ip}/${port}/${region_name}/start
```

Los pasos anteriores se pueden implementar mediante un PowerShell script de Windows.

En los pasos siguientes se explica cómo crear una automatización para crear un PAC mediante la reutilización del PowerShell script de Windows.

1. Cree una plantilla de lanzamiento de Amazon EC2 que descargue o cree el PowerShell script de Windows como parte del proceso de arranque. Por ejemplo, puede emplear datos de usuario de EC2 para descargar el script de un bucket de Amazon Simple Storage Service (Amazon S3).
2. Cree un runbook de AWS Systems Manager Automation para invocar el script de Windows PowerShell .
3. Asocie el manual de procedimientos a la instancia de ESCWA mediante la etiqueta de instancia.
4. Cree un grupo de escalado automático ESCWA utilizando la plantilla de lanzamiento.

Puede usar el siguiente CloudFormation fragmento de AWS de ejemplo para crear el runbook de automatización.

CloudFormation Fragmento de ejemplo de un manual de automatización de Systems Manager utilizado para la creación de un PAC

```
PACInitDocument:
   Type: AWS::SSM::Document
   Properties:
     DocumentType: Command
     Content:
       schemaVersion: '2.2'
       description: Operation Runbook to create Enterprise Server PAC
       mainSteps:
       - action: aws:runPowerShellScript
         name: CreatePAC
         inputs:
           onFailure: Abort
           timeoutSeconds: "1200"
           runCommand:
           - |
             C:\Scripts\PAC-Init.ps1
PacInitAutomation:
   Type: AWS::SSM::Document
   Properties:
     DocumentType: Automation
     Content:
```

```
        description: Prepare Micro Focus PAC Cluster via ESCWA Server
        schemaVersion: '0.3'
        assumeRole: !GetAtt SsmAssumeRole.Arn
        mainSteps:
          - name: RunPACInitDocument
            action: aws:runCommand
            timeoutSeconds: 300
            onFailure: Abort
            inputs:
              DocumentName: !Ref PACInitDocument
              Targets:
                - Key: tag:Enterprise Server - ESCWA
                  Values:
                    - "true"
  PacInitDocumentAssociation:
    Type: AWS::SSM::Association
    Properties:
      DocumentVersion: "$LATEST"
      Name: !Ref PACInitDocument
      Targets:
        - Key: tag:Enterprise Server - ESCWA
          Values:
            - "true"
```

Para obtener más información, consulte Micro Focus Enterprise Server: Configuración de un PAC.

Automatización para escalado horizontal con una nueva instancia de Enterprise Server

Cuando una instancia de Enterprise Server se escala horizontalmente, su región de Enterprise Server debe añadirse al PAC. En los siguientes pasos se explica cómo invocar las API de ESCWA y añadir la región de Enterprise Server al PAC.

1. Instale la definición de PAC en las regiones de Enterprise Server.

```
POST '/server/v1/config/mfds'
POST /native/v1/config/groups/pacs/${pac_uid}/install
```

2. Inicie en caliente la región en el PAC.

```
POST /native/v1/regions/${host_ip}/${port}/${region_name}/start
```

3. Agregue la instancia de Enterprise Server al equilibrador de carga asociando el grupo de escalado automático al equilibrador de carga.

Los pasos anteriores se pueden implementar mediante un script de Windows. PowerShell Para obtener más información, consulte Micro Focus Enterprise Server: Configuración de un PAC.

Los siguientes pasos se pueden utilizar para crear una automatización basada en eventos que permita añadir una instancia de Enterprise Server recién lanzada a un PAC reutilizando el PowerShell script de Windows.

1. Cree una plantilla de lanzamiento de Amazon EC2 para una instancia de Enterprise Server que aprovisione una región de Enterprise Server durante su arranque. Por ejemplo, puede usar el comando mfds de Micro Focus Enterprise Server para importar una configuración regional. Para obtener más detalles y ver las opciones disponibles para este comando, consulte la referencia de Enterprise Server.
2. Cree un grupo de escalado automático de Enterprise Server que emplee la plantilla de lanzamiento creada en el paso anterior.
3. Cree un manual de automatización de Systems Manager para invocar el script de Windows PowerShell .
4. Asocie el manual de procedimientos a la instancia de ESCWA mediante la etiqueta de instancia.
5. Cree una EventBridge regla de Amazon para filtrar el evento EC2 Instance Launch Successful para el grupo de escalado automático de Enterprise Server y cree el objetivo para utilizar el manual de automatización.

Puede utilizar el siguiente CloudFormation fragmento de ejemplo para crear el manual de automatización y la regla. EventBridge

CloudFormation Fragmento de ejemplo de Systems Manager utilizado para escalar instancias de Enterprise Server

```
ScaleOutDocument:
   Type: AWS::SSM::Document
   Properties:
     DocumentType: Command
     Content:
       schemaVersion: '2.2'
       description: Operation Runbook to Adding MFDS Server into an existing PAC
       parameters:
         MfdsPort:
           type: String
         InstanceIpAddress:
           type: String
```

```
            default: "Not-Available"
          InstanceId:
            type: String
            default: "Not-Available"
        mainSteps:
        - action: aws:runPowerShellScript
          name: Add_MFDS
          inputs:
            onFailure: Abort
            timeoutSeconds: "300"
            runCommand:
            - |
              $ip = "{{InstanceIpAddress}}"
              if ( ${ip} -eq "Not-Available" ) {
                $ip = aws ec2 describe-instances --instance-id {{InstanceId}} --output
text --query "Reservations[0].Instances[0].PrivateIpAddress"
              }
              C:\Scripts\Scale-Out.ps1 -host_ip ${ip} -port {{MfdsPort}}

  PacScaleOutAutomation:
    Type: AWS::SSM::Document
    Properties:
      DocumentType: Automation
      Content:
        parameters:
          MfdsPort:
            type: String
          InstanceIpAddress:
            type: String
            default: "Not-Available"
          InstanceId:
            type: String
            default: "Not-Available"
        description: Scale Out 1 New Server in Micro Focus PAC Cluster via ESCWA
Server
        schemaVersion: '0.3'
        assumeRole: !GetAtt SsmAssumeRole.Arn
        mainSteps:
          - name: RunScaleOutCommand
            action: aws:runCommand
            timeoutSeconds: 300
            onFailure: Abort
            inputs:
              DocumentName: !Ref ScaleOutDocument
```

```
            Parameters:
              InstanceIpAddress: "{{InstanceIpAddress}}"
              InstanceId: "{{InstanceId}}"
              MfdsPort: "{{MfdsPort}}"
            Targets:
              - Key: tag:Enterprise Server - ESCWA
                Values:
                  - "true"
```

Automatización para reducir horizontalmente una instancia de Enterprise Server

Al igual que el escalado horizontal, cuando una instancia de Enterprise Server se reduce horizontalmente, se inicia la acción de ciclo de vida de finalización de la instancia de EC2, y se necesitan las siguientes llamadas al proceso y a la API para eliminar una instancia de Micro Focus Enterprise Server del PAC.

1. Detenga la región de la instancia de Enterprise Server que está finalizando.

```
POST "/native/v1/regions/${host_ip}/${port}/${region_name}/stop"
```

2. Elimine la instancia de Enterprise Server del PAC.

```
DELETE "/server/v1/config/mfds/${uid}"
```

3. Envíe una señal para continuar con la finalización de la instancia de Enterprise Server.

Los pasos anteriores se pueden implementar en un script de Windows PowerShell . Para obtener más información sobre este proceso, consulte el documento de Micro Focus Enterprise Server: Administración de un PAC.

En los siguientes pasos se explica cómo crear una automatización basada en eventos para cerrar una instancia de Enterprise Server desde un PAC mediante la reutilización del script de Windows. PowerShell

1. Cree un manual de automatización de Systems Manager para invocar el script de Windows PowerShell .
2. Asocie el manual de procedimientos a la instancia de ESCWA mediante la etiqueta de instancia.
3. Cree un enlace de ciclo de vida de grupo de escalado automático para la finalización de la instancia de EC2.

4. Cree una EventBridge regla de Amazon para filtrar el evento de acción del ciclo de vida de finalización de la instancia de EC2 para el grupo de escalado automático de Enterprise Server y cree el objetivo para usar el manual de automatización.

Puede utilizar la siguiente CloudFormation plantilla de ejemplo para crear un manual, un enlace de ciclo de vida y una EventBridge regla de Systems Manager Automation.

CloudFormation Fragmento de ejemplo de un manual de automatización de Systems Manager utilizado para escalar en una instancia de Enterprise Server

```
 ScaleInDocument:
    Type: AWS::SSM::Document
    Properties:
      DocumentType: Command
      Content:
        schemaVersion: '2.2'
        description: Operation Runbook to Remove MFDS Server from PAC
        parameters:
          MfdsPort:
            type: String
          InstanceIpAddress:
            type: String
            default: "Not-Available"
          InstanceId:
            type: String
            default: "Not-Available"
        mainSteps:
        - action: aws:runPowerShellScript
          name: Remove_MFDS
          inputs:
            onFailure: Abort
            runCommand:
            - |
              $ip = "{{InstanceIpAddress}}"
              if ( ${ip} -eq "Not-Available" ) {
                $ip = aws ec2 describe-instances --instance-id {{InstanceId}} --output
text --query "Reservations[0].Instances[0].PrivateIpAddress"
              }
              C:\Scripts\Scale-In.ps1 -host_ip ${ip} -port {{MfdsPort}}

  PacScaleInAutomation:
    Type: AWS::SSM::Document
```

```
    Properties:
      DocumentType: Automation
      Content:
        parameters:
          MfdsPort:
            type: String
          InstanceIpAddress:
            type: String
            default: "Not-Available"
          InstanceId:
            type: String
            default: "Not-Available"
        description: Scale In 1 New Server in Micro Focus PAC Cluster via ESCWA Server
        schemaVersion: '0.3'
        assumeRole: !GetAtt SsmAssumeRole.Arn
        mainSteps:
          - name: RunScaleInCommand
            action: aws:runCommand
            timeoutSeconds: "600"
            onFailure: Abort
            inputs:
              DocumentName: !Ref ScaleInDocument
              Parameters:
                InstanceIpAddress: "{{InstanceIpAddress}}"
                MfdsPort: "{{MfdsPort}}"
                InstanceId: "{{InstanceId}}"
              Targets:
                - Key: tag:Enterprise Server - ESCWA
                  Values:
                    - "true"
          - name: TerminateTheInstance
            action: aws:executeAwsApi
            inputs:
              Service: autoscaling
              Api: CompleteLifecycleAction
              AutoScalingGroupName: !Ref AutoScalingGroup
              InstanceId: "{{ InstanceId }}"
              LifecycleActionResult: CONTINUE
              LifecycleHookName: !Ref ScaleInLifeCycleHook
```

Automatización para un desencadenante de escalado automático de Amazon EC2

El proceso de configuración de una política de escalado para instancias de Enterprise Server requiere comprender el comportamiento de la aplicación. En la mayoría de los casos, puede establecer políticas de escalado de seguimiento de objetivos. Por ejemplo, puedes usar el uso promedio de la CPU como CloudWatch métrica de Amazon para configurar la política de escalado automático. Para obtener más información, consulte Políticas de escalado de seguimiento de destino de Amazon EC2 Auto Scaling. Para aplicaciones con patrones de tráfico regulares, considere la posibilidad de usar una política de escalado predictivo. Para más información, consulte Escalado predictivo para Amazon EC2 Auto Scaling.

Cree una arquitectura sin servidor multiusuario en Amazon Service OpenSearch

Creado por Tabby Ward (AWS) y Nisha Gambhir (AWS)

Entorno: PoC o piloto	Tecnologías: modernización; SaaS; sin servidor	Carga de trabajo: código abierto
Servicios de AWS: Amazon OpenSearch Service; AWS Lambda; Amazon S3; Amazon API Gateway		

Resumen

Amazon OpenSearch Service es un servicio gestionado que facilita la implementación, el funcionamiento y el escalado de Elasticsearch, un popular motor de búsqueda y análisis de código abierto. Amazon OpenSearch Service ofrece búsquedas de texto libre, así como ingestión y creación de paneles prácticamente en tiempo real para la transmisión de datos, como registros y métricas.

Los proveedores de software como servicio (SaaS) suelen utilizar Amazon OpenSearch Service para abordar una amplia gama de casos de uso, como obtener información sobre los clientes de forma escalable y segura y, al mismo tiempo, reducir la complejidad y el tiempo de inactividad.

El uso de Amazon OpenSearch Service en un entorno multiusuario introduce una serie de consideraciones que afectan a la partición, el aislamiento, la implementación y la administración de la solución SaaS. Los proveedores de SaaS deben considerar cómo escalar de manera efectiva sus clústeres de Elasticsearch con cargas de trabajo en constante cambio. También deben tener en cuenta cómo pueden afectar la estratificación y el ruido aledaño a su modelo de particionamiento.

Este patrón revisa los modelos empleados para representar y aislar los datos de los usuarios con constructos de Elasticsearch. Además, el patrón se centra en una arquitectura de referencia sencilla sin servidor como ejemplo para demostrar la indexación y la búsqueda mediante Amazon OpenSearch Service en un entorno multiusuario. Implementa el modelo de particionamiento de datos de grupos, que comparte un mismo índice entre todos los usuarios y, al mismo tiempo, mantiene el aislamiento de los datos de los mismos. Este patrón utiliza los siguientes servicios de Amazon Web

Services (AWS): Amazon API Gateway, AWS Lambda, Amazon Simple Storage Service (Amazon S3) y Amazon Service. OpenSearch

Para obtener más información sobre el modelo de grupo y otros modelos de particionamiento de datos, consulte la sección de Información adicional.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Interfaz de la línea de comandos de AWS (AWS CLI) versión 2.x, instalada y configurada en Linux, macOS o Windows
- Python versión 3.7
- pip3: el código fuente de Python se proporciona como un archivo .zip para implementarlo en una función de Lambda. Si quiere usar el código localmente o personalizarlo, siga estos pasos para desarrollar y recompilar el código fuente:
  1. Genere el archivo `requirements.txt` ejecutando el siguiente comando en el mismo directorio que los scripts de Python: `pip3 freeze > requirements.txt`
  2. Instale las dependencias: `pip3 install -r requirements.txt`

Limitaciones

- Este código se ejecuta en Python y, actualmente, no es compatible con otros lenguajes de programación.
- La aplicación de muestra no incluye soporte multirregional ni de recuperación de desastres (DR) de AWS.
- Este patrón sólo pretende servir de ejemplo. No está pensado para ser utilizado en un entorno de producción.

Arquitectura

El siguiente diagrama ilustra la arquitectura de alto nivel de este patrón. La arquitectura incluye lo siguiente:

- AWS Lambda, para indexar y consultar el contenido

- Amazon OpenSearch Service para realizar búsquedas
- Amazon API Gateway, para proporcionar a la API interacción con el usuario
- Amazon S3, para almacenar datos sin procesar (no indexados)
- Amazon CloudWatch supervisará los registros
- AWS Identity y Access Management (IAM) para crear roles y políticas de usuario

Automatizar y escalar

Para mayor simplicidad, el patrón usa la CLI de AWS para aprovisionar la infraestructura e implementar el código de muestra. Puede crear una CloudFormation plantilla de AWS o scripts del AWS Cloud Development Kit (AWS CDK) para automatizar el patrón.

Herramientas

Servicios de AWS

- CLI de AWS: la interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta unificada para administrar los servicios y recursos de AWS mediante comandos en su intérprete de línea de comandos.
- AWS Lambda: AWS Lambda es un servicio informático que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo.
- Amazon API Gateway: Amazon API Gateway es un servicio de AWS para crear, publicar, mantener, supervisar y proteger REST, HTTP y WebSocket API a cualquier escala.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos que permite almacenar y recuperar cualquier cantidad de información en cualquier momento y desde cualquier lugar de la web.
- Amazon OpenSearch Service: Amazon OpenSearch Service es un servicio totalmente gestionado que te facilita la implementación, la protección y la ejecución de Elasticsearch a escala y de forma rentable.

Código

El archivo adjunto incluye archivos de muestra para este patrón. Entre ellos se incluyen:

- `index_lambda_package.zip`— La función Lambda para indexar datos en Amazon OpenSearch Service mediante el modelo de grupo.
- `search_lambda_package.zip`— La función Lambda para buscar datos en Amazon OpenSearch Service.
- `Tenant-1-data` — Muestra de datos sin procesar (no indexados) para Usuario-1.
- `Tenant-2-data`: muestra de datos sin procesar (no indexados) para Usuario-2.

Importante: las historias de este patrón incluyen ejemplos de comandos de CLI formateados para Unix, Linux y macOS. Para Windows, sustituya la barra diagonal invertida (\) utilizada como carácter de continuación de Unix al final de cada línea por el signo de intercalación (^).

Epics

Creación y configuración de un bucket de S3

Tarea	Descripción	Habilidades requeridas
Crear un bucket de S3.	Cree un bucket de S3 en su región de AWS. Este bucket contendrá los datos de usuarios no indexados de la aplicación de muestra. Asegúrese de que el nombre del bucket de S3 es único a nivel mundial, ya que el espacio de nombres es compartido por todas las cuentas de AWS. Para crear un bucket de S3, puede usar el comando create-bucket en AWS CLI de la siguiente manera: `aws s3api create-bucket \`	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	`--bucket tenantrawdata \` `--region <your-AWS-Region>` donde `tenantrawdata` es el nombre de bucket de S3. (Puede usar cualquier nombre único que siga las pautas de nomenclatura de buckets).	

Cree y configure un clúster de Elasticsearch

Tarea	Descripción	Habilidades requeridas
Crea un dominio OpenSearch de Amazon Service.	Ejecute el create-elasticsearch-domaincomando AWS CLI para crear un dominio OpenSearch de Amazon Service: `aws es create-elasticsearch-domain \` `--domain-name vpc-cli-example \` `--elasticsearch-version 7.10 \` `--elasticsearch-cluster-config InstanceType=t3.medium.elasticsearch,InstanceCount=1 \` `--ebs-options EBSEnabled=true,VolumeType=gp2,VolumeSize=10 \`	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	`--domain-endpoint-options "{\"EnforceHTTPS\": true}" \ --encryption-at-rest-options "{\"Enabled\": true}" \ --node-to-node-encryption-options "{\"Enabled\": true}" \ --advanced-security-options "{\"Enabled\": true, \"InternalUserDatabaseEnabled\": true, \ \"MasterUserOptions\": {\"MasterUserName\": \"KibanaUser\", \ \"MasterUserPassword\": \"NewKibanaPassword@123\"}}" \ --vpc-options "{\"SubnetIds\": [\"<subnet-id>\"], \"SecurityGroupIds\": [\"<sg-id>\"]}" \ --access-policies "{\"Version\": \"2012-10-17\", \"Statement\": [{ \"Effect\": \"Allow\", \ \"Principal\": {\"AWS\": \"*\" }, \"Action\":\"es:*\", \ \"Resource\": \"arn:aws:es:region:account-id:domain\/vpc-cli-example\/*\" }] }"`	

Tarea	Descripción	Habilidades requeridas
	El número de instancias está establecido en 1, ya que el dominio se usa para realizar pruebas. Debe habilitar un control de acceso detallado mediante el parámetro `advanced-security-options` , ya que los detalles no se pueden cambiar una vez creado el dominio. Este comando crea un nombre de usuario maestro (`KibanaUser`) y una contraseña que le permitirá iniciar sesión en la consola de Kibana. Como el dominio forma parte de una nube privada virtual (VPC), debe asegurarse de poder acceder a la instancia de Elasticsearch especific ando la política de acceso que va a usar. Para obtener más informaci ón, consulte Lanzamiento de dominios de Amazon OpenSearch Service mediante una VPC en la documentación de AWS.	

Tarea	Descripción	Habilidades requeridas
Instale un host bastión.	Configure una instancia de Windows de Amazon Elastic Compute Cloud (Amazon EC2) como host bastión para acceder a la consola de Kibana. El grupo de seguridad de Elasticsearch debe permitir el tráfico procedente del grupo de seguridad de Amazon EC2. Para obtener más instrucciones, consulte la publicación del blog Controlar el acceso de red a las instancias de EC2 mediante un servidor bastión. Cuando se haya configurado el host bastión y tenga disponible el grupo de seguridad asociado a la instancia, utilice el authorize-security-group-ingresscomando AWS CLI para añadir permisos al grupo de seguridad de Elasticsearch a fin de permitir el puerto 443 del grupo de seguridad Amazon EC2 (host bastión). `aws ec2 authorize-security-group-ingress \` `  --group-id <SecurityGroupIdfElasticSearch> \` `  --protocol tcp \` `  --port 443 \`	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	`--source-group <SecurityGroupIdfBashionHostEC2>`	

Crear y configurar la función de índice de Lambda

Tarea	Descripción	Habilidades requeridas
Para crear el rol de ejecución de Lambda	Ejecute el comando create-role en la CLI de AWS para conceder a la función de índice de Lambda acceso a los servicios y recursos de AWS: `aws iam create-role \ --role-name index-lambda-role \ --assume-role-policy-document file://lambda_assume_role.json` donde `lambda_assume_role.json` es un documento JSON en la carpeta actual que concede permisos de `AssumeRole` a la función de Lambda, de la siguiente manera: `{ "Version": "2012-10-17", "Statement": [ {`	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	"Effect": "Allow", "Principal": { "Service": "lambda.amazonaws.com" }, "Action": "sts:AssumeRole" }] }	

Tarea	Descripción	Habilidades requeridas
Adjunte políticas gestionadas al rol de Lambda.	Ejecute el attach-role-policy comando AWS CLI para adjuntar políticas administr adas al rol creado en el paso anterior. Estas dos políticas otorgan al rol permisos para crear una interfaz de red elástica y escribir CloudWatch registros en Logs. `aws iam attach-role-policy \` `  --role-name index-lambda-role \` `  --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole` `aws iam attach-role-policy \` `  --role-name index-lambda-role \` `  --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole`	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Cree una política para dar permisos a la función de índice de Lambda de modo que pueda leer los objetos de S3.	Ejecute el comando create-policy en la CLI de AWS para conceder permisos de `s3:GetObject` a la función de índice de Lambda de modo que pueda leer los objetos del bucket de S3: `aws iam create-policy \ --policy-name s3-permission-policy \ --policy-document file://s3-policy.json` El archivo `s3-policy.json` es un documento JSON en la carpeta actual que concede permisos de `s3:GetObject` para permitir el acceso de lectura a los objetos de S3. Si ha usado un nombre diferente al crear el bucket de S3, proporcione el nombre correcto en sección `Resource` de: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "s3:GetObject",`	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	<pre>"Resource ": "arn:aws:s3:::tena ntrawdata/*" }] }</pre>	
Adjunte la política de permisos de Amazon S3 al rol de ejecución de Lambda.	Ejecute el attach-role-policycomando AWS CLI para adjuntar la política de permisos de Amazon S3 que creó en el paso anterior a la función de ejecución de Lambda: <pre>aws iam attach-role- policy \ --role-name index-lam bda-role \ --policy-arn <PolicyARN></pre> donde `PolicyARN` es el Nombre de recurso de Amazon (ARN) de la política de permisos de Amazon S3. Puede obtener este valor del resultado del comando anterior.	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Cree la función de indexar de Lambda.	Ejecute el comando create-function de la AWS CLI para crear la función de índice Lambda, que accederá a Amazon Service: OpenSearch `aws lambda create-function \ --function-name index-lambda-function \ --zip-file fileb://index_lambda_package.zip \ --handler lambda_index.lambda_handler \ --runtime python3.7 \ --role "arn:aws:iam::account-id:role/index-lambda-role" \ --timeout 30 \ --vpc-config "{\"SubnetIds\": [\"<subnet-id1\>", \"<subnet-id2>\"], \ \"SecurityGroupIds\": [\"<sg-1>\"]}"`	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Permita que Amazon S3 llame a la función de índice de Lambda.	Ejecute el comando add-permission en la CLI de AWS para conceder a Amazon S3 el permiso de llamar a la función de índice de Lambda: `aws lambda add-permission \ --function-name index-lambda-function \ --statement-id s3-permissions \ --action lambda:InvokeFunction \ --principal s3.amazonaws.com \ --source-arn "arn:aws:s3:::tenantrawdata" \ --source-account "<account-id>"`	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Añada un desencadenante de Lambda para el evento de Amazon S3.	Ejecute el put-bucket-notification-configuration comando AWS CLI para enviar notificaciones a la función de índice Lambda cuando se detecte el `ObjectCreated` evento de Amazon S3. La función de índice se ejecuta cada vez que se carga un objeto en el bucket de S3. `aws s3api put-bucket-notification-configuration \ --bucket tenantrawdata \ --notification-configuration file://s3-trigger.json` El archivo `s3-trigger.json` es un documento JSON de la carpeta actual que añade la política de recursos a la función de Lambda cuando se produce el evento `ObjectCreated` de Amazon S3.	Arquitecto de la nube, administrador de la nube

Crear y configurar la función de búsqueda de Lambda

Tarea	Descripción	Habilidades requeridas
Para crear el rol de ejecución de Lambda	Ejecute el comando create-role en la CLI de AWS para	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	conceder a la función de búsqueda de Lambda acceso a los servicios y recursos de AWS: `aws iam create-role \ --role-name search-lambda-role \ --assume-role-policy-document file://lambda_assume_role.json` donde `lambda_assume_role.json` es un documento JSON en la carpeta actual que concede permisos de `AssumeRole` a la función de Lambda, de la siguiente manera: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "lambda.amazonaws.com" }, "Action": "sts:AssumeRole" } ] }`	

Tarea	Descripción	Habilidades requeridas
Adjunte políticas gestionadas al rol de Lambda.	Ejecute el attach-role-policy comando AWS CLI para adjuntar políticas administr adas al rol creado en el paso anterior. Estas dos políticas otorgan al rol permisos para crear una interfaz de red elástica y escribir CloudWatch registros en Logs. `aws iam attach-role-policy \` `  --role-name search-lambda-role \` `  --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole` `aws iam attach-role-policy \` `  --role-name search-lambda-role \` `  --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole`	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Cree la función de búsqueda de Lambda.	Ejecute el comando create-function de la AWS CLI para crear la función de búsqueda Lambda, que accederá a Amazon Service: OpenSearch `aws lambda create-function \ --function-name search-lambda-function \ --zip-file fileb://search_lambda_package.zip \ --handler lambda_search.lambda_handler \ --runtime python3.7 \ --role "arn:aws:iam::account-id:role/search-lambda-role" \ --timeout 30 \ --vpc-config "{\"SubnetIds\": [\"<subnet-id1\>", \"<subnet-id2>\"], \ \"SecurityGroupIds\": [\"<sg-1>\"]}"`	Arquitecto de la nube, administrador de la nube

Cree y configure los roles de usuario

Tarea	Descripción	Habilidades requeridas
Cree roles de IAM para los usuarios.	Ejecute el comando create-role en la CLI de AWS para crear dos roles de usuario que servirán para probar la funcionalidad de búsqueda:	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	`aws iam create-role \ --role-name Tenant-1-role \ --assume-role-policy-document file://assume-role-policy.json` `aws iam create-role \ --role-name Tenant-2-role \ --assume-role-policy-document file://assume-role-policy.json` El archivo `assume-role-policy.json` es un documento JSON en la carpeta actual que concede permisos de `AssumeRole` al rol de ejecución de Lambda: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": "<Lambda execution role for index function>", "AWS": "<Lambda execution role for search function>" }, "Action": "sts:AssumeRole"`	

Tarea	Descripción	Habilidades requeridas
	<pre> }] }</pre>	

Tarea	Descripción	Habilidades requeridas
Crear una política de IAM de usuario.	Ejecute el comando create-policy en la CLI de AWS para crear una política de usuario que conceda acceso a las operaciones de Elasticsearch: `aws iam create-policy \ --policy-name tenant-policy \ --policy-document file://policy.json` El archivo `policy.json` es un documento JSON en la carpeta actual que concede permisos en Elasticsearch: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "es:ESHttpDelete", "es:ESHttpGet", "es:ESHttpHead", "es:ESHttpPost", "es:ESHttpPut", "es:ESHttpPatch" ],`	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	<pre>"Resource": ["<ARN of Elasticsearch domain created earlier>"] }] }</pre>	
Adjunte la política de IAM del usuario a los roles del usuario.	Ejecute el attach-role-policy comando AWS CLI para adjuntar la política de IAM de inquilinos a las dos funciones de inquilino que creó en el paso anterior: <pre>aws iam attach-role-policy \ --policy-arn arn:aws:iam::account-id:policy/tenant-policy \ --role-name Tenant-1-role aws iam attach-role-policy \ --policy-arn arn:aws:iam::account-id:policy/tenant-policy \ --role-name Tenant-2-role</pre> La política ARN procede de lo obtenido en el paso anterior.	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Cree una política de IAM para conceder permisos de asunción de rol a Lambda.	Ejecute el comando create-policy en la CLI de AWS para crear una política que permita a Lambda asumir el rol de usuario `aws iam create-policy \ --policy-name assume-tenant-role-policy \ --policy-document file://lambda_policy.json` El archivo `lambda_policy.json` es un documento JSON en la carpeta actual que concede permisos a `AssumeRole` : `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "sts:AssumeRole", "Resource": "<ARN of tenant role created earlier>" } ] }` En `Resource`, puede usar un carácter comodín para evitar	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	crear una nueva política para cada usuario.	
Cree una política de IAM para conceder permisos al rol de indexación de Lambda para acceder a Amazon S3.	Ejecute el comando create-policy en la CLI de AWS para conceder permiso a la función de índice de Lambda de modo que pueda acceder a los objetos en el bucket de S3: `aws iam create-policy \ --policy-name s3-permission-policy \ --policy-document file://s3_lambda_policy.json` El archivo `s3_lambda_policy.json` es el siguiente documento de política de JSON de la carpeta actual: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "s3:GetObject", "Resource": "arn:aws:s3:::tenantrawdata/*" } ] }`	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Adjunte la política al rol de ejecución de Lambda.	Ejecute el attach-role-policy comando AWS CLI para adjuntar la política creada en el paso anterior al índice Lambda y a las funciones de ejecución de búsquedas que creó anteriormente: `aws iam attach-role-policy \` `  --policy-arn arn:aws:iam::account-id:policy/assume-tenant-role-policy \` `  --role-name index-lambda-role` `aws iam attach-role-policy \` `  --policy-arn arn:aws:iam::account-id:policy/assume-tenant-role-policy \` `  --role-name search-lambda-role` `aws iam attach-role-policy \` `  --policy-arn arn:aws:iam::account-id:policy/s3-permission-policy \` `  --role-name index-lambda-role` La política ARN procede de lo obtenido en el paso anterior.	Arquitecto de la nube, administrador de la nube

Cree y configure una API de búsqueda

Tarea	Descripción	Habilidades requeridas
Cree una API de REST en API Gateway.	Ejecute el create-rest-apicomando CLI para crear un recurso de API REST: `aws apigateway create-rest-api \ --name Test-Api \ --endpoint-configuration "{ \"types\": [\"REGIONAL\"] }"` En el tipo de configuración de punto de conexión, puede especificar `EDGE` en lugar de `REGIONAL` para usar ubicaciones periféricas en lugar de una región de AWS concreta. Anote el valor del campo `id` en el resultado del comando. Esta es la ID de API que usará en los siguientes comandos.	Arquitecto de la nube, administrador de la nube
Cree un recurso para la API de búsqueda.	El recurso de la API de búsqueda inicia la función de búsqueda de Lambda con el nombre de recurso `search`. (No es necesario crear una API para la función de índice de Lambda, ya que se ejecuta automáticamente cuando se cargan objetos en el bucket de S3).	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	1. Ejecute el comando get-resources en la CLI de AWS para obtener la ID principal de la ruta raíz: `aws apigateway get-resources \ --rest-api-id <API-ID>` Observe el valor del campo ID. Usará esta ID principal en el siguiente comando. `{ "items": [ { "id": "zpsri964ck", "path": "/" } ] }` 2. Ejecute el comando create-resource en la CLI de AWS para crear un recurso para la API de búsqueda. En `parent-id` , especifique la ID del comando anterior. `aws apigateway create-resource \ --rest-api-id <API-ID> \ --parent-id <Parent-ID> \`	

Tarea	Descripción	Habilidades requeridas
	`--path-part search`	
Cree un método GET para la API de búsqueda.	Ejecute el comando put-method en la CLI de AWS para crear un método `GET` para la API de búsqueda: `aws apigateway put-method \ --rest-api-id <API-ID> \ --resource-id <ID from the previous command output> \ --http-method GET \ --authorization-type "NONE" \ --no-api-key-required` Para `resource-id`, especifique la ID de lo obtenido del comando `create-resource`.	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Cree un método de respuesta para la API de búsqueda.	Ejecute el put-method-responsecomando AWS CLI para añadir una respuesta de método para la API de búsqueda: `aws apigateway put-method-response \ --rest-api-id <API-ID> \ --resource-id <ID from the create-resource command output> \ --http-method GET \ --status-code 200 \ --response-models "{\"application/json\": \"Empty\"}"` En `resource-id` , especifique la ID del resultado del anterior comando `create-resource` .	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Configure una integración de Lambda proxy para la API de búsqueda.	Ejecute el comando put-integration en la CLI de AWS para configurar una integración con la función de búsqueda de Lambda: `aws apigateway put-integration \` `  --rest-api-id <API-ID> \` `  --resource-id  <ID from the create-resource command output> \` `  --http-method GET \` `  --type AWS_PROXY \` `  --integration-http-method GET \` `  --uri arn:aws:apigateway:region:lambda:path/2015-03-31/functions/arn:aws:lambda:<region>:<account-id>:function:<function-name>/invocations` En `resource-id` , especifique la ID del anterior comando `create-resource` .	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Otorgue permiso a API Gateway para llamar a la función de búsqueda de Lambda.	Ejecute el comando add-permission en la CLI de AWS para conceder permiso a API Gateway para usar la función de búsqueda: `aws lambda add-permission \ --function-name <function-name> \ --statement-id apigateway-get \ --action lambda:InvokeFunction \ --principal apigateway.amazonaws.com \ --source-arn "arn:aws:execute-api:<region>:<account-id>:api-id/*/GET/search"` Cambie la ruta `source-arn` si ha usado un nombre de recurso de API en lugar de `search`.	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Implemente la API de búsqueda.	Ejecute el comando create-deployment en la CLI de AWS para crear un recurso de fase denominado `dev`: `aws apigateway create-deployment \ --rest-api-id <API-ID> \ --stage-name dev` Si actualiza la API, puede usar el mismo comando de CLI para reimplementarlo de nuevo en la misma etapa.	Arquitecto de la nube, administrador de la nube

Crear y configurar roles de Kibana

Tarea	Descripción	Habilidades requeridas
Inicie sesión en la consola Kibana.	1. Encuentra el enlace a Kibana en el panel de control de tu dominio en la consola de Amazon OpenSearch Service. La URL tiene el formato: `<domain-endpoint>/_plugin/kibana/` . 2. Use el host bastión que configuró en la primera épica para acceder a la consola de Kibana. 3. Inicia sesión en la consola de Kibana con el nombre	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	de usuario y la contraseña maestros del paso anterior, cuando creaste el dominio de Amazon OpenSearch Service. 4. Cuando se le pida que seleccione un usuario, elija Privado.	

Tarea	Descripción	Habilidades requeridas
Cree y configure roles de Kibana.	Para aislar los datos y garantizar que un usuario no pueda recuperar los datos de otro, debe proteger los documentos con seguridad . Así, los usuarios podrán acceder únicamente a aquellos documentos que contienen su ID de usuario. 1. En la consola Kibana, en el panel de navegación, seleccione Seguridad, Rol. 2. Cree un nuevo rol de usuario. 3. Establece los permisos de clúster en`indices_all` , lo que otorga permisos de creación, lectura, actualización y eliminación (CRUD) en el índice de Amazon OpenSearch Service. 4. Restrinja los permisos de indexación al índice `tenant-data` . (El nombre del índice debe coincidir con el nombre de las funciones de búsqueda e indexación de Lambda). 5. Defina los permisos de indexación en `indices_all` para que los usuarios puedan realizar todas las operaciones relacionadas	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	con la indexación. (Puede restringir las operaciones para brindar un acceso más detallado en función de sus necesidades). 6. Para garantizar la seguridad a nivel de documento, use la siguiente política para filtrar los documentos por ID de usuario, a fin de aislar los datos de los usuarios en un índice compartido: `{ "bool": { "must": { "match": { "TenantId": "Tenant-1" } } } }` El nombre del índice, las propiedades y los valores distinguen entre mayúsculas y minúsculas.	

Tarea	Descripción	Habilidades requeridas
Asigne usuarios a los roles.	1. Seleccione la pestaña Usuarios asignados para el rol y, a continuación, elija Asignar usuarios. 2. En la sección Roles de backend, especifique el ARN del rol de usuario de IAM que creó anteriorm ente y, a continuación, elija Asignar. Se asignará el rol de usuario de IAM al rol de Kibana para que la búsqueda específica del usuario arroje datos únicamente de ese usuario. Por ejemplo, si el nombre del rol de IAM del Usuario-1 es `Tenant-1-Role` , especifique el ARN de `Tenant-1-Role` (de la épica Crear y configura r roles de usuario) en la casilla Roles de backend para el rol Usuario-1 de Kibana. 3. Repita los pasos 1 y 2 para Usuario-2. Le recomendamos que automatice la creación de los roles de usuario y roles de Kibana en el momento de la incorporación del usuario.	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Cree el índice de datos de usuarios.	En el panel de navegación, en Administración, seleccione Herramientas de desarrollo y, a continuación, ejecute el siguiente comando. Este comando crea el índice `tenant-data` para definir la asignación de la propiedad `TenantId`. `PUT /tenant-data` `{` `  "mappings": {` `  "properties": {` `  "TenantId":` `  { "type": "keyword"}` `  }` `  }` `}`	Arquitecto de la nube, administrador de la nube

Cree puntos de conexión de VPC para Amazon S3 y AWS STS

Tarea	Descripción	Habilidades requeridas
Crear un punto de conexión de VPC para Amazon S3 .	Ejecute el create-vpc-endpoint comando AWS CLI para crear un punto de enlace de VPC para Amazon S3. El punto de conexión permite que la función de índice de Lambda de la VPC acceda al servicio Amazon S3. `aws ec2 create-vpc-endpoint \`	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	`--vpc-id <VPC-ID> \ --service-name com.amazonaws.us-east-1.s3 \ --route-table-ids <route-table-ID>` En `vpc-id`, especifique la VPC que está usando para la función de índice de Lambda. En `service-name`, use la URL correcta del punto de conexión Amazon S3. En `route-table-ids`, especifique la tabla de enrutamiento asociada al punto de conexión de VPC.	

Tarea	Descripción	Habilidades requeridas
Crear un punto de conexión de VPC para AWS STS.	Ejecute el create-vpc-endpoint comando AWS CLI para crear un punto de enlace de VPC para AWS Security Token Service (AWS STS). El punto de conexión permite que las funciones de índice y búsqueda de Lambda en la VPC accedan al servicio AWS STS. Las funciones usan AWS STS cuando asumen el rol de IAM. `aws ec2 create-vpc-endpoint \ --vpc-id <VPC-ID> \ --vpc-endpoint-type Interface \ --service-name com.amazonaws.us-east-1.sts \ --subnet-id <subnet-ID> \ --security-group-id <security-group-ID>` Para `vpc-id`, especifique la VPC que va a utilizar para las funciones de índice y búsqueda de Lambda. En `subnet-id` , proporcione la subred en la que se debe crear este punto de conexión. En `security-group-id` , especifique el grupo de seguridad al que	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	desea asociar este punto de conexión. (Puede ser el mismo que el grupo de seguridad que usa Lambda).	

Pruebe el multiusuario y el aislamiento de datos

Tarea	Descripción	Habilidades requeridas
Actualice los archivos de Python para las funciones de índice y búsqueda.	1. En el archivo `index_lambda_package.zip`, edite el archivo `lamba_index.py` para actualizar la información de ID de cuenta de AWS, región de AWS y punto de conexión de Elasticsearch. 2. En el archivo `search_lambda_package.zip`, edite el archivo `lambda_search.py` para actualizar la información de ID de cuenta de AWS, región de AWS y punto de conexión de Elasticsearch. Puedes obtener el punto de conexión de Elasticsearch desde la pestaña Descripción general de la consola de Amazon OpenSearch Service. Tiene el formato `<AWS-Regi`	Arquitecto de la nube, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	on>.es.amazonaws.com .	
Actualizar el código de Lambda.	Utilice el update-function-codecomando de la AWS CLI para actualizar el código Lambda con los cambios realizados en los archivos de Python: `aws lambda update-function-code \` `  --function-name index-lambda-function \` `  --zip-file fileb://index_lambda_package.zip` `aws lambda update-function-code \` `  --function-name search-lambda-function \` `  --zip-file fileb://search_lambda_package.zip`	Arquitecto de la nube, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Cargue los datos sin procesar en el bucket S3.	Ejecute el comando cp en la CLI de AWS para cargar los datos de los objetos Usuario-1 y Usuario-2 en el bucket `tenantrawdata` (especifi que el nombre del bucket de S3 que creó para este fin): `aws s3 cp tenant-1-data s3://tenantrawdata` `aws s3 cp tenant-2-data s3://tenantrawdata` El bucket de S3 está configura do para ejecutar la función de índice de Lambda siempre que se carguen datos, de modo que el documento se indexe en Elasticsearch.	Arquitecto de la nube, administrador de la nube
Busque datos desde la consola de Kibana.	En la consola de Kibana, ejecute la siguiente consulta: `GET tenant-data/_searc h` Esta consulta muestra todos los documentos indexados en Elasticsearch. En este caso, debería ver dos documentos separados para Usuario-1 y Usuario-2.	Arquitecto de la nube, administrador de la nube

Tarea	Descripción	Habilidades requeridas
Pruebe la API de búsqueda desde API Gateway.	1. En la consola de API Gateway, abra la API de búsqueda, elija el método `GET` en recurso de búsqueda y seleccione Probar. 2. En la ventana de prueba, introduzca la siguiente cadena de consulta (distingue entre mayúsculas y minúsculas) para la ID de usuario y, a continuación, seleccione Probar. `TenantId=Tenant-1` La función Lambda envía una consulta a Amazon OpenSearch Service que filtra el documento del inquilino en función de la seguridad a nivel de documento. El método devuelve el documento que pertenece a Usuario-1. 3. Cambie la cadena de consulta a: `TenantId=Tenant-2` Esta consulta nos devuelve el documento que pertenece al Usuario-2.	Arquitecto de la nube, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	Para ver una ilustración de la pantalla, consulte la sección de Información adicional.	

Recursos relacionados

- AWS SDK para Python (Boto3)
- Documentación de AWS Lambda
- Documentación de Amazon API Gateway
- Documentación de Amazon S3
- Documentación OpenSearch de Amazon Service
  - Control de acceso detallado en Amazon Service OpenSearch
  - Creación de una aplicación de búsqueda con Amazon OpenSearch Service
  - Lanzamiento de tus dominios OpenSearch de Amazon Service dentro de una VPC

Información adicional

Modelos de particionamiento de datos

Hay tres modelos comunes de particionamiento de datos que se emplean en los sistemas multiusuario: silos, agrupados e híbridos. El modelo que elija dependerá de las necesidades de cumplimiento, ruido, operaciones y aislamiento de su entorno.

Modelo de silo

En el modelo de silo, los datos de cada usuario se almacenan en un área de almacenamiento distinta, por lo que los datos de los usuarios no se mezclan. Puedes usar dos enfoques para implementar el modelo de silo con Amazon OpenSearch Service: dominio por inquilino e índice por inquilino.

- Dominio por inquilino: puedes usar un dominio de Amazon OpenSearch Service independiente (sinónimo de un clúster de Elasticsearch) por inquilino. Tener a cada usuario en su propio dominio proporciona todos los beneficios de tener los datos en un constructo independiente. Sin embargo, este enfoque presenta desafíos de gestión y agilidad. Su naturaleza distribuida dificulta

la agregación y la evaluación del estado operativo y la actividad de los usuarios. Se trata de una opción costosa que requiere que cada dominio de Amazon OpenSearch Service tenga como mínimo tres nodos maestros y dos nodos de datos para las cargas de trabajo de producción.

- Índice por inquilino: puedes colocar los datos del inquilino en índices separados dentro de un clúster de Amazon OpenSearch Service. Con este enfoque, se usa un identificador de usuario al crear y asignar un nombre al índice, anteponiendo el identificador de usuario al nombre del índice. El enfoque de índice por usuario le ayuda a alcanzar sus objetivos de compartimentación sin tener que introducir un clúster completamente separado para cada usuario. Sin embargo, si aumenta el número de índices, es posible que la memoria se agote, ya que este enfoque requiere más particiones y el nodo maestro tiene que gestionar una mayor asignación y reequilibrio.

Modelo de aislamiento en silo: en el modelo de silo, se emplean políticas de IAM para aislar los dominios o índices que contienen los datos de cada usuario. Estas políticas impiden que un usuario acceda a los datos de otro. Para implementar su modelo de aislamiento en silos, puede crear una política basada en recursos que controle el acceso al recurso de su usuario. Esta suele ser una política de acceso al dominio que especifica qué acciones puede realizar una entidad principal en los subrecursos del dominio, incluidos los índices y las API de Elasticsearch. Con las políticas de IAM basadas en la identidad, puedes especificar las acciones permitidas o denegadas en el dominio, los índices o las API de Amazon Service. OpenSearch El elemento `Action` de una política de IAM describe la acción o acciones específicas permitidas y denegadas por la política. El elemento `Principal` especifica las cuentas, usuarios o roles afectados.

El siguiente ejemplo de política otorga a Usuario-1 acceso total (según lo especificado en `es:*`) únicamente a los subrecursos del dominio `tenant-1`. El `/*` de seguimiento en el elemento `Resource` indica que esta política se aplica a los sub-recursos del dominio, no al dominio en sí. Cuando esta política esté en vigor, los usuarios no podrán crear un dominio nuevo ni modificar la configuración de un dominio existente.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
```

```
         "Principal": {
            "AWS": "arn:aws:iam::aws-account-id:user/Tenant-1"
         },
         "Action": "es:*",
         "Resource": "arn:aws:es:Region:account-id:domain/tenant-1/*"
      }
   ]
}
```

Para implementar el modelo de silo de índice por usuario, tendrá que modificar este ejemplo de política para restringir aún más a Usuario-1 al índice o índices especificados, indicando el nombre del índice. El siguiente ejemplo de política restringe a Usuario-1 al índice `tenant-index-1`.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::123456789012:user/Tenant-1"
         },
         "Action": "es:*",
         "Resource": "arn:aws:es:Region:account-id:domain/test-domain/tenant-index-1/*"
      }
   ]
}
```

Modelo de grupo

En el modelo de grupo, todos los datos de los usuarios se almacenan en un índice dentro del mismo dominio. El identificador del usuario se incluye en los datos (documento) y se usa como clave de partición, de modo que puede determinar qué datos pertenecen a cada usuario. Este modelo reduce la sobrecarga de administración. Operar y administrar un índice agrupado es más fácil y eficiente que administrar varios índices. Sin embargo, dado que los datos de los usuarios están mezclados en el mismo índice, se pierde el aislamiento natural de los usuarios que proporciona el modelo de silos. Este enfoque también podría reducir el rendimiento debido al efecto de ruido aledaño.

Aislamiento de usuarios en el modelo de grupo: en general, el aislamiento de usuarios es difícil de implementar en el modelo de grupo. El mecanismo de IAM usado con el modelo de silo no permite describir el aislamiento en función del identificador de usuario almacenado en el documento.

Un enfoque alternativo consiste en usar el control de acceso detallado (FGAC) que proporciona Open Distro para Elasticsearch. El FGAC permite controlar los permisos a nivel de índice, documento o campo. En cada solicitud, el FGAC evalúa las credenciales del usuario y autentica o deniega el acceso. Si el FGAC autentica al usuario, obtiene todos los roles mapeados a ese usuario y utiliza el conjunto completo de permisos para determinar cómo gestionar la solicitud.

Para lograr el aislamiento requerido en el modelo agrupado, puede usar seguridad a nivel de documento, que le permite restringir un rol a un subconjunto de documentos de un índice. El siguiente ejemplo de rol restringe las consultas a Usuario-1. Al aplicar este rol a Usuario-1, puede lograr el aislamiento necesario.

```
{
   "bool": {
     "must": {
       "match": {
         "tenantId": "Tenant-1"
       }
     }
   }
 }
```

Modelo híbrido

El modelo híbrido emplea una combinación de los modelos de silo y grupo en el mismo entorno para ofrecer experiencias únicas a cada nivel de usuario (como los niveles gratuito, estándar y prémium). Cada nivel sigue el mismo perfil de seguridad que se usó en el modelo de grupo.

Aislamiento de usuarios en el modelo híbrido: en el modelo híbrido, se sigue el mismo perfil de seguridad que en el modelo de grupo. El uso del modelo de seguridad FGAC a nivel de documento proporciona aislamiento a los usuarios. Si bien esta estrategia simplifica la administración de clústeres y ofrece agilidad, complica otros aspectos de la arquitectura. Por ejemplo, el código requiere una complejidad adicional para determinar qué modelo está asociado a cada usuario. También deberá asegurarse de que las consultas de un solo usuario no saturen todo el dominio ni degraden la experiencia de otros usuarios.

Pruebas en API Gateway

Ventana de prueba para consulta de Usuario-1

Ventana de prueba para consulta de Usuario-2

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Implemente aplicaciones de varias pilas mediante AWS CDK con TypeScript

Creado por el Dr. Rahul Sharad Gaikwad (AWS)

Entorno: producción	Tecnologías: modernización; migración; DevOps	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon API Gateway; AWS Lambda; Amazon Kinesis		

Resumen

Este patrón proporciona un step-by-step enfoque para la implementación de aplicaciones en Amazon Web Services (AWS) mediante el AWS Cloud Development Kit (AWS CDK) con TypeScript. Por ejemplo, el patrón implementa una aplicación de análisis en tiempo real sin servidor.

El patrón crea e implementa aplicaciones de pila anidada. La CloudFormation pila de AWS principal llama a las pilas secundarias o anidadas. Cada pila secundaria crea e implementa los recursos de AWS que se definen en la CloudFormation pila. AWS CDK Toolkit, el comando de la interfaz de línea de comandos (CLI)`cdk`, es la interfaz principal de las CloudFormation pilas.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una nube privada virtual (VPC) y subredes existentes
- Kit de herramientas de AWS CDK instalado y configurado
- Un usuario con permisos de administrador y un conjunto de claves de acceso.
- Node.js
- Interfaz de la línea de comandos de AWS (AWS CLI)

Limitaciones

- Como la CDK de AWS utiliza AWS CloudFormation, las aplicaciones de la CDK de AWS están sujetas a cuotas de CloudFormation servicio. Para obtener más información, consulte CloudFormation Cuotas de AWS.

Versiones de producto

Este patrón se ha creado y probado usando las siguientes herramientas y versiones.

- Kit de herramientas de AWS CDK 1.83.0
- Node.js 14.13.0
- npm 7.0.14

El patrón debería funcionar con cualquier versión de AWS CDK o npm. Tenga en cuenta que las versiones 13.0.0 a 13.6.0 de Node.js no son compatibles con AWS CDK.

Arquitectura

Pila de tecnología de destino

- Consola de AWS Amplify
- Amazon API Gateway
- AWS CDK
- Amazon CloudFront
- Amazon Cognito
- Amazon DynamoDB
- Amazon Data Firehose
- Amazon Kinesis Data Streams
- AWS Lambda
- Amazon Simple Storage Service (Amazon S3)

Arquitectura de destino

En el siguiente diagrama se muestra la implementación de aplicaciones de varias pilas mediante AWS CDK con. TypeScript

En el siguiente diagrama se muestra la arquitectura de la aplicación en tiempo real sin servidor de ejemplo.

Herramientas

Herramientas

- La Consola de AWS Amplify es el centro de control para las implementaciones de aplicaciones web y móviles de pila completa en AWS. El alojamiento de la consola de Amplify proporciona un flujo de trabajo basado en Git para alojar aplicaciones web sin servidor de pila completa con implementación continua. La interfaz de usuario de administración es una interfaz visual para que los desarrolladores de frontend web y móvil puedan crear y administrar el backend de aplicaciones fuera de la Consola de AWS.
- Amazon API Gateway es un servicio de AWS para crear, publicar, mantener, supervisar y proteger REST, HTTP y WebSocket API a cualquier escala.
- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura de la nube de AWS en código.
- El Kit de herramientas de AWS CDK es un kit de desarrollo en la nube de línea de comandos que le ayuda a interactuar con su aplicación AWS CDK. El comando `cdk` de la CLI es la herramienta principal para interactuar con su aplicación AWS CDK. Ejecuta su aplicación, interroga el modelo de aplicación que ha definido y produce e implementa las CloudFormation plantillas de AWS generadas por la CDK de AWS.
- Amazon CloudFront es un servicio web que acelera la distribución de contenido web estático y dinámico, como .html, .css, .js y archivos de imagen. CloudFront entrega su contenido a través de una red mundial de centros de datos denominados ubicaciones perimetrales para reducir la latencia y mejorar el rendimiento.
- Amazon Cognito ofrece autenticación, autorización y administración de usuarios para sus aplicaciones móviles y web. Sus usuarios pueden iniciar sesión directamente o a través de un tercero.
- Amazon DynamoDB es un servicio de base de datos NoSQL totalmente administrado que ofrece un rendimiento rápido y predecible, así como una perfecta escalabilidad.
- Amazon Data Firehose es un servicio totalmente gestionado para entregar datos de streaming en tiempo real a destinos como Amazon S3, Amazon Redshift, OpenSearch Amazon Service,

Splunk y cualquier punto de enlace HTTP personalizado o punto de enlace HTTP propiedad de proveedores de servicios externos compatibles.

- Amazon Kinesis Data Streams es un servicio que permite recopilar y procesar grandes flujos de registros de datos en tiempo real.
- AWS Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo. Solo pagará por el tiempo de computación que consuma, no se aplican cargos cuando el código no se está ejecutando.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Código

Se adjunta el código de este patrón.

Epics

Instalación del kit de herramientas de AWS CDK

Tarea	Descripción	Habilidades requeridas
Instale el kit de herramientas de AWS CDK.	Para instalar el kit de herramientas de AWS CDK a nivel global, ejecute el siguiente comando. `npm install -g aws-cdk`	DevOps
Verificar la versión.	Para verificar la versión del kit de herramientas de AWS CDK, ejecute el siguiente comando. `cdk --version`	DevOps

Configuración de las credenciales de AWS

Tarea	Descripción	Habilidades requeridas
Configurar las credenciales.	Para configurar las credencia les, ejecute el comando `aws configure` y siga las instrucciones. `$aws configure` `AWS Access Key ID` `[None]:` `AWS Secret Access Key` `[None]: your_secr` `et_access_key` `Default region name` `[None]:` `Default output format` `[None]:`	DevOps

Descarga del código del proyecto

Tarea	Descripción	Habilidades requeridas
Descargar el código del proyecto adjunto.	Para obtener más informaci ón sobre la estructura de los directorios y archivos, consulte la sección Informaci ón adicional.	DevOps

Inicie el entorno de AWS CDK

Tarea	Descripción	Habilidades requeridas
Inicie el entorno.	Para implementar la CloudFormation plantilla de AWS en la cuenta y la región	DevOps

Tarea	Descripción	Habilidades requeridas
	de AWS que desee usar, ejecute el siguiente comando. `cdk bootstrap <account>/<Region>` Para obtener más información, consulte la documentación de AWS.	

Crear e implementar el proyecto

Tarea	Descripción	Habilidades requeridas
Compilar el proyecto.	Para compilar el código del proyecto, ejecute el comando `npm run build`.	DevOps
Implementar el proyecto.	Para implementar el código del proyecto, ejecute el comando `cdk deploy`.	

Verificación de resultados

Tarea	Descripción	Habilidades requeridas
Verificar la creación de la pila.	En la consola de administración de AWS, elija CloudFormation. En las pilas del proyecto, verifique que se hayan creado una pila principal y dos pilas secundarias.	DevOps

Pruebe la aplicación

Tarea	Descripción	Habilidades requeridas
Enviar datos a Kinesis Data Streams.	Configure su cuenta de AWS para enviar datos a Kinesis Data Streams mediante Amazon Kinesis Data Generator (KDG). Para obtener más información, consulte Amazon Kinesis Data Generator.	DevOps
Crear un usuario de Amazon Cognito.	Para crear un usuario de Amazon Cognito, descargue la plantilla cognito-setup.json de la sección Crear un usuario de Amazon Cognito de CloudFormation la página de ayuda de Kinesis Data Generator. Inicie la plantilla y, a continuación, introduzc a su nombre de usuario y contraseña de Amazon Cognito. La pestaña Salidas muestra la URL de Kinesis Data Generator.	DevOps
Inicio de sesión en Kinesis Data Generator	Para iniciar sesión en KDG, utilice las credenciales de Amazon Cognito que ha introducido y la URL de Kinesis Data Generator.	DevOps
Probar la aplicación.	En KDG, en Plantilla de registro, Plantilla 1, pegue	DevOps

Tarea	Descripción	Habilidades requeridas
	el código de prueba de la sección Información adicional y seleccione Enviar datos.	
Probar API Gateway.	Una vez incorporados los datos, pruebe API Gateway mediante el método `GET` para recuperar los datos.	DevOps

Recursos relacionados

Referencias

- AWS Cloud Development Kit
- AWS CDK en GitHub
- Uso de pilas anidadas
- Ejemplo de muestra de AWS: análisis en tiempo real sin servidor

Información adicional

Detalles del directorio y el archivo

Este patrón configura las tres siguientes pilas.

- `parent-cdk-stack.ts`: esta pila actúa como pila principal y llama a las dos aplicaciones secundarias como pilas anidadas.
- `real-time-analytics-poc-stack.ts`: esta pila anidada contiene la infraestructura y el código de la aplicación.
- `real-time-analytics-web-stack.ts`: esta pila anidada contiene únicamente el código estático de la aplicación web.

Archivos importantes y su funcionalidad

- `bin/real-time-analytics-poc.ts`: punto de entrada de la aplicación AWS CDK. Carga todas las pilas definidas en `lib/`.
- `lib/real-time-analytics-poc-stack.ts`: definición de la pila de la aplicación AWS CDK (`real-time-analytics-poc`).
- `lib/real-time-analytics-web-stack.ts`: definición de la pila de la aplicación AWS CDK (`real-time-analytics-web-stack`).
- `lib/parent-cdk-stack.ts`: definición de la pila de la aplicación AWS CDK (`parent-cdk`).
- `package.json`: manifiesto del módulo npm, que incluye el nombre, la versión y las dependencias de la aplicación.
- `package-lock.json`: mantenimiento por parte de npm.
- `cdk.json`: kit de herramientas para ejecutar la aplicación.
- `tsconfig.json`— La TypeScript configuración del proyecto.
- `.gitignore`: lista de archivos que Git debe excluir del control de código de origen.
- `node_modules`: mantenimiento por parte de npm; incluye las dependencias del proyecto.

La siguiente sección de código de la pila principal llama a las aplicaciones secundarias como pilas anidadas de AWS CDK.

```
import * as cdk from '@aws-cdk/core';
import { Construct, Stack, StackProps } from '@aws-cdk/core';
import { RealTimeAnalyticsPocStack } from './real-time-analytics-poc-stack';
import { RealTimeAnalyticsWebStack } from './real-time-analytics-web-stack';


export class CdkParentStack extends Stack {
  constructor(scope: Construct, id: string, props?: StackProps) {
    super(scope, id, props);


    new RealTimeAnalyticsPocStack(this, 'RealTimeAnalyticsPocStack');
    new RealTimeAnalyticsWebStack(this, 'RealTimeAnalyticsWebStack');
  }
}
```

Código para realizar pruebas

```
session={{date.now('YYYYMMDD')}}|sequence={{date.now('x')}}|
reception={{date.now('x')}}|instrument={{random.number(9)}}|
l={{random.number(20)}}|price_0={{random.number({"min":10000,
 "max":30000})}}|price_1={{random.number({"min":10000, "max":30000})}}|
price_2={{random.number({"min":10000, "max":30000})}}|
price_3={{random.number({"min":10000, "max":30000})}}|
price_4={{random.number({"min":10000, "max":30000})}}|
price_5={{random.number({"min":10000, "max":30000})}}|
price_6={{random.number({"min":10000, "max":30000})}}|
price_7={{random.number({"min":10000, "max":30000})}}|
price_8={{random.number({"min":10000, "max":30000})}}|
```

Pruebas de API Gateway

En la consola de API Gateway, pruebe API Gateway mediante el método `GET`.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Automatice la implementación de aplicaciones anidadas mediante SAM de AWS

Creado por Dr. Rahul Sharad Gaikwad (AWS), Dmitry Gulin (AWS), Ishwar Chaauthaiwale (AWS) y Tabby Ward (AWS)

Repositorio de código: - sample aws-sam-nested-stack	Entorno: PoC o piloto	Tecnologías: modernización; sin servidor; DevOps
Carga de trabajo: todas las demás cargas de trabajo	Servicios de AWS: Repositorio de aplicaciones sin servidor de AWS	

Resumen

En Amazon Web Services (AWS), el AWS Serverless Application Model (AWS SAM) es un marco de código abierto que proporciona una sintaxis abreviada para expresar funciones, API, bases de datos y asignaciones de orígenes de eventos. Con solo unas pocas líneas para cada recurso, puede definir la aplicación que desee y modelarla mediante YAML. Durante la implementación, SAM transforma y expande la sintaxis de SAM en una CloudFormation sintaxis de AWS que puede usar para crear aplicaciones sin servidor con mayor rapidez.

SAM de AWS simplifica el desarrollo, la implementación y la administración de aplicaciones sin servidor en la plataforma AWS. Proporciona un marco estandarizado, una implementación más rápida, capacidades de pruebas locales, administración de recursos, una integración perfecta con las herramientas de desarrollo y una comunidad de apoyo. Estas características lo convierten en una herramienta valiosa para crear aplicaciones sin servidor de manera eficiente y eficaz.

Este patrón utiliza plantillas SAM de AWS para automatizar la implementación de aplicaciones anidadas. Una aplicación anidada es una aplicación dentro de otra aplicación. Las aplicaciones principales llaman a las aplicaciones secundarias. Se trata de componentes con acoplamiento flexible de una arquitectura sin servidor.

Con aplicaciones anidadas, puede crear rápidamente arquitecturas sin servidor altamente sofisticadas mediante la reutilización de servicios o componentes que se crean y mantienen de forma independiente, pero que se componen con SAM de AWS y Repositorio de aplicaciones

sin servidor. Las aplicaciones anidadas le ayudan a crear aplicaciones más potentes, evitar la duplicación del trabajo y garantizar la coherencia y las prácticas recomendadas en todos sus equipos y organizaciones. Para mostrar las aplicaciones anidadas, el patrón implementa un ejemplo de aplicación de carrito de compras sin servidor de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una nube privada virtual (VPC) y subredes existentes
- Un entorno de desarrollo integrado, como AWS Cloud9 o Visual Studio Code (para obtener más información, consulte Herramientas para crear en AWS)
- Biblioteca de ruedas de Python instalada con pip install wheel, si aún no está instalada

Limitaciones

- El número máximo de aplicaciones que se pueden anidar en una aplicación sin servidor es de 200.
- El número máximo de parámetros que puede tener una aplicación anidada es 60.

Versiones de producto

- Esta solución se basa en la versión 1.21.1 de la interfaz de la línea de comandos de SAM de AWS (CLI de SAM de AWS), pero esta arquitectura debería funcionar con versiones posteriores de la CLI de SAM de AWS.

Arquitectura

Pila de tecnología de destino

- Amazon API Gateway
- SAM de AWS
- Amazon Cognito
- Amazon DynamoDB
- AWS Lambda
- Cola de Amazon Simple Queue Service (Amazon SQS)

Arquitectura de destino

El siguiente diagrama muestra cómo se realizan las solicitudes de los usuarios a los servicios de compras mediante llamadas a las API. La solicitud del usuario, incluida toda la información necesaria, se envía a Amazon API Gateway y al autorizador de Amazon Cognito, que ejecuta los mecanismos de autenticación y autorización de las API.

Cuando se agrega, elimina o actualiza un elemento en DynamoDB, se coloca un evento en DynamoDB Streams, que a su vez inicia una función de Lambda. Para evitar la eliminación inmediata de elementos antiguos como parte de un flujo de trabajo sincrónico, los mensajes se colocan en una cola de SQS, lo que inicia una función de trabajo para eliminarlos.

En esta configuración de solución, la CLI de AWS SAM sirve de interfaz para las CloudFormation pilas de AWS. Las plantillas SAM de AWS implementan automáticamente aplicaciones anidadas. La plantilla SAM principal llama a las plantillas secundarias y la CloudFormation pila principal implementa las pilas secundarias. Cada pila secundaria crea los recursos de AWS que se definen en las CloudFormation plantillas de AWS SAM.

1. Genere e implemente las pilas.
2. La CloudFormation pila de autenticación contiene Amazon Cognito.
3. La CloudFormation pila de productos contiene una función Lambda y Amazon API Gateway
4. La CloudFormation pila de compras contiene una función Lambda, Amazon API Gateway, la cola SQS y la base de datos Amazon DynamoDB.

Herramientas

Herramientas

- Amazon API Gateway le ayuda a crear, publicar, mantener, supervisar y proteger REST, HTTP y WebSocket API a cualquier escala.
- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- Amazon Cognito ofrece autenticación, autorización y administración de usuarios para aplicaciones móviles y web.

- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Serverless Application Model (AWS SAM) es un marco de código abierto que permite crear aplicaciones sin servidor en la nube de AWS.
- Amazon Simple Queue Service (Amazon SQS) ofrece una cola alojada segura, duradera y disponible que le permite integrar y desacoplar sistemas y componentes de software distribuidos.

Código

El código de este patrón está disponible en el repositorio de muestras de GitHub AWS SAM Nested Stack.

Epics

Instalar la CLI de SAM de AWS

Tarea	Descripción	Habilidades requeridas
Instalar la CLI de SAM de AWS.	Para instalar la CLI de SAM de AWS, siga las instrucciones de la documentación de SAM de AWS.	DevOps ingeniero
Configure las credenciales de AWS.	Para configurar las credenciales de AWS para que la CLI de SAM de AWS pueda realizar llamadas a los servicios de AWS en su nombre, ejecute el comando `aws configure` y siga las instrucciones. `$aws configure`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`AWS Access Key ID [None]: <your_access_key_id>` `AWS Secret Access Key [None]: your_secret_access_key` `Default region name [None]:` `Default output format [None]:` Para obtener más información sobre cómo configurar sus credenciales, consulte credenciales de autenticación y acceso.	

Inicie el proyecto SAM de AWS

Tarea	Descripción	Habilidades requeridas
Clone el repositorio de código de SAM de AWS.	1. Introduzca el siguiente comando para clonar el repositorio de pilas de muestras anidadas de AWS para este patrón. `git clone https://github.com/aws-samples/aws-sam-nested-stack-sample.git` 2. Acceda al directorio clonado ejecutando el siguiente comando.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`cd aws-sam-nested-stack-sample`	
Implemente plantillas para iniciar el proyecto.	Ejecute el comando `SAM init` para iniciar el proyecto. Cuando se le pida que elija una fuente de plantilla, elija `Custom Template Location`.	DevOps ingeniero

Compile y cree el código de la plantilla SAM

Tarea	Descripción	Habilidades requeridas
Revise las plantillas de aplicaciones SAM de AWS.	Revise las plantillas de las aplicaciones anidadas. En este ejemplo se utilizan las siguientes plantillas de aplicaciones anidadas: • `auth.yaml` : esta plantilla configura los recursos relacionados con la autenticación, como Amazon Cognito y Almacén de parámetros de AWS Systems Manager. • `product-mock.yaml` : esta plantilla implement a recursos relacionados con el producto, como las funciones de Lambda y Amazon API Gateway.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	• `shoppingcart-service.yaml` : esta plantilla configura los recursos relacionados con los carritos de compras, como AWS Identity and Access Management (IAM), tablas de DynamoDB y funciones de Lambda.	
Revise la plantilla principal.	Revise la plantilla que invocará las plantillas de aplicación anidadas. En este ejemplo, la plantilla principal es `template.yml` . Todas las aplicaciones independientes están anidadas en la plantilla principal única `template.yml` .	DevOps ingeniero
Compile y cree el código de la plantilla SAM de AWS.	Ejecute el siguiente comando utilizando la CLI de SAM de AWS. `sam build`	DevOps ingeniero

Implemente la plantilla SAM de AWS

Tarea	Descripción	Habilidades requeridas
Implemente las aplicaciones.	Para lanzar el código de plantilla SAM que crea las CloudFormation pilas de aplicaciones anidadas y despliega el código en el	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	entorno de AWS, ejecute el siguiente comando. `sam deploy --guided --stack-name shopping-cart-nested-stack --capabilities CAPABILITY_IAM CAPABILITY_AUTO_EXPAND` El comando aparecerá con algunas preguntas. Responda a todas las preguntas con y.	

Verifique la implementación

Tarea	Descripción	Habilidades requeridas
Verifique las pilas.	Para revisar las CloudFormation pilas de AWS y los recursos de AWS que se definieron en las plantillas de AWS SAM, haga lo siguiente: 1. Inicie sesión en la consola de administración de AWS y navegue hasta la CloudFormationconsola. 2. Compruebe que las pilas principal y secundaria estén en la lista. En este ejemplo, `sam-shopping-cart` es la pila principal que llama a	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	las pilas anidadas de Auth, Product y Shopping. La pila de productos proporciona el enlace URL de Product API Gateway como salida.	

Recursos relacionados

Referencias

- AWS Serverless Application Model (AWS SAM)
- AWS SAM en GitHub
- Microservicio de carrito de compras sin servidor (ejemplo de aplicación de AWS)

Tutoriales y videos

- Cree una aplicación sin servidor
- Charlas técnicas online de AWS: creación e implementación de aplicaciones sin servidor con SAM de AWS

Información adicional

Una vez colocado todo el código, el ejemplo tiene la siguiente estructura de directorios:

- sam_stacks: esta carpeta contiene la capa `shared.py`. Una capa es un archivo que contiene bibliotecas, un tiempo de ejecución personalizado u otras dependencias. Con las capas, puede utilizar las bibliotecas en la función sin necesidad de incluirlas en el paquete de implementación.
- product-mock-service— Esta carpeta contiene todos los archivos y funciones de Lambda relacionados con el producto.
- shopping-cart-service— Esta carpeta contiene todas las funciones y archivos de Lambda relacionados con las compras.

Implemente el aislamiento de usuarios de SaaS para Amazon S3 mediante una máquina expendedora de tokens de AWS Lambda

Creado por Tabby Ward (AWS), Sravan Periyathambi (AWS) y Thomas Davis (AWS)

Entorno: PoC o piloto	Tecnologías: modernización; SaaS	Servicios de AWS: AWS Identity and Access Management; AWS Lambda; Amazon S3; AWS STS

Resumen

Las aplicaciones SaaS multiusuario deben implementar sistemas para garantizar que se mantenga el aislamiento de los usuarios. Cuando almacena datos de usuarios en un mismo recurso de Amazon Web Services (AWS) (por ejemplo, varios usuarios almacenan datos en un mismo bucket de Amazon Simple Storage Service (Amazon S3), debe asegurarse de impedir el acceso cruzado de los usuarios. Las máquinas expendedoras de tokens (TVM) permiten aislar los datos de los usuarios. Estas máquinas proporcionan un mecanismo para obtener tokens y, al mismo tiempo, simplifican la complejidad inherente a la creación de dichos tokens. Los desarrolladores pueden usar una TVM sin tener un conocimiento detallado de cómo la máquina produce los tokens.

Este patrón implementa una TVM mediante AWS Lambda. La TVM genera un token con credenciales del servicio de token de seguridad (STS) temporales que limitan el acceso a los datos de un único usuario de SaaS en un bucket de S3.

Las TVM, y el código que se proporciona con este patrón, suelen usarse con afirmaciones derivadas de los JSON Web Tokens (JWT) para asociar las solicitudes de recursos de AWS a una política de AWS Identity and Access Management (IAM) dirigida a los usuarios. Puede usar el código de este patrón como base para implementar una aplicación SaaS que genere credenciales STS temporales y limitadas en función de las afirmaciones proporcionadas en un token JWT.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.

- Interfaz de la línea de comandos de AWS (AWS CLI) versión 1.19.0 o posterior, instalada y configurada en macOS, Linux, o Windows. Como alternativa, puede usar la versión 2.1 o posterior de la CLI de AWS.

Limitaciones

- Este código se ejecuta en Java y, actualmente, no es compatible con otros lenguajes de programación.
- La aplicación de muestra no incluye soporte multirregional ni de recuperación de desastres (DR) de AWS.
- Este patrón demuestra cómo puede proporcionar acceso limitado a los usuarios una TVM de Lambda para una aplicación SaaS. No está diseñado para usarse en entornos de producción.

Arquitectura

Pila de tecnología de destino

- AWS Lambda
- Amazon S3
- IAM
- AWS Security Token Service (AWS STS)

Arquitectura de destino

Herramientas

Servicios de AWS

- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que permite interactuar con los servicios de AWS mediante comandos en el intérprete de comandos de línea de comandos.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.

- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Security Token Service (AWS STS) le ayuda a solicitar credenciales temporales con privilegios limitados para los usuarios.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Código

El código fuente de este patrón está disponible como archivo adjunto, e incluye los siguientes archivos:

- `s3UploadSample.jar` proporciona el código fuente de una función de Lambda que carga un documento JSON en un bucket de S3.
- `tvm-layer.zip` proporciona una biblioteca Java reutilizable que suministra un token (credenciales temporales de STS) para que la función de Lambda acceda al bucket de S3 y cargue el documento JSON.
- `token-vending-machine-sample-app.zip` proporciona el código fuente usado para crear estos artefactos y las instrucciones de compilación.

Para usar el código de muestra, siga los pasos de la siguiente sección.

Epics

Determine los valores de las variables

Tarea	Descripción	Habilidades requeridas
Determine los valores de las variables.	La implementación de este patrón incluye varios nombres de variables que deben usarse de manera coherente . Determine los valores a usar para cada variable y proporcio	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	ne cada valor cuando se le solicite en los siguientes pasos. <AWS Account ID> – La ID de 12 dígitos asociada a la cuenta de AWS en la que está implementando este patrón. Para obtener información acerca de cómo encontrar su ID de su cuenta AWS, consulte su ID de cuenta AWS y alias en la documentación de IAM. <AWS Region> – La región de AWS en la que está implementando este patrón. Para obtener más información sobre las regiones de AWS, consulte Regiones y zonas de disponibilidad en la web de AWS. < sample-tenant-name > – El nombre del inquilino que se utilizará en la solicitud. Le recomendamos que introduzca únicamente caracteres alfanuméricos en este valor por motivos de simplicidad, pero puede usar cualquier nombre válido para una clave de objeto de S3.	

Tarea	Descripción	Habilidades requeridas
	< sample-tvm-role-name > – El nombre de la función de IAM asociada a la función Lambda que ejecuta la TVM y la aplicación de ejemplo. El nombre del rol es una cadena compuesta por caracteres alfanuméricos en mayúscula y minúscula sin espacios. También puede incluir los siguientes caracteres: guion bajo (_), signo más (+), signo igual (=), coma (,), punto (.), arroba (@) y guion (-). El nombre del rol debe ser único dentro de la cuenta. < sample-app-role-name > – El nombre de la función de IAM que asume la función Lambda cuando genera credenciales STS temporale s y con ámbito específico. El nombre del rol es una cadena compuesta por caracteres alfanuméricos en mayúscula y minúscula sin espacios. También puede incluir los siguientes caracteres: guion bajo (_), signo más (+), signo igual (=), coma (,), punto (.), arroba (@) y guion (-). El nombre del rol debe ser único dentro de la cuenta.	

Tarea	Descripción	Habilidades requeridas
	< sample-app-function-name > – El nombre de la función Lambda. Es una cadena de hasta 64 caracteres de longitud. < sample-app-bucket-name > – El nombre de un bucket de S3 al que se debe acceder con permisos que estén sujetos a un inquilino específico. Nombre del bucket de S3: • Deben tener entre 3 y 63 caracteres de longitud. • Deben contener solo letras minúsculas, números, puntos (.) y guiones (-). • Deben comenzar y terminar por una letra o un número. • No pueden tener el formato de una dirección IP (por ejemplo, 192.168.5.4). • Debe ser exclusivo dentro de una partición. Una partición es un grupo de regiones. Actualmente, AWS tiene tres particiones: `aws` (regiones estándar), `aws-cn` (regiones de China) y `aws-us-gov` (regiones de AWS GovCloud [EE. UU.]).	

Cree un bucket de S3

Tarea	Descripción	Habilidades requeridas
Crear un entorno de S3 para la aplicación de ejemplo.	Puede utilizar el comando AWS CLI para crear el bucket de S3. Introduzca el valor **<** sample-app-bucket-name **>** en el fragmento de código: `aws s3api create-bucket --bucket <sample-app-bucket-name>` La aplicación de ejemplo de Lambda carga archivos JSON en este bucket.	Administrador de la nube

Creación de una política y un rol de IAM TVM

Tarea	Descripción	Habilidades requeridas
Crear un rol de TVM.	Ejecute uno de los siguiente s comandos de la CLI de AWS para crear un rol de IAM. Proporcione el valor **<** sample-tvm-role-name **>** en el comando. Para los intérprete de comandos para macOS o Linux: `aws iam create-role \ --role-name <sample-tvm-role-name> \ --assume-role-policy-document '{`	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	<pre>"Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Principal": { "Service": "lambda.amazonaws.com" }, "Action": "sts:AssumeRole" }]}'</pre> En la línea de comandos de Windows: <pre>aws iam create-role ^ --role-name <sample-tvm-role-name> ^ --assume-role-policy-document "{\"Version\": \"2012-10-17\", \"Statement\": [{\"Effect\": \"Allow\", \"Principal\": {\"Service\": \"lambda.amazonaws.com\"}, \"Action\": \"sts:AssumeRole\" }]}"</pre> La aplicación de ejemplo de Lambda asume este rol cuando se invoca la aplicación. La capacidad de asumir	

Tarea	Descripción	Habilidades requeridas
	el rol de aplicación con una política específica otorga al código permisos más amplios para acceder al bucket de S3.	

Tarea	Descripción	Habilidades requeridas
Cree una política de rol de TVM en línea.	Ejecute uno de los siguientes comandos de CLI de AWS para crear una política de IAM. Proporcione los <AWS Account ID>valores < sample-tvm-role-name > y < sample-app-role-name > en el comando. Para los intérprete de comandos para macOS o Linux: `aws iam put-role-policy \` `--role-name <sample-tvm-role-name> \` `--policy-name assume-app-role \` `--policy-document '{` `"Version": "2012-10-17",` `"Statement": [` `{` `"Effect": "Allow",` `"Action": "sts:AssumeRole",` `"Resource": "arn:aws:iam::<AWS Account ID>:role/<sample-app-role-name>"` `}` `]}'` En la línea de comandos de Windows:	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	`aws iam put-role-policy ^ --role-name <sample-tvm-role-name> ^ --policy-name assume-app-role ^ --policy-document "{\"Version\": \"2012-10-17\", \"Statement\": [{\"Effect\": \"Allow\", \"Action\": \"sts:AssumeRole\", \"Resource\": \"arn:aws:iam::<AWS Account ID>:role/<sample-app-role-name>\"}]}"` Esta política está asociada al rol de TVM. Proporciona la capacidad de asumir el rol de aplicación que otorga permisos más amplios para acceder al bucket de S3.	

Tarea	Descripción	Habilidades requeridas
Adjunte la política de Lambda gestionada.	Utilice el siguiente comando de AWS CLI para adjuntar la política de IAM `AWSLambdaBasicExecutionRole`. Proporcione el valor **<** sample-tvm-role-name **>** en el comando: `aws iam attach-role-policy \ --role-name <sample-tvm-role-name> \ --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole` En la línea de comandos de Windows: `aws iam attach-role-policy ^ --role-name <sample-tvm-role-name> ^ --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole` Esta política gestionada se adjunta a la función TVM para permitir que Lambda envíe registros a Amazon. CloudWatch	Administrador de la nube

Cree la política y el rol de aplicación de IAM

Tarea	Descripción	Habilidades requeridas
Crear el rol de la aplicación.	Ejecute uno de los siguiente s comandos de la CLI de AWS para crear un rol de IAM. Proporcione los <AWS Account ID>valores < sample-app-role-name > y < sample-tvm-role-name > en el comando. Para los intérprete de comandos para macOS o Linux: `aws iam create-role \ --role-name <sample-app-role-name> \ --assume-role-policy-document '{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": "arn:aws:iam::<AWS Account ID>:role/<sample-tvm-role-name>" }, "Action": "sts:AssumeRole" } ]}'`	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	En la línea de comandos de Windows: `aws iam create-role ^ --role-name <sample-app-role-name> ^ --assume-role-policy-document "{\"Version\": \"2012-10-17\", \"Statement\": [{\"Effect\": \"Allow\",\"Principal\": {\"AWS\": \"arn:aws:iam::<AWS Account ID>:role/<sample-tvm-role-name>\"},\"Action\": \"sts:AssumeRole\" }]}"` La aplicación de ejemplo de Lambda asume esta función con una política específica para obtener acceso basado en usuario a un bucket de S3.	

Tarea	Descripción	Habilidades requeridas
Cree una política de rol de aplicación en línea.	Ejecute uno de los siguientes comandos de CLI de AWS para crear una política de IAM. Proporcione los valores **<** sample-app-role-name **>** y **<** sample-app-bucket-name **>** en el comando. Para los intérprete de comandos para macOS o Linux: `aws iam put-role-policy \ --role-name <sample-app-role-name> \ --policy-name s3-bucket-access \ --policy-document '{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"], "Resource": "arn:aws:s3:::<sample-app-bucket-name>/*" }, {`	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	<pre>"Effect": "Allow", "Action": ["s3:ListBucket"], "Resource ": "arn:aws:s3:::<sam ple-app-bucket-name>" }]}'</pre> En la línea de comandos de Windows: <pre>aws iam put-role-policy ^ --role-name <sample-a pp-role-name> ^ --policy-name s3-bucket -access ^ --policy-documen t "{\"Version\": \"2012-10-17\", \"Statement\": [{\"Effect\": \"Allow \", \"Action\": [\"s3:PutObject\", \"s3:GetObject\", \"s3:DeleteObject\ \"], \"Resource\": \"arn:aws:s3:::<sa mple-app-bucket-na me>/*\"}, {\"Effect\": \"Allow\", \"Action\ \": [\"s3:ListBucket \"], \"Resource\": \"arn:aws:s3:::<sa mple-app-bucket-name> \"}]}"</pre>	

Tarea	Descripción	Habilidades requeridas
	Esta política está asociada al rol de la aplicación. Proporciona un acceso amplio a los objetos del bucket de S3. Cuando la aplicación de ejemplo asume el rol, estos permisos se asignan a un usuario específico con la política de TVM generada de forma dinámica.	

Cree la aplicación de muestra de Lambda con TVM

Tarea	Descripción	Habilidades requeridas
Descargue los archivos fuente compilados.	Descargue los archivos `s3UploadSample.jar` y `tvm-layer.zip`, que se incluyen como adjuntos. El código fuente utilizado para crear estos artefactos y las instrucciones de compilación se proporcionan en `token-vending-machine-sample-app.zip`.	Administrador de la nube
Cree la capa de Lambda.	Ejecute el siguiente comando en la CLI de AWS para crear una capa de Lambda que permita a Lambda acceder a la TVM. Nota: si no ejecuta este comando desde la ubicación	Administrador de la nube, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	en la que descargó `tvm-layer.zip`, indique la ruta correcta a `tvm-layer.zip` en el parámetro `--zip-file`. `aws lambda publish-layer-version \ --layer-name sample-token-vending-machine \ --compatible-runtimes java11 \ --zip-file fileb://tvm-layer.zip` En la línea de comandos de Windows: `aws lambda publish-layer-version ^ --layer-name sample-token-vending-machine ^ --compatible-runtimes java11 ^ --zip-file fileb://tvm-layer.zip` Este comando crea una capa de Lambda que contiene la biblioteca TVM reutilizable.	

Tarea	Descripción	Habilidades requeridas
Crear la función de Lambda.	Use el siguiente comando de la CLI para crear la función de Lambda. Proporcione los <AWS Account ID><AWS Region>valores < sample-app-function-name >,, < sample-tvm-role-name >, < sample-app-bucket-name > y < sample-app-role-name > en el comando. Nota: si no ejecuta este comando desde la ubicación en la que descargó `s3UploadSample.jar` , indique la ruta correcta a `s3UploadSample.jar` en el parámetro `--zip-file` . `aws lambda create-function \ --function-name <sample-app-function-name> \ --timeout 30 \ --memory-size 256 \ --runtime java11 \ --role arn:aws:iam::<AWS Account ID>:role/<sample-tvm-role-name> \ --handler com.amazon.aws.s3UploadSample.App \ --zip-file fileb://s3UploadSample.jar \ --layers arn:aws:lambda:<AWS Region>:<AWS Account ID>:layer`	Administrador de la nube, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	:sample-token-vend ing-machine:1 \ --environment "Variable s={S3_BUCKET=<sample- app-bucket-name>, ROLE=arn:aws:iam::<AWS Account ID>:role/ <sample-app-role-n ame>}" Para la línea de comandos de Windows: aws lambda create-fu nction ^ --function-name <sample-app-function- name> ^ --timeout 30 ^ --memory-size 256 ^ --runtime java11 ^ --role arn:aws:i am::<AWS Account ID>:role/<sample-tvm- role-name> ^ --handler com.amazo n.aws.s3UploadSamp le.App ^ --zip-file fileb://s 3UploadSample.jar ^ --layers arn:aws:l ambda:<AWS Region>:< AWS Account ID>:layer :sample-token-vend ing-machine:1 ^ --environment "Variable s={S3_BUCKET=<samp le-app-bucket-name >,ROLE=arn:aws:iam ::<AWS Account	

Tarea	Descripción	Habilidades requeridas
	`ID>:role/<sample-app-role-name>}"` Este comando crea una función de Lambda con el código de la aplicación de ejemplo y la capa de TVM adjunta. También establece dos variables de entorno: `S3_BUCKET` y `ROLE`. La aplicación de ejemplo usa estas variables para determinar el rol que debe asumir y el bucket de S3 en el que se deben cargar los documentos JSON.	

Pruebe la aplicación de muestra y TVM

Tarea	Descripción	Habilidades requeridas
Invoque la aplicación de ejemplo de Lambda.	Ejecute uno de los siguientes comandos en la CLI de AWS para iniciar la aplicación de ejemplo de Lambda con la carga útil esperada. Proporcione los valores **<** sample-app-function-name **>** y **<** sample-tenant-name **>** en el comando. Para intérprete de comandos macOS y Linux: `aws lambda invoke \`	Administrador de la nube, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`--function <sample-app-function-name> \ --invocation-type RequestResponse \ --payload '{"tenant": "<sample-tenant-name>"}' \ --cli-binary-format raw-in-base64-out response.json` En la línea de comandos de Windows: `aws lambda invoke ^ --function <sample-app-function-name> ^ --invocation-type RequestResponse ^ --payload "{\"tenant\": \"<sample-tenant-name>\"}" ^ --cli-binary-format raw-in-base64-out response.json` Este comando llama a la función de Lambda y devuelve el resultado en un documento `response.json` . En muchos sistemas basados en Unix, puede cambiar `response.json` a `/dev/stdout` para enviar los resultados directamente a su intérprete de comandos sin necesidad de crear otro archivo.	

Tarea	Descripción	Habilidades requeridas
	Nota: Al cambiar el valor < sample-tenant-name > en las siguientes invocaciones de esta función Lambda, se modifica la ubicación del documento JSON y los permisos que proporciona el token.	
Acceda al bucket de S3 para ver los objetos creados.	Navegue hasta el bucket de S3 (< sample-app-bucket-name >) que creó anteriorm ente. Este depósito contiene un prefijo de objeto S3 con el valor < sample-tenant-name >. Bajo ese prefijo, encontrará un documento JSON denominad o con un UUID. Si invoca la aplicación de ejemplo varias veces, se añadirán más documentos JSON.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Acceda a los registros de Cloudwatch de la aplicación de muestra.	Vea los registros de Cloudwatch asociados a la función Lambda denominad a sample-app-function-name < >. Para obtener instrucci ones, consulte Acceso a CloudWatch los registros de Amazon para AWS Lambda en la documentación de AWS Lambda. En estos registros puede ver la política basada en usuario generada por la TVM. Esta política dirigida al inquilino otorga permisos para la aplicación de ejemplo a Amazon S3 PutObject,, y a ListBucketlas API GetObject DeleteObject, pero solo para el prefijo de objeto asociado a < >. sample-tenant-name En las siguientes invocaciones de la aplicación de ejemplo, si se cambia la opción < sample-tenant-name >, el TVM actualiza la política de ámbito para que se ajuste al inquilino proporcionado en la carga útil de invocación. Esta política generada dinámicam ente muestra cómo se puede mantener el acceso basado en usuario con una TVM en aplicaciones SaaS.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	La funcionalidad de TVM se proporciona en una capa de Lambda. Así, es posible adjuntarla a otras funciones de Lambda usadas por una aplicación sin tener que replicar el código. Para ver un ejemplo de la política generada dinámicam ente, consulte la sección de Información adicional.	

Recursos relacionados

- Aislar a los usuarios con políticas de IAM generadas dinámicamente (publicación del blog)
- Aplicar políticas de aislamiento generadas dinámicamente en un entorno SaaS (publicación del blog)
- AWS SaaS Boost (un entorno de referencia de código abierto que le ayuda a trasladar su oferta de SaaS a AWS)

Información adicional

El siguiente registro de Amazon Cloudwatch muestra la política generada de forma dinámica y creada por el código de TVM siguiendo este patrón. En esta captura de pantalla, **<** sample-app-bucket-name **>** es **`DOC-EXAMPLE-BUCKET`** y **< >** es. sample-tenant-name `test-tenant-1` Las credenciales de STS emitidas por esta política limitada no pueden realizar ninguna acción en los objetos del bucket de S3, excepto en aquellos objetos asociados al prefijo de clave de objeto `test-tenant-1`.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Implementar el patrón saga sin servidor mediante AWS Step Functions

Creado por Tabby Ward (AWS), Rohan Mehta (AWS) y Rimpy Tewani (AWS)

Entorno: PoC o piloto	Tecnologías: modernización; sin servidor; nativas en la nube	Carga de trabajo: código abierto
Servicios de AWS: Amazon API Gateway; Amazon DynamoDB; AWS Lambda; Amazon SNS; AWS Step Functions		

Resumen

En una arquitectura de microservicios, el objetivo principal es crear componentes disociados e independientes para promover la agilidad, la flexibilidad y reducir el tiempo de comercialización de sus aplicaciones. Como resultado del desacoplamiento, cada componente del microservicio tiene su propia capa de persistencia de datos. En una arquitectura distribuida, las transacciones comerciales pueden abarcar varios microservicios. Como estos microservicios no pueden utilizar una sola transacción de atomicidad, coherencia, aislamiento y durabilidad (ACID), es posible que acabe con transacciones parciales. En este caso, se necesita alguna lógica de control para deshacer las transacciones que ya se han procesado. El patrón saga distribuido se utiliza normalmente para este propósito.

El patrón saga es un patrón de gestión de fallos que ayuda a establecer la coherencia en las aplicaciones distribuidas y coordina las transacciones entre varios microservicios para mantener la coherencia de los datos. Si se utiliza el patrón «saga», cada servicio que realiza una transacción publica un evento que desencadena que los servicios subsiguientes realicen la siguiente transacción de la cadena. Esto continúa hasta que se complete la última transacción de la cadena. Si una transacción comercial fracasa, Saga organiza una serie de transacciones compensatorias que anulan los cambios introducidos en las transacciones anteriores.

Este patrón demuestra cómo automatizar la configuración y el despliegue de una aplicación de muestra (que gestiona las reservas de viajes) con tecnologías sin servidor, como AWS Step Functions, AWS Lambda y Amazon DynamoDB. La aplicación de ejemplo también utiliza Amazon API Gateway y Amazon Simple Notification Service (Amazon SNS) para implementar un coordinador de ejecución de saga. El patrón se puede implementar con un marco de infraestructura como código (IaC), como el AWS Cloud Development Kit (AWS CDK), el AWS Serverless Application Model (AWS Serverless Application Model SAM) o Terraform.

Para obtener más información sobre el patrón saga y otros patrones de persistencia de datos, consulte la guía Habilitar la persistencia de datos en microservicios en el sitio web de Recomendaciones de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Permisos para crear una CloudFormation pila de AWS. Para obtener más información, consulte Controlar el acceso en la CloudFormation documentación.
- El marco de IaC de su elección (AWS CDK, AWS SAM o Terraform) se configuró con su cuenta de AWS para que pueda usar la CLI del marco para implementar la aplicación.
- NodejS, utilizado para compilar la aplicación y ejecutarla localmente.
- Un editor de código de su elección (como Visual Studio Code, Sublime o Atom).

Versiones de producto

- NodeJS versión 14
- AWS CDK versión 2.37.1
- AWS SAM versión 1.71.0
- Terraform versión 1.3.7

Limitaciones

El abastecimiento de eventos es una forma natural de implementar el patrón de orquestación de la saga en una arquitectura de microservicios en la que todos los componentes están acoplados de forma flexible y no se conocen directamente entre sí. Si su transacción incluye un número reducido

de pasos (de tres a cinco), el patrón saga podría ser una buena opción. Sin embargo, la complejidad aumenta con el número de microservicios y el número de pasos.

Las pruebas y la depuración pueden resultar difíciles cuando se utiliza este diseño, ya que es necesario tener todos los servicios en ejecución para poder simular el patrón de transacciones.

Arquitectura

Arquitectura de destino

La arquitectura propuesta utiliza AWS Step Functions para crear un patrón de saga para reservar vuelos, reservar alquileres de vehículos y procesar los pagos de las vacaciones.

El siguiente diagrama de flujo de trabajo ilustra el flujo típico del sistema de reservas de viajes. El flujo de trabajo consiste en reservar un viaje en avión («ReserveFlight»), reservar un coche («ReserveCarRental»), procesar los pagos («ProcessPayment»), confirmar las reservas de vuelos («ConfirmFlight») y confirmar el alquiler de vehículos («ConfirmCarRental»), seguido de una notificación de confirmación cuando se hayan completado estos pasos. Sin embargo, si el sistema detecta algún error al ejecuter alguna de estas transacciones, empezará a fallar hacia atrás. Por ejemplo, un error en el procesamiento del pago («ProcessPayment») desencadena un reembolso («RefundPayment»), que luego desencadena la cancelación del coche de alquiler y del vuelo («CancelRentalReservation» y «CancelFlightReservation»), lo que finaliza toda la transacción con un mensaje de error.

Este patrón implementa funciones Lambda independientes para cada tarea que se resalta en el diagrama, así como tres tablas de DynamoDB para vuelos, alquileres de vehículos y pagos. Cada función de Lambda crea, actualiza o elimina las filas de las tablas de DynamoDB respectivas, en función de si la transacción se confirma o se revierte. El patrón utiliza Amazon SNS para enviar mensajes de texto (SMS) a los suscriptores y notificarles las transacciones fallidas o satisfactorias.

Automatizar y escalar

Puede crear la configuración de esta arquitectura mediante uno de los marcos de IaC. Utilice uno de los siguientes enlaces para su iAC preferido.

- Implementar con AWS CDK
- Implementar con AWS SAM

- Implementar con Terraform

Herramientas

Servicios de AWS

- AWS Step Functions es un servicio de orquestación sin servidor que le permite combinar funciones de Lambda AWS y otros servicios de AWS para crear aplicaciones esenciales desde el punto de vista empresarial. A través de la consola gráfica Step Functions, puede ver el flujo de trabajo de su aplicación como una serie de pasos basados en eventos.
- Amazon DynamoDB es un servicio de base de datos NoSQL totalmente administrado que ofrece un rendimiento rápido y predecible, así como una perfecta escalabilidad. Puede utilizar DynamoDB para crear una tabla de base de datos capaz de almacenar y recuperar cualquier cantidad de datos, así como de atender cualquier nivel de tráfico de solicitudes.
- AWS Lambda es un servicio informático que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo.
- Amazon API Gateway es un servicio de AWS para crear, publicar, mantener, supervisar y proteger REST, HTTP y WebSocket API a cualquier escala.
- Amazon Simple Notification Service (Amazon SNS) es un servicio administrado que proporciona la entrega de mensajes de los publicadores a los suscriptores.
- El AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software para definir los recursos de las aplicaciones en la nube mediante lenguajes de programación conocidos TypeScript, como Python JavaScript, Java y C#/.Net.
- AWS Serverless Application Model (AWS SAM) es un marco de código abierto que permite crear aplicaciones sin servidor. Proporciona una sintaxis abreviada para expresar funciones, API, bases de datos y mapeos de fuentes de eventos.

Código

El código de una aplicación de ejemplo que muestra el patrón saga, incluida la plantilla IaC (AWS CDK, AWS SAM o Terraform), las funciones de Lambda y las tablas de DynamoDB, se encuentra en los siguientes enlaces. Siga las instrucciones de la primera epic para instalarlos.

- Implementar con AWS CDK
- Implementar con AWS SAM

- Implementar con Terraform

Epics

Instalar paquetes, compilar y compilar

Tarea	Descripción	Habilidades requeridas
Instalar los paquetes NPM.	Cree un directorio nuevo, navegue hasta ese directorio en una terminal y clone el GitHub repositorio que prefiera en la sección de código que aparece anteriormente en este patrón. En la carpeta raíz que contiene el archivo `package.json` , ejecute el siguiente comando para descargar e instalar todos los paquetes de Node Package Manager (NPM): `npm install`	Desarrollador, arquitecto de la nube
Compilar scripts.	En la carpeta raíz, ejecute el siguiente comando para indicar al TypeScript transpilador que cree todos los archivos necesarios: JavaScript `npm run build`	Desarrollador, arquitecto de la nube
Esté atento a los cambios y vuelva a compilar.	En la carpeta raíz, ejecute el siguiente comando en	Desarrollador, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	una ventana de terminal independiente para comprobar si hay cambios en el código y compílalo cuando lo detecte: `npm run watch`	
Ejecute pruebas unitarias (solo AWS CDK).	Si utiliza el CDK de AWS, en la carpeta raíz, ejecute el siguiente comando para realizar las pruebas unitarias de Jest: `npm run test`	Desarrollador, arquitecto de la nube

Implemente recursos en la cuenta de AWS de destino

Tarea	Descripción	Habilidades requeridas
Implemente la pila de demostración en AWS.	Importante: La aplicación es independiente de la región de AWS. Si utiliza un perfil, debe declarar la región de forma explícita en el perfil de la interfaz de la línea de comandos de AWS (AWS CLI) o mediante variables de entorno de la CLI de AWS. En la carpeta raíz, ejecute el siguiente comando para crear un ensamblaje de implement ación e implementarlo en	Desarrollador, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	la cuenta y región de AWS predeterminadas. AWS CDK: `cdk bootstrap` `cdk deploy` AWS SAM: `sam build` `sam deploy --guided` Terraform: `terraform init` `terraform apply` Este paso puede tardar varios minutos en completarse. Este comando usa las credencia les predeterminadas que se configuraron para la AWS CLI. Anote la URL de API Gateway que se muestra en la consola una vez completada la implementación. Necesitará esta información para probar el flujo de ejecución de la saga.	

Tarea	Descripción	Habilidades requeridas
Compare la pila implementada con el estado actual.	En la carpeta raíz, ejecute el siguiente comando para comparar la pila implementada con el estado actual después de realizar cambios en el código fuente: AWS CDK: `cdk diff` AWS SAM: `sam deploy` Terraform: `terraform plan`	Desarrollador, arquitecto de la nube

Pruebe el flujo de ejecución

Tarea	Descripción	Habilidades requeridas
Probar el flujo de ejecución de la saga.	Navegue hasta la URL de API Gateway que indicó en el paso anterior, cuando implementó la pila. Esta URL activa el inicio de la máquina de estados. Para obtener más información sobre cómo manipular el flujo de la máquina de estados pasando diferentes parámetro	Desarrollador, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	s de URL, consulte la sección de Información adicional. Para ver los resultados, inicie sesión en la consola de administración de AWS y vaya a la consola de Step Functions . Aquí puede ver todos los pasos de la saga State Machine. También puede ver la tabla de DynamoDB para ver los registros insertado s, actualizados o eliminado s. Si actualiza la pantalla con frecuencia, puede ver cómo el estado de la transacci ón cambia de `apending`. `confirmed` Puedes suscribirte al tema de las redes sociales actualiza ndo el código del archivo `stateMachine.ts` con tu número de teléfono móvil para recibir mensajes SMS cuando las reservas se hayan realizado o no se hayan realizado correctamente. Para obtener más información, consulte Amazon SNS en la sección Información adicional.	

Limpieza

Tarea	Descripción	Habilidades requeridas
Limpiar recursos.	Para limpiar los recursos desplegados para esta aplicación, puede usar uno de los siguientes comandos. AWS CDK: `cdk destroy` AWS SAM: `sam delete` Terraform: `terraform destroy`	Desarrollador de aplicaciones, arquitecto de la nube

Recursos relacionados

Documentos técnicos

- Implementación de microservicios en AWS
- Aplicaciones sin servidor
- Permitir la persistencia de los datos en los microservicios

Documentación de servicio de AWS

- Introducción a los AWS SDK
- Introducción a AWS SAM
- AWS Step Functions
- Amazon DynamoDB

- AWS Lambda
- Amazon API Gateway
- Amazon SNS

Tutoriales

- Talleres prácticos sobre informática sin servidor

Información adicional

Código

Con fines de prueba, este patrón implementa API Gateway y una función de Lambda de prueba que activa la máquina de estados Step Functions. Con Step Functions, puedes controlar la funcionalidad del sistema de reservas de viajes pasando un `run_type` parámetro para imitar los errores en «ReserveFlightReserveCarRental,» «ProcessPayment,» «ConfirmFlight,» y «»ConfirmCarRental.

La `saga`función de Lambda (`sagaLambda.ts`) toma la entrada de los parámetros de consulta de la URL de la API Gateway, crea el siguiente objeto JSON y lo pasa a Step Functions para su ejecución:

```
let input = {
"trip_id": tripID, //  value taken from query parameter, default is AWS request ID
"depart_city": "Detroit",
"depart_time": "2021-07-07T06:00:00.000Z",
"arrive_city": "Frankfurt",
"arrive_time": "2021-07-09T08:00:00.000Z",
"rental": "BMW",
"rental_from": "2021-07-09T00:00:00.000Z",
"rental_to": "2021-07-17T00:00:00.000Z",
"run_type": runType // value taken from query parameter, default is "success"
};
```

Puede experimentar con diferentes flujos de la máquina de estados Step Functions pasando los siguientes parámetros de URL:

- Ejecución correcta: https://{api gateway url}
- Error en la reserva del vuelo — https://{api gateway url}? Tipo de ejecución = failFlightsReservation
- Confirma el error del vuelo — https://{api gateway url}? Tipo de ejecución = failFlightsConfirmation

- Error al alquilar un coche al reservar – https://{api gateway url}? RunType = Reserva failCarRental
- Confirme que el alquiler del vehículo ha fallado – https://{api gateway url}? RunType = Confirmación failCarRental
- Error al procesar el pago: https://{api gateway url}?runType=failPayment
- Pasar un identificador de viaje: https://{api gateway url}? tripID= {de forma predeterminada, el ID de viaje será el ID de solicitud de AWS}

Plantillas de iAC

Los repositorios enlazados incluyen plantillas de IaC que puede utilizar para crear toda la aplicación de reserva de viajes de muestra.

- Implementar con AWS CDK
- Implementar con AWS SAM
- Implementar con Terraform

Tablas de DynamoDB

Estos son los modelos de datos para las tablas de vuelos, alquileres de coches y pagos.

```
Flight Data Model:
 var params = {
      TableName: process.env.TABLE_NAME,
      Item: {
        'pk' : {S: event.trip_id},
        'sk' : {S: flightReservationID},
        'trip_id' : {S: event.trip_id},
        'id': {S: flightReservationID},
        'depart_city' : {S: event.depart_city},
        'depart_time': {S: event.depart_time},
        'arrive_city': {S: event.arrive_city},
        'arrive_time': {S: event.arrive_time},
        'transaction_status': {S: 'pending'}
      }
    };

Car Rental Data Model:
var params = {
      TableName: process.env.TABLE_NAME,
```

```
      Item: {
        'pk' : {S: event.trip_id},
        'sk' : {S: carRentalReservationID},
        'trip_id' : {S: event.trip_id},
        'id': {S: carRentalReservationID},
        'rental': {S: event.rental},
        'rental_from': {S: event.rental_from},
        'rental_to': {S: event.rental_to},
        'transaction_status': {S: 'pending'}
      }
    };

Payment Data Model:
var params = {
      TableName: process.env.TABLE_NAME,
      Item: {
        'pk' : {S: event.trip_id},
        'sk' : {S: paymentID},
        'trip_id' : {S: event.trip_id},
        'id': {S: paymentID},
        'amount': {S: "750.00"}, // hard coded for simplicity as implementing any
 monetary transaction functionality is beyond the scope of this pattern
        'currency': {S: "USD"},
        'transaction_status': {S: "confirmed"}
      }
    };
```

Funciones de Lambda

Se crearán las siguientes funciones para respaldar el flujo y la ejecución de la máquina de estados en Step Functions:

- Reservar vuelos: introduzca un registro en la tabla de vuelos de DynamoDB con `transaction_status` un `pending` de para reservar un vuelo.
- Confirmar vuelo: actualiza el registro de la tabla de vuelos de DynamoDB para establecer `transaction_status` en `confirmed`, para confirmar el vuelo.
- Cancelar reserva de vuelos: elimina el registro de la tabla de vuelos de DynamoDB para cancelar el vuelo pendiente.
- Reserve vehículos de alquiler: inserta un registro en la tabla de CarRentals DynamoDB con `transaction_status` un `pending` de para reservar un alquiler de vehículos.

- Confirmar alquileres de vehículos: actualiza el registro de la tabla de CarRentals DynamoDB para `transaction_status` `confirmed` establecerlo en y confirmar el alquiler de vehículos.
- Cancelar reserva de vehículos de alquiler: elimina el registro de la tabla de CarRentals DynamoDB para cancelar el alquiler de vehículos pendiente.
- Procesar pago: inserta un registro en la tabla de pagos de DynamoDB para el pago.
- Cancelar pago: elimina el registro del pago de la tabla de pagos de DynamoDB.

Amazon SNS

La aplicación de ejemplo crea el tema y la suscripción siguientes para enviar mensajes SMS y notificar al cliente si las reservas se han realizado o no se han realizado correctamente. Si desea recibir mensajes de texto mientras prueba la aplicación de ejemplo, actualice la suscripción de SMS con su número de teléfono válido en el archivo de definición de la máquina de estados.

Fragmento de CDK de AWS (añada el número de teléfono en la segunda línea del siguiente código):

```
const topic = new  sns.Topic(this, 'Topic');
topic.addSubscription(new subscriptions.SmsSubscription('+11111111111'));
const snsNotificationFailure = new tasks.SnsPublish(this ,'SendingSMSFailure', {
topic:topic,
integrationPattern: sfn.IntegrationPattern.REQUEST_RESPONSE,
message: sfn.TaskInput.fromText('Your Travel Reservation Failed'),
});

const snsNotificationSuccess = new tasks.SnsPublish(this ,'SendingSMSSuccess', {
topic:topic,
integrationPattern: sfn.IntegrationPattern.REQUEST_RESPONSE,
message: sfn.TaskInput.fromText('Your Travel Reservation is Successful'),
});
```

Fragmento de SAM de AWS (sustituya las cadenas +1111111111 por su número de teléfono válido):

```
  StateMachineTopic11111111111:
    Type: 'AWS::SNS::Subscription'
    Properties:
      Protocol: sms
      TopicArn:
        Ref: StateMachineTopic
      Endpoint: '+11111111111'
```

```
    Metadata:
      'aws:sam:path': SamServerlessSagaStack/StateMachine/Topic/+11111111111/Resource
```

Fragmento de Terraform (sustituya la cadena +111111111 por su número de teléfono válido):

```
resource "aws_sns_topic_subscription" "sms-target" {
  topic_arn = aws_sns_topic.topic.arn
  protocol  = "sms"
  endpoint  = "+11111111111"
}
```

Reservas realizadas satisfactoriamente

El siguiente flujo ilustra una reserva correcta con «ReserveFlight,»ReserveCarRental, «» y «» seguidos de «ProcessPayment» y «ConfirmFlight». ConfirmCarRental Se notifica al cliente que la reserva se ha realizado correctamente mediante mensajes SMS que se envían al suscriptor del tema de las redes sociales.

Reservas fallidas

Este flujo es un ejemplo de fracaso en el patrón de la saga. Si, después de reservar vuelos y alquileres de vehículos, «ProcessPayment» falla, los pasos se cancelan en orden inverso. Se cancelan las reservas y se notifica al cliente del error mediante mensajes SMS que se envían al suscriptor del tema de las redes sociales.

Gestión de las aplicaciones de contenedores en las instalaciones mediante la configuración de Amazon ECS Anywhere con AWS CDK

Creado por el Dr. Rahul Sharad Gaikwad (AWS)

Repositorio de código: - samples amazon-ecs-anywhere-cdk	Entorno: PoC o piloto	Tecnologías: modernización; contenedores y microservicios; nube híbrida DevOps; infraestructura
Carga de trabajo: todas las demás cargas de trabajo	Servicios de AWS: AWS CDK; Amazon ECS; AWS Identity and Access Management	

Resumen

Amazon ECS Anywhere es una extensión de Amazon Elastic Container Service (Amazon ECS). Puede usar ECS Anywhere para implementar tareas nativas de Amazon ECS en un entorno en las instalaciones o administrado por el cliente. Esta característica ayuda a reducir los costos y a mitigar la compleja orquestación y las operaciones de los contenedores locales. Puede usar ECS Anywhere para implementar y ejecutar aplicaciones de contenedor tanto en entornos en las instalaciones como en la nube. Evita que su equipo tenga que aprender varios dominios y conjuntos de habilidades, o administrar software complejo por su cuenta.

Este patrón muestra los pasos para configurar ECS Anywhere mediante pilas del AWS Cloud Development Kit (AWS CDK).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.

- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada. (Consulte Instalación, actualización y desinstalación de la CLI de AWS en la documentación de la CLI de AWS).
- Kit de herramientas de AWS CDK, instalado y configurado. (Consulte el kit de herramientas de AWS CDK en la documentación de AWS CDK y siga las instrucciones para instalar la versión 2 en todo el mundo).
- Administrador de paquetes de nodos (npm), instalado y configurado para la AWS CDK en. TypeScript (Consulte Descargar e instalar Node.js y npm en la documentación de npm).

Limitaciones

- Para ver las limitaciones y consideraciones, consulte Instancias externas (Amazon ECS Anywhere) en la documentación de Amazon ECS.

Versiones de producto

- AWS CDK Toolkit versión 2
- npm versión 7.20.3 o posterior
- Node.js versión 16.6.1 o posterior

Arquitectura

Pila de tecnología de destino

- AWS CloudFormation
- AWS CDK
- Amazon ECS Anywhere
- AWS Identity y Access Management (IAM)

Arquitectura de destino

El siguiente diagrama ilustra una arquitectura de sistema de alto nivel de la configuración de ECS Anywhere que utiliza la AWS CDK con TypeScript, tal como se implementa mediante este patrón.

1. Al implementar la pila de CDK de AWS, se crea una CloudFormation pila en AWS.

2. La CloudFormation pila aprovisiona un clúster de Amazon ECS y los recursos de AWS relacionados.
3. Para registrar una instancia externa en un clúster de Amazon ECS, debe instalar AWS Systems Manager Agent (SSM Agent) en su máquina virtual (VM) y registrar la VM como instancia administrada por AWS Systems Manager.
4. También debe instalar el agente de contenedores de Amazon ECS y Docker en su máquina virtual para registrarla como instancia externa en el clúster de Amazon ECS.
5. Cuando la instancia externa está ya registrada y configurada con el clúster de Amazon ECS, puede ejecutar varios contenedores en su máquina virtual, registrada como instancia externa.

Automatizar y escalar

El GitHub repositorio que se proporciona con este patrón utiliza la CDK de AWS como herramienta de infraestructura como código (IaC) para crear la configuración de esta arquitectura. AWS CDK le ayuda a orquestar los recursos y configurar ECS Anywhere.

Herramientas

- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura de la nube de AWS en código.
- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.

Código

El código fuente de este patrón está disponible en el GitHub repositorio de muestras de CDK de Amazon ECS Anywhere. Para clonar y utilizar el repositorio, siga las instrucciones de la siguiente sección.

Epics

Verificar la configuración de AWS CDK

Tarea	Descripción	Habilidades requeridas
Verifique la versión de AWS CDK.	Compruebe la versión del kit de herramientas de AWS CDK mediante el siguiente comando: `cdk --version` Este patrón requiere la versión 2 de AWS CDK. Si tiene una versión anterior de AWS CDK siga las instrucciones de la documentación de AWS CDK para actualizarla.	DevOps ingeniero
Configure las credenciales de AWS.	Para configurar las credencia les, ejecute el comando `aws configure` y siga las instrucciones: `$aws configure` `AWS Access Key ID [None]: <your-access-key-ID>` `AWS Secret Access Key [None]: <your-secret-access-key>` `Default region name [None]: <your-Region-name>` `Default output format [None]:`	DevOps ingeniero

Inicie el entorno de AWS CDK

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio de código de AWS CDK.	Clona el repositorio de GitHub código de este patrón mediante el comando: `git clone https://github.com/aws-samples/amazon-ecs-anywhere-cdk-samples.git`	DevOps ingeniero
Inicie el entorno.	Para implementar la CloudFormation plantilla de AWS en la cuenta y la región de AWS que desee usar, ejecute el siguiente comando: `cdk bootstrap <account-number>/<Region>` Para obtener más información, consulte Proceso de arranque en la documentación de AWS CDK.	DevOps ingeniero

Crear e implementar el proyecto

Tarea	Descripción	Habilidades requeridas
Instale las dependencias de los paquetes y compile TypeScript los archivos.	Instale las dependencias del paquete y compile los TypeScript archivos ejecutando los siguientes comandos:	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`$cd amazon-ecs-anywhere-cdk-samples` `$npm install` `$npm fund` Estos comandos instalan todos los paquetes del repositorio de muestra. Importante: Si se muestra algún error acerca de paquetes que faltan, utilice uno de los siguientes comandos: `$npm ci` —o— `$npm install -g @aws-cdk/<package_name>` Para obtener más información, consulte npm ci y npm install en la documentación de npm.	

Tarea	Descripción	Habilidades requeridas
Compilar el proyecto.	Ejecute el siguiente comando para compilar el código del proyecto: `npm run build` Para obtener más informaci ón sobre la compilaci ón e implementación del proyecto, consulte Su primera aplicación de AWS CDK en la documentación de AWS CDK.	DevOps ingeniero
Implementar el proyecto.	Para implementar el código del proyecto, ejecute el comando: `cdk deploy`	DevOps ingeniero
Verifique la creación y el resultado de la pila.	Abra la CloudFormation consola de AWS en https://console.aws.amazon.com/cloudformation y elija la `EcsAnywhereStack` pila. La pestaña Salidas muestra los comandos que se deben ejecutar en su máquina virtual externa.	DevOps ingeniero

Configuración de una máquina en las instalaciones

Tarea	Descripción	Habilidades requeridas
Configure su máquina virtual mediante Vagrant.	Con fines de demostración, puede usar HashiCorp Vagrant para crear una máquina virtual. Vagrant es una utilidad de código abierto para compilar y mantener entornos de desarrollo de software virtual portátiles. Cree una máquina virtual Vagrant ejecutando el comando `vagrant up` desde el directorio raíz donde se encuentra Vagrantfile. Para obtener más información, consulte la documentación de Vagrant.	DevOps ingeniero
Registre su máquina virtual como instancia externa.	1. Inicie sesión en la máquina virtual de Vagrant mediante el comando `vagrant ssh`. Para obtener más información, consulte la documentación de Vagrant. 2. Cree un código de activación y una ID que usará para registrar su máquina virtual en AWS Systems Manager y activar su instancia externa. El resultado de este comando incluye valores `ActivationId` y `ActivationCode` :	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`aws ssm create-activation --iam-role EcsAnywhereInstanceRole | tee ssm-activation.json` 3. Exporte el ID de activación y los valores del código: `export ACTIVATION_ID=<activation-ID>` `export ACTIVATION_CODE=<activation-code>` 4. Descargar el script de instalación en el servidor ubicado en las instalaciones o en la máquina virtual (VM): `curl -o "ecs-anywhere-install.sh" "https://amazon-ecs-agent.s3.amazonaws.com/ecs-anywhere-install-latest.sh" && sudo chmod +x ecs-anywhere-install.sh` 5. Ejecute el script de instalación en el servidor ubicado en las instalaciones o en la máquina virtual (VM). `sudo ./ecs-anywhere-install.sh \` `--cluster test-ecs-anywhere \`	

Tarea	Descripción	Habilidades requeridas
	`--activation-id $ACTIVATION_ID \ --activation-code $ACTIVATION_CODE \ --region <Region>` Para obtener más información sobre la configuración y el registro de su máquina virtual, consulte Registrar una instancia externa en un clúster en la documentación de Amazon ECS.	
Verifique el estado de ECS Anywhere y de la máquina virtual externa.	Para verificar si su caja virtual está conectada al plano de control de Amazon ECS y en funcionamiento, utilice los siguientes comandos: `aws ssm describe-instance-information` `aws ecs list-container-instances --cluster $CLUSTER_NAME`	DevOps ingeniero

Limpieza

Tarea	Descripción	Habilidades requeridas
Limpie y elimine recursos.	Después de seguir este patrón, debe eliminar los recursos que ha creado para evitar incurrir en cargos adicionales. Para limpiar, ejecute el comando:	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`cdk destroy`	

Recursos relacionados

- Documentación de Amazon ECS Anywhere
- Amazon ECS Anywhere Demo
- Muestras de talleres sobre Amazon ECS Anywhere

Modernizar las aplicaciones de ASP.NET Web Forms en AWS

Creado por Vijai Anand Ramalingam (AWS) y Sreelaxmi Pai (AWS)

Entorno: PoC o piloto	Tecnologías: modernización; contenedores y microservicios; desarrollo y pruebas de software; aplicaciones web y móviles	Carga de trabajo: Microsoft
Servicios de AWS: Amazon CloudWatch; Amazon ECS; AWS Systems Manager		

Resumen

Este patrón describe los pasos para modernizar una aplicación antigua y monolítica de ASP.NET Web Forms mediante su migración a ASP.NET Core en AWS.

La migración de las aplicaciones de ASP.NET Web Forms a ASP.NET Core le ayuda a aprovechar el rendimiento, el ahorro de costos y el sólido ecosistema de Linux. Sin embargo, puede suponer un esfuerzo manual considerable. En este patrón, la aplicación heredada se moderniza gradualmente mediante un enfoque gradual y, a continuación, se divide en contenedores en la nube de AWS.

Pensemos en una aplicación heredada y monolítica para un carrito de compras. Supongamos que se creó como una aplicación de ASP.NET Web Forms y consta de páginas .aspx con un archivo de código subyacente (`aspx.cs`). El proceso de modernización consta de estos pasos:

1. Divida el monolito en microservicios utilizando los patrones de descomposición adecuados. Para obtener más información, consulte la guía Cómo descomponer monolitos en microservicios en el sitio web de Recomendaciones de AWS.
2. Transfiera su aplicación heredada de ASP.NET Web Forms (.NET Framework) a ASP.NET Core en .NET 5 o posterior. En este patrón, usted utiliza el Asistente de portabilidad para .NET para analizar su aplicación ASP.NET Web Forms e identificar las incompatibilidades con ASP.NET Core. Esto reduce el esfuerzo de portabilidad manual.

3. Vuelva a desarrollar la capa de interfaz de usuario de Web Forms mediante React. Este patrón no cubre la remodelación de la interfaz de usuario. Para obtener instrucciones, consulte Crear una nueva aplicación de React en la documentación de React.
4. Vuelva a desarrollar el archivo de código subyacente de Web Forms (interfaz empresarial) como una API web de ASP.NET Core. Este patrón utiliza los informes de NDepend para ayudar a identificar los archivos y las dependencias necesarios.
5. Actualice los proyectos comunes o compartidos, como Business Logic y Data Access, de su aplicación heredada a .NET 5 o posterior mediante el Asistente de portabilidad para .NET.
6. Añada servicios de AWS para complementar su aplicación. Por ejemplo, puede usar Amazon CloudWatch Logs para monitorear, almacenar y acceder a los registros de su aplicación, y AWS Systems Manager para almacenar la configuración de la aplicación.
7. Ponga en contenedores la aplicación ASP.NET Core modernizada. Este patrón crea un archivo Docker orientado a Linux en Visual Studio y usa Docker Desktop para probarlo localmente. En este paso se asume que la aplicación heredada ya se ejecuta en una instancia de Windows en las instalaciones o en Amazon Elastic Compute Cloud (Amazon EC2). Para obtener más información, consulte el patrón Ejecutar un contenedor de Docker de la API web de ASP.NET Core en una instancia de Amazon EC2 Linux.
8. Implemente la aplicación principal ASP.NET modernizada en Amazon Elastic Container Service (Amazon ECS). Este patrón no cubre el paso de implementación. Para obtener instrucciones, consulte el Taller de Amazon ECS.

Nota: Este patrón no incluye los pasos de desarrollo de la interfaz de usuario, modernización de bases de datos o despliegue de contenedores.

Requisitos previos y limitaciones

Requisitos previos

- Visual Studio o Visual Studio Code, descargados e instalados.
- Acceso a una cuenta de AWS mediante la Consola de administración de AWS y la Interfaz de la línea de comandos de AWS (AWS CLI) versión 2. (Consulte las Instrucciones para configurar la CLI de AWS).
- El Toolkit de AWS para Visual Studio (consulte las instrucciones de configuración).
- Docker Desktop, descargado e instalado.
- .NET SDK, descargado e instalado.

- Herramienta nDepend, descargada e instalada. Para instalar la extensión NDepend para Visual Studio, ejecute `NDepend.VisualStudioExtension.Installer` (consulte las instrucciones). Puede seleccionar Visual Studio 2019 o 2022, según sus necesidades.
- Asistente de portabilidad para .NET, descargado e instalado.

Arquitectura

Modernización de la aplicación de carrito de compras

El siguiente diagrama ilustra el proceso de modernización de una aplicación heredada de carrito de compras de ASP.NET.

Arquitectura de destino

En el siguiente diagrama se ilustra la arquitectura de la aplicación de carrito de compras modernizada en AWS. Las API web de ASP.NET Core se implementan en un clúster de Amazon ECS. Los servicios de registro y configuración los proporcionan Amazon CloudWatch Logs y AWS Systems Manager.

Herramientas

Servicios de AWS

- Amazon ECS: Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores altamente escalable y rápido para ejecutar, detener y administrar contenedores en un clúster. Las tareas y los servicios se pueden ejecutar en una infraestructura sin servidor administrada por AWS Fargate. Si desea más control sobre su infraestructura, puede ejecutar las tareas y los servicios en un clúster de instancias de EC2 que usted administre.
- Amazon CloudWatch Logs: Amazon CloudWatch Logs centraliza los registros de todos los sistemas, aplicaciones y servicios de AWS que utilice. Esto le permite consultarlos, buscar códigos de error o patrones específicos, filtrarlos en función de campos específicos o archivarlos de forma segura para análisis futuros.
- AWS Systems Manager: AWS Systems Manager es un servicio que puede utilizar para ver y controlar su infraestructura en AWS. Mediante la consola de Systems Manager, puede ver los datos operativos de varios servicios de AWS y automatizar las tareas operativas en sus recursos

de AWS. Systems Manager le ayuda a mantener la seguridad y la conformidad mediante el análisis de sus instancias administradas y el informe sobre las infracciones de las políticas que detecte (o la toma de medidas correctivas con respecto a estas).

Herramientas

- Visual Studio o Visual Studio Code – Herramientas para crear aplicaciones.NET, API web y otros programas.
- AWS Toolkit for Visual Studio – Una extensión para Visual Studio que ayuda a desarrollar, depurar e implementar aplicaciones .NET que utilizan servicios de AWS.
- Docker Desktop – Una herramienta que simplifica la compilación e implementación de aplicaciones en contenedores.
- NDepend – Un analizador que supervisa el código.NET para detectar dependencias, problemas de calidad y cambios en el código.
- Asistente de portabilidad para .NET – Una herramienta de análisis que escanea el código.NET para identificar incompatibilidades con .NET Core y estimar el esfuerzo de migración.

Epics

Transfiera su aplicación heredada a .NET 5 o a una versión posterior

Tarea	Descripción	Habilidades requeridas
Actualice su aplicación heredada de.NET Framework a .NET 5.	Puede usar el Asistente de portabilidad para .NET para convertir su aplicación heredada de ASP.NET Web Forms a .NET 5 o posterior . Siga las instrucciones de la documentación del Asistente de portabilidad para .NET.	Desarrollador de aplicaciones
Genere informes de NDepend.	Al modernizar la aplicació n ASP.NET Web Forms descomponiéndola en microservicios, es posible	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	que no necesite todos los archivos .cs de la aplicación heredada. Puede usar NDepend para generar un informe para cualquier archivo con código subyacente (.cs), a fin de obtener todas las personas que llaman y a las que llaman. Este informe le ayuda a identificar y usar solo los archivos necesarios en sus microservicios. Tras instalar NDepend (consulte la sección Requisitos previos), abra la solución (archivo.sln) para su aplicación heredada en Visual Studio y siga estos pasos: 1. Cree la aplicación heredada en Visual Studio. 2. En la barra de menús de Visual Studio, seleccione NDepend Adjuntar nuevo proyecto de NDepend a la solución VS actual. 3. Seleccione Analizar ensamblados de .NET. 4. Cuando se complete el análisis, navegue hasta el proyecto en el Explorador de soluciones. Haga clic con el botón derecho en cualquier archivo con	

Tarea	Descripción	Habilidades requeridas
	código subyacente (por ejemplo, `listprodu cts.aspx.cs`) para el que desee generar el informe y, a continuación, seleccione Mostrar en gráfico de dependencias. 5. En la barra de navegació n, seleccione Emisores y destinatarios de llamadas y, a continuación, seleccione Editar consulta de código. 6. En el Panel de edición de consultas y reglas, seleccione la flecha de descarga y, a continuac ión, seleccione Exportar a Excel. Este proceso genera un informe para el archivo con el código subyacente en el que se enumeran todas los emisores y destinatarios de llamadas. Para obtener más información acerca del gráfico de dependencias, consulte la documentación de NDepend.	

Tarea	Descripción	Habilidades requeridas
Cree una nueva solución .NET 5.	Para crear una nueva estructura de .NET 5 (o posterior) para las API web modernizadas de ASP.NET Core: 1. Open Visual Studio. 2. Cree una nueva solución en blanco. 3. Cree nuevos proyectos que se dirijan a .NET 5 (o versiones posteriores), en función de su aplicación heredada. Para ver ejemplos de proyectos heredados y nuevos para una aplicación de carrito de compras, consulte la sección de Información adicional. 4. Utilice el informe NDepend del paso anterior para identificar todos los archivos necesarios. Copie estos archivos de la aplicación que actualizó anteriormente y agréguelos a la nueva solución. 5. Cree la solución y corrija todos los problemas. Para obtener más información acerca de la creación de proyectos y soluciones,	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	consulte la documentación de Visual Studio. Nota: A medida que cree la solución y compruebe su funcionalidad, es posible que identifique varios archivos adicionales para añadirlos a la solución, además de los archivos que identificó NDepend.	

Actualice su código de la aplicación.

Tarea	Descripción	Habilidades requeridas
Implementación de API web con ASP.NET Core.	Supongamos que uno de los microservicios que identificó en su aplicación heredada de carrito de compras monolítico es Productos. Usted creó un nuevo proyecto de API web de ASP.NET Core para Productos en la épica anterior. En este paso, usted identificará y modernizará todos los formularios web (páginas .aspx) relacionados con los Productos. Supongamos que Productos consta de cuatro formularios web, tal y como se ha ilustrado anteriormente en la sección de Arquitectura:	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	• Enumeración de los productos • Ver producto • Añadir/editar producto • Eliminar producto Debe analizar cada formulario web, identificar todas las solicitudes que se envían a la base de datos para realizar alguna lógica y obtener respuestas. Puede implementar cada solicitud como un punto de conexión de la API web. Gracias a sus formularios web, los productos pueden tener los siguientes puntos de conexión posibles: • `/api/products` • `/api/products/{id}` • `/api/products/add` • `/api/products/update/{id}` • `/api/products/delete/{id}` Como se mencionó anteriormente, también puede reutilizar todos los demás proyectos que haya actualizado a .NET 5, incluidos Business Logic,	

Tarea	Descripción	Habilidades requeridas
	Data Access y proyectos compartidos o comunes.	
Configura Amazon CloudWatch Logs.	Puedes usar Amazon CloudWatch Logs para monitorear, almacenar y acceder a los registros de tu aplicación. Puede registrar datos en Amazon CloudWatch Logs mediante un SDK de AWS. También puede integrar aplicaciones de.NET con CloudWatch Logs utilizando los marcos de registro de.NET más populares, como NLog, Log4Net y el marco de registro ASP.NET Core. Para obtener más información sobre este paso, consulte la entrada del blog Amazon CloudWatch Logs y.NET Logging Frameworks.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Configurar el almacén de parámetros de AWS Systems Manager.	Puede usar el Almacén de parámetros de AWS Systems Manager para almacenar la configuración de la aplicació n, como las cadenas de conexión, de forma separada del código de la aplicación. El NuGet paquete Amazon.Ex tensions.Configuration. SystemsManagersimplifica la forma en que su aplicación carga estos ajustes del AWS Systems Manager Parameter Store al sistema de configura ción .NET Core. Para obtener más información sobre este paso, consulte la entrada del blog Proveedor de configuración .NET Core para AWS Systems Manager.	Desarrollador de aplicaciones

Cómo añadir autenticación y autorización

Tarea	Descripción	Habilidades requeridas
Utilice una cookie compartida para la autenticación.	La modernización de una aplicación heredada monolític a es un proceso iterativo y requiere que el monolito y su versión modernizada coexistan. Puede usar una cookie compartida para lograr una autenticación perfecta	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	entre las dos versiones. La aplicación ASP.NET heredada sigue validando las credencia les de los usuarios y emite la cookie, mientras que la aplicación ASP.NET Core modernizada valida la cookie. Para obtener instrucciones y un código de muestra, consulte el GitHub proyecto de ejemplo.	

Compilación y ejecución del contenedor de forma local

Tarea	Descripción	Habilidades requeridas
Cree una imagen de Docker con Visual Studio.	En este paso, usted crea un archivo de Docker mediante la API web de Visual Studio para .NET Core. 1. Open Visual Studio. 2. En el explorador de soluciones, desde el menú contextual (haga clic con el botón derecho) de su proyecto, seleccione Añadir soporte de Docker. 3. Seleccione Linux como sistema operativo de destino .	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	Visual Studio crea un archivo de Docker para su proyecto. Para ver un archivo de muestra de Docker, consulte Herramientas de contenedor de Visual Studio para Docker en el sitio web de Microsoft.	

Tarea	Descripción	Habilidades requeridas
Cree y ejecute el contenedor mediante Docker Desktop.	Ahora puede compilar, crear y ejecutar el contenedor en Docker Desktop. 1. Abra una ventana del símbolo del sistema. Navegue hasta la carpeta de soluciones en la que se encuentra el archivo de Docker. Ejecute el siguiente comando para crear la imagen de Docker: `docker build -t aspnetcorewebapiimage -f Dockerfile .` 2. Ejecute el siguiente comando para ver todas las imágenes de Docker: `docker images` 3. Ejecute el siguiente comando para crear y ejecutar un contenedor: `docker run -d -p 8080:80 --name aspnetcorewebapicontainer aspnetcorewebapiimage` 4. Abra Docker Desktop y, a continuación, seleccione Contenedores/Aplicaciones. Puede ver un	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	nuevo contenedor llamado `aspnetcorewebapicontainer` ejecutándose.	

Recursos relacionados

- Ejecute un contenedor de Docker de la API web de ASP.NET Core en una instancia Linux de Amazon EC2 (Recomendaciones de AWS)
- Taller de Amazon ECS
- Realice implementaciones azul/verde de ECS mediante CodeDeploy AWS (documentación de CloudFormation AWS) CloudFormation
- Introducción a NDepend (documentación de NDepend)
- Asistente de portabilidad para .NET

Información adicional

En las tablas siguientes se proporcionan ejemplos de proyectos de muestra para una aplicación de carrito de compras heredada y los proyectos equivalentes de una aplicación ASP.NET Core modernizada.

Solución heredada:

Nombre del proyecto	Plantilla de proyecto	Target framework
Interfaz empresarial	Biblioteca de clases	.NET Framework
BusinessLogic	Biblioteca de clases	.NET Framework
WebApplication	Aplicación web ASP.NET Framework	.NET Framework
UnitTests	Proyecto NUnit Test	.NET Framework
Compartido ->Común	Biblioteca de clases	.NET Framework

Compartido ->Marco	Biblioteca de clases	.NET Framework

Nueva solución:

Nombre del proyecto	Plantilla de proyecto	Target framework
BusinessLogic	Biblioteca de clases	.NET 5.0
<WebAPI>	API web ASP.NET Core	.NET 5.0
<WebAPI>. UnitTests	Proyecto de prueba de NUnit 3	.NET 5.0
Compartido ->Común	Biblioteca de clases	.NET 5.0
Compartido ->Marco	Biblioteca de clases	.NET 5.0

Ejecute cargas de trabajo programadas y basadas en eventos a escala con AWS Fargate.

Creado por HARI OHM PRASATH RAJAGOPAL (AWS)

Entorno: PoC o piloto	Tecnologías: modernización; sin servidor; operaciones	Carga de trabajo: código abierto
Servicios de AWS: Amazon EC2 Container Registry; Amazon ECS; AWS; CodeCommit AWS Fargate; AWS Lambda; Amazon SNS		

Resumen

Este patrón describe cómo ejecutar cargas de trabajo programadas y basadas en eventos a escala en la nube de Amazon Web Services (AWS) mediante AWS Fargate.

En el caso de uso que configura este patrón, cada vez que se envía una solicitud de extracción, se escanea el código en busca de información confidencial de AWS, como el número de cuenta y las credenciales de AWS. La solicitud de extracción inicia una función de Lambda. La función de Lambda invoca una tarea de Fargate que se encarga del escaneo del código. Lambda se inicia cada vez que se genera una nueva solicitud de extracción. Si el escaneo encuentra información confidencial, Amazon Simple Notification Service (Amazon SNS) envía los resultados del escaneo en un mensaje de correo electrónico.

Este patrón resulta útil en los siguientes casos de uso empresarial:

- Si su empresa debe ejecutar muchas cargas de trabajo programadas y basadas en eventos que AWS Lambda no puede ejecutar debido a limitaciones en cuanto al tiempo de ejecución (un límite de 15 minutos) o la memoria
- Si desea que AWS administre las instancias aprovisionadas para estas cargas de trabajo

Al usar este patrón, tiene la opción de crear una nueva nube privada virtual (VPC).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- AWS CodeCommit para alojar la base de código y crear solicitudes de cambios
- Interfaz de la línea de comandos de AWS (AWS CLI) versión 1.7, instalada y configurada en Linux, macOS o Windows
- Cargas de trabajo que se ejecutan en contenedores
- Ejecutable de Apache Maven configurado en classpath

Arquitectura

El flujo general incluye los siguientes pasos.

1. Cada vez que se envía una nueva solicitud de extracción CodeCommit, se inicia una función Lambda. La función Lambda escucha el evento a `CodeCommit Pull Request State Change` través de Amazon. EventBridge
2. La función de Lambda envía una nueva tarea de Fargate con los siguientes parámetros de entorno para extraer el código y escanearlo.

   ```
   RUNNER # <<TaskARN>>
   SNS_TOPIC # <<SNSTopicARN>>
   SUBNET # <<Subnet in which Fargate task gets launched>>
   ```

   Si el escaneo encuentra información confidencial en el código, Fargate envía un nuevo mensaje al tema Amazon SNS.
3. Un suscriptor de SNS lee el mensaje del tema y envía un mensaje de correo electrónico.

Tecnología

- AWS CodeCommit
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon Elastic Container Service (Amazon ECS)

- Amazon EventBridge
- AWS Fargate
- AWS Lambda
- Amazon SNS
- Docker

Herramientas

Herramientas

- La interfaz de la línea de comandos (CLI) de AWS es una herramienta unificada para administrar los servicios de AWS.
- AWS CodeCommit: AWS CodeCommit es un servicio de control de código fuente totalmente gestionado que aloja repositorios seguros basados en Git. Al usarlo CodeCommit, los equipos pueden colaborar en el código en un entorno seguro y altamente escalable.
- Amazon Elastic Container Registry (Amazon ECR) es un registro de contenedores de Docker completamente administrado que facilita el almacenamiento, la administración y la implementación de imágenes de contenedores de Docker.
- Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores muy escalable y rápido. Puede utilizar Amazon ECS para ejecutar, detener y administrar contenedores en un clúster.
- AWS Fargate: AWS Fargate es una tecnología que se puede utilizar en Amazon ECS para ejecutar contenedores sin tener que administrar servidores ni clústeres de instancias de Amazon EC2.
- AWS Lambda: AWS Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) es un servicio administrado con el que se ofrece la entrega de mensajes de los publicadores a los suscriptores (también conocido como productores y consumidores). Los publicadores se comunican de forma asíncrona con los suscriptores mediante el envío mensajes a un tema, que es un punto de acceso lógico y un canal de comunicación. Los clientes pueden suscribirse al tema de SNS y recibir mensajes publicados mediante un tipo de protocolo compatible, como Lambda, correo electrónico, notificaciones push móviles y mensajes de texto móviles (SMS).
- Docker ayuda a crear, probar y entregar aplicaciones en paquetes llamados contenedores.

- Cliente Git: herramienta de línea de comandos o de escritorio para comprobar los artefactos necesarios
- Maven: Apache Maven es una herramienta de gestión de proyectos para gestionar de forma centralizada la creación, los informes y la documentación de un proyecto.

Epics

Configurar un repositorio local

Tarea	Descripción	Habilidades requeridas
Descargue el código.	En la sección de Adjuntos, descargue el archivo .zip y extraiga los archivos.	Desarrollador, administrador del sistema AWS
Configure el repositorio.	Ejecute `mvn clean install` en la carpeta raíz.	Desarrollador, administrador del sistema AWS

Cree una imagen de Amazon ECR e inserte la imagen

Tarea	Descripción	Habilidades requeridas
Cree un repositorio de Amazon ECR e inicie sesión.	Abra la consola de Amazon ECR. En el panel de navegación, seleccione Repositories (Repositorios) y seleccione Create repositor y (Crear repositorio). Para obtener ayuda con esta y otras explicaciones, consulte la sección Recursos relaciona dos.	Desarrollador, administrador del sistema AWS
Envíe la imagen del contenedor:	Abra el repositorio, seleccion e View push commands (Ver comandos push) e inicie	Desarrollador, administrador del sistema AWS

Tarea	Descripción	Habilidades requeridas
	sesión en Docker. Una vez iniciada la sesión, ejecute los comandos, con las sustituciones necesarias, que se encuentran bajo Push the container image (Inserte la imagen del contenedor) en la sección Additional information (Información adicional). De este modo, se carga la imagen del contenedor de Docker que se utiliza para escanear el código. Cuando se complete la carga, copie la URL de la última compilación en el repositorio de Amazon ECR.	

Cree el CodeCommit repositorio

Tarea	Descripción	Habilidades requeridas
Cree el CodeCommit repositorio.	Para crear un CodeCommit repositorio de AWS nuevo, ejecute el comando en Crear el CodeCommit repositorio en la sección Información adicional.	Desarrollador, administrador del sistema AWS

Crear la VPC (opcional)

Tarea	Descripción	Habilidades requeridas
Cree una VPC.	Si desea utilizar una VPC nueva en lugar de una existente, ejecute los comandos de Create a VPC (Cree una VPC) en la sección Additional informati on (Información adicional). El script del AWS Cloud Development Kit (AWS CDK) generará los ID de la VPC y la subred que se crearon.	Desarrollador, administrador del sistema AWS

Cree el clúster de Amazon ECS y la tarea Fargate

Tarea	Descripción	Habilidades requeridas
Cree el clúster y la tarea.	Para crear un clúster de Amazon ECS y una definició n de tarea de Fargate, ejecute los comandos de Create the cluster and task (Cree el clúster y la tarea) en la sección Additional informati on (Información adicional). Asegúrese de que el ID de VPC y el URI del repositorio de Amazon ECR correctos se pasen como parámetros mientras se ejecuta el script de intérprete de comandos. El script crea una definició n de tarea de Fargate que	Desarrollador, administrador del sistema AWS

Tarea	Descripción	Habilidades requeridas
	apunta a la imagen de Docker (responsable del escaneo). A continuación, el script crea un trabajo y un rol de ejecución asociado.	
Verifique el clúster de Amazon ECS.	Abra la consola de Amazon ECS. En el panel de navegación, seleccione Clusters y elija el clúster de Amazon ECS recién creado denominado Fargate-Job-Cluster. Después, elija Definición de tarea en el panel de navegación y confirme que haya una nueva definició n de tarea con el prefijo `awscdkfargateecsTa skDef` .	Desarrollador, administrador del sistema AWS

Crear un tema de SNS y una suscripción.

Tarea	Descripción	Habilidades requeridas
Cree un tema de SNS.	Para crear un tema de SNS, ejecute el comando que se encuentra en Create the SNS topic (Crear el tema de SNS), en la sección Additiona l information (Información adicional). Cuando la creación se haya realizado correctam ente, anote el `SNS ARN`, que	Desarrollador, administrador del sistema AWS

Tarea	Descripción	Habilidades requeridas
	se utilizará en el siguiente paso.	
Cree el suscriptor de SNS.	Para crear un correo suscriptor para el tema SNS, ejecute el comando que se encuentra en Create the SNS subscriber (Crear el tema de suscriptor SNS), en la sección Información adicional. Asegúrese de reemplazar `TopicARN` y `Email address` utilizados en el comando CLI. Para recibir notificaciones por correo electrónico, asegúrese de confirmar la dirección de correo electrónico que utiliza como suscriptor.	Desarrollador, administrador del sistema AWS

Cree la función Lambda y active CodeCommit

Tarea	Descripción	Habilidades requeridas
Cree la función y el desencadenador.	Para crear una función Lambda con un CodeCommit activador, ejecute el comando en Función y CodeCommit disparador Lambda en la sección Información adicional. Asegúrese de reemplazar los parámetros por los valores correspondientes antes de ejecutar el comando. El script crea la función de Lambda y la configura para que se invoque	Desarrollador, administrador del sistema AWS

Tarea	Descripción	Habilidades requeridas
	cuando se realice una nueva solicitud de extracción.	

Pruebe la aplicación

Tarea	Descripción	Habilidades requeridas
Probar la aplicación.	Si registra información confidencial de AWS en el CodeCommit repositorio, se debe iniciar la función Lambda. La función de Lambda inicia la tarea Fargate, que escanea el código y envía los resultados del escaneo en una notificac ión por correo electrónico.	Desarrollador, administrador del sistema AWS

Recursos relacionados

- Creación de un nuevo repositorio de Amazon ECR
- Inserción de imágenes de Windows en Amazon ECR

Información adicional

Inserte la imagen del contenedor

```
> cd 1-ecr-image-push
> ./run.sh <<ecr-repository>>
```

Cree el repositorio CodeCommit

```
aws codecommit create-repository --repository-name test-repo --repository-description
 "My Test repository"
```

Creación de una VPC

```
> cd 2-create-vpc
> ./run.sh
```

Salida

```
aws-batch-cdk-vpc-efs-launch-template.privatesubnet = subnet-<<id>>
aws-batch-cdk-vpc-efs-launch-template.publicsubnet = subnet-<<id>>
aws-batch-cdk-vpc-efs-launch-template.vpcid = vpc-<<id>>
```

Cree el clúster y la tarea

```
> export CDK_DEFAULT_ACCOUNT = <<aws_account_id>>
> export CDK_DEFAULT_REGION = <<aws_region>>
> cd 3-create-ecs-task
> ./run.sh <<vpc-id>> <<ecr-repo-uri>>
```

Salida

```
aws-cdk-fargate-ecs.CLUSTERNAME = Fargate-Job-Cluster
aws-cdk-fargate-ecs.ClusterARN = <<cluster_arn>>
aws-cdk-fargate-ecs.ContainerARN = Fargate-Container
aws-cdk-fargate-ecs.TaskARN = <<task_arn>>
aws-cdk-fargate-ecs.TaskExecutionRole = <<execution_role_arn>>
aws-cdk-fargate-ecs.TaskRole = <<task_role_arn>>
```

Cree el tema de SNS

```
aws sns create-topic --name code-commit-topic
```

Cree el suscriptor de SNS

```
aws sns subscribe \
    --topic-arn <<topic_arn>> \
    --protocol email \
```

```
    --notification-endpoint <<email_address>>
```

Función Lambda y disparador CodeCommit

```
> export CDK_DEFAULT_ACCOUNT = <<aws_account_id>>
> export CDK_DEFAULT_REGION = <<aws_region>>
> cd 5-Lambda-CodeCommit-Trigger
> ./run.sh <<taskarn>> <<snstopicarn>> subnet-<<id>> <<codecommitarn>>
```

Salida

```
aws-cdk-fargate-lambda-event.Cloudwatchrule = <<cloudwatchrule>>
aws-cdk-fargate-lambda-event.CodeCommitLambda = AWS-Code-Scanner-Function
aws-cdk-fargate-lambda-event.LambdaRole = <<lambdaiamrole>>
```

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Incorporación de inquilinos en la arquitectura SaaS para el modelo de silo mediante C# y AWS CDK

Creado por Tabby Ward (AWS), Susmitha Reddy Gankidi (AWS) y Vijai Anand Ramalingam (AWS)

Repositorio de código: Tennat Onboarding Silo	Entorno: PoC o piloto	Tecnologías: modernización; nativa de la nube; SaaS; DevOps
Carga de trabajo: código abierto	Servicios de AWS: AWS CloudFormation; Amazon DynamoDB; Amazon DynamoDB Streams; AWS Lambda; Amazon API Gateway	

Resumen

Las aplicaciones de software como servicio (SaaS) se pueden crear con una variedad de modelos arquitectónicos diferentes. El modelo de silo se refiere a una arquitectura en la que los inquilinos reciben recursos específicos.

Las aplicaciones SaaS se basan en un modelo sencillo para introducir nuevos inquilinos en su entorno. Esto suele requerir la orquestación de varios componentes para aprovisionar y configurar correctamente todos los elementos necesarios para crear un nuevo inquilino. Este proceso, en la arquitectura SaaS, se denomina incorporación de inquilinos. La incorporación debe automatizarse por completo en todos los entornos de SaaS y utilizar la infraestructura como código en el proceso de incorporación.

Este patrón le guía a través de un ejemplo de creación de un inquilino y aprovisionamiento de una infraestructura básica para el inquilino en Amazon Web Services (AWS). El patrón utiliza C# y el AWS Cloud Development Kit (AWS CDK).

Como este patrón crea una alarma de facturación, le recomendamos implementar la pila en la región Este de EE. UU. (Norte de Virginia) o us-east-1 de AWS. Para obtener más información, consulte la documentación de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una entidad principal de AWS Identity and Access Management (IAM) con acceso suficiente de IAM para crear recursos de AWS para este patrón. Para obtener más información, consulte Roles de IAM.
- Instale Amazon Command Line Interface (AWS CLI) y configure la CLI de AWS para realizar la implementación de la CDK de AWS.
- Visual Studio 2022 descargado o instalado o Visual Studio Code descargado o instalado.
- Configuración de AWS Toolkit para Visual Studio.
- .NET Core 3.1 o posterior (necesario para las aplicaciones de AWS CDK de C#)
- Amazon.Lambda.Tools instalado.

Limitaciones

- La CDK de AWS utiliza AWS CloudFormation, por lo que las aplicaciones de la CDK de AWS están sujetas a cuotas de CloudFormation servicio. Para obtener más información, consulte CloudFormation Cuotas de AWS.
- La CloudFormation pila de inquilinos se crea con un rol de CloudFormation servicio `infra-cloudformation-role` con caracteres comodín en las acciones (`sns*` `ysqs*`), pero con los recursos limitados al `tenant-cluster` prefijo. Para un caso de uso de producción, evalúe esta configuración y proporcione únicamente el acceso obligatorio a este rol de servicio. La función `InfrastructureProvision` Lambda también usa un carácter comodín (`cloudformation*`) para aprovisionar la CloudFormation pila, pero con los recursos limitados al prefijo. `tenant-cluster`
- La compilación de docker de este ejemplo de código utiliza `--platform=linux/amd64` para forzar imágenes basadas en `linux/amd64`. Esto es para garantizar que los artefactos de imagen finales sean adecuados para Lambda, que de forma predeterminada utiliza una arquitectura x86-64. Si necesita cambiar la arquitectura Lambda de destino, asegúrese de cambiar los códigos CDK de Dockerfiles y de AWS. Para obtener más información, consulte esta entrada de blog: Migración de funciones de Lambda de AWS a procesadores AWS Graviton2 basados en ARM.

- El proceso de eliminación de la pila no limpiará CloudWatch los registros (grupos de registros y registros) generados por la pila. Debe limpiar los registros manualmente a través de la consola de administración de AWS, la CloudWatch consola Amazon o la API.

Este patrón se configura a modo de ejemplo. Para su uso en producción, evalúe las siguientes configuraciones y realice los cambios en función de los requisitos de su empresa:

- Para simplificar, el bucket de AWS Simple Storage Service (Amazon S3) de este ejemplo no tiene habilitado el control de versiones. Evalúe y actualice la configuración según sea necesario.
- Para simplificar, en este ejemplo se configuran los puntos de conexión de la API de REST de Amazon API Gateway sin autenticación, autorización ni limitación. Para uso en producción, recomendamos integrar el sistema con la infraestructura de seguridad empresarial. Evalúe esta configuración y añada la configuración de seguridad necesaria según sea necesario.
- Para este ejemplo de infraestructura de inquilinos, Amazon Simple Notification Service (Amazon SNS) y Amazon Simple Queue Service (Amazon SQS) solo tienen configuraciones mínimas. El AWS Key Management Service (AWS KMS) de cada inquilino permite que los servicios de Amazon CloudWatch y Amazon SNS de la cuenta los consuman según la política de claves de AWS KMS. La configuración es solo un marcador de posición de ejemplo. Ajuste las configuraciones según sea necesario en función de su caso de uso empresarial.
- Toda la configuración, que incluye, entre otros, el aprovisionamiento y la eliminación de los puntos de enlace de las API y de los inquilinos de backend mediante AWS CloudFormation, abarca únicamente el caso básico de la ruta feliz. Evalúe y actualice la configuración con la lógica de reintentos necesaria, la lógica adicional de gestión de errores y la lógica de seguridad en función de las necesidades de su empresa.
- En el momento de escribir este artículo, el código de ejemplo se ha probado con up-to-date cdk-nag para comprobar si existen políticas. Es posible que se apliquen nuevas políticas en el futuro. Es posible que estas nuevas políticas requieran que modifique manualmente la pila en función de las recomendaciones antes de poder implementarla. Revise el código existente para asegurarse de que se ajusta a los requisitos de su empresa.
- El código se basa en la CDK de AWS para generar un sufijo al azar en lugar de depender de nombres físicos estáticos asignados a la mayoría de los recursos creados. Esta configuración sirve para garantizar que estos recursos sean únicos y no entren en conflicto con otras pilas. Para obtener más información, consulte la documentación de AWS CDK. Ajústelo en función de los requisitos de su empresa.

- Este código de ejemplo empaqueta artefactos .NET Lambda en imágenes basadas en Docker y se ejecuta con el Tiempo de ejecución de imágenes de contenedor proporcionado por Lambda. El tiempo de ejecución de la imagen del contenedor presenta ventajas como mecanismo estándar de transferencia y almacenamiento (registros de contenedores) y entornos de prueba locales más precisos (a través de la imagen del contenedor). Puede cambiar el proyecto para que utilice los tiempos de ejecución de .NET proporcionados por Lambda para reducir el tiempo de compilación de las imágenes de Docker, pero después tendrá que configurar los mecanismos de transferencia y almacenamiento y asegurarse de que la configuración local coincida con la configuración de Lambda. Ajuste el código para adaptarlo a los requisitos empresariales de los usuarios.

Versiones de producto

- CDK de AWS, versión 2.45.0 o posterior
- Visual Studio 2022

Arquitectura

Pila de tecnología

- Amazon API Gateway
- AWS CloudFormation
- Amazon CloudWatch
- Amazon DynamoDB
- AWS Identity y Access Management (IAM)
- AWS KMS
- AWS Lambda
- Amazon S3
- Amazon SNS
- Amazon SQS

Arquitectura

En el siguiente diagrama se muestra el flujo de creación de la pila de inquilinos. Para obtener más información sobre los paquetes de tecnología del plano de control y del inquilino, consulte la sección de Información adicional.

Flujo de creación de pilas de inquilinos

1. El usuario envía una solicitud de API POST con la carga útil del nuevo inquilino (nombre del inquilino, descripción del inquilino) en JSON a una API de REST alojada en Amazon API Gateway. La API de puerta de enlace procesa la solicitud y la reenvía a la función de Lambda backend de incorporación de inquilinos. En este ejemplo, no hay autorización ni autenticación. En una configuración de producción, esta API debe integrarse con el sistema de seguridad de la infraestructura SaaS.
2. La función de incorporación de inquilinos verifica la solicitud. A continuación, intenta almacenar el registro del inquilino, que incluye el nombre del inquilino, el identificador único universal (UUID) generado y la descripción del inquilino, en la tabla de incorporación de inquilinos de Amazon DynamoDB.
3. Una vez que DynamoDB almacena el registro, una transmisión de DynamoDB inicia la función de infraestructura de inquilinos de Lambda descendente.
4. La función de Lambda de la infraestructura de inquilino actúa en función de la transmisión de DynamoDB recibida. Si la transmisión es para el evento INSERT, la función utiliza la NewImage sección de la transmisión (registro de última actualización, campo Nombre del inquilino) CloudFormation para crear una nueva infraestructura de arrendatario utilizando la plantilla que está almacenada en el bucket de S3. La CloudFormation plantilla requiere el parámetro Tenant Name.
5. AWS CloudFormation crea la infraestructura de inquilinos en función de la CloudFormation plantilla y los parámetros de entrada.
6. Cada configuración de infraestructura arrendataria tiene una CloudWatch alarma, una alarma de facturación y un evento de alarma.
7. El evento de alarma se convierte en un mensaje dirigido a un tema de SNS, que se cifra con la clave de AWS KMS del inquilino.
8. El tema de SNS reenvía el mensaje de alarma recibido a la cola de SQS, que está cifrada por la clave de cifrado AWS KMS del inquilino.

Se pueden integrar otros sistemas con Amazon SQS para realizar acciones basadas en los mensajes en cola. En este ejemplo, para mantener el código genérico, los mensajes entrantes permanecen en cola y es necesario eliminarlos manualmente.

Flujo de eliminación de pilas de inquilinos

1. El usuario envía una solicitud de DELETE API con la carga útil del nuevo inquilino (nombre del inquilino, descripción del inquilino) en JSON a la API de REST alojada por Amazon API Gateway, que procesará la solicitud y la reenviará a la función de incorporación de inquilino. En este ejemplo, no hay autorización ni autenticación. En una configuración de producción, esta API se integrará con el sistema de seguridad de la infraestructura SaaS.
2. La función de incorporación de inquilinos verificará la solicitud y, a continuación, intentará eliminar el registro del inquilino (nombre del inquilino) de la tabla de incorporación de inquilinos.
3. Una vez que DynamoDB elimina el registro correctamente (el registro existe en la tabla y se elimina), una transmisión de DynamoDB inicia la función de infraestructura de inquilinos de Lambda descendente.
4. La función de Lambda de la infraestructura de inquilino actúa en base a la transmisión de DynamoDB recibida. Si la transmisión es para el evento REMOVE, la función usa la OldImage sección del registro (información del registro y campo Nombre del inquilino, antes del último cambio, que es eliminar) para iniciar la eliminación de una pila existente en función de la información de ese registro.
5. AWS CloudFormation elimina la pila de inquilinos de destino en función de la entrada.

Herramientas

Servicios de AWS

- Amazon API Gateway le ayuda a crear, publicar, mantener, supervisar y proteger REST, HTTP y WebSocket API a cualquier escala.
- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura de la nube de AWS en código.
- Kit de herramientas de AWS CDK es un kit de desarrollo en la nube de línea de comandos que ayuda a interactuar con la aplicación AWS Cloud Development Kit (AWS CDK).
- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.
- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.

- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Key Management Service (AWS KMS) facilita poder crear y controlar claves criptográficas para proteger los datos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- Amazon Simple Queue Service (Amazon SQS) ofrece una cola alojada segura, duradera y disponible que le permite integrar y desacoplar sistemas y componentes de software distribuidos.
- AWS Toolkit para Visual Studio es un complemento para el entorno de desarrollo integrado (IDE) de Visual Studio. El Toolkit para Visual Studio permite desarrollar, depurar e implementar aplicaciones .NET que utilizan los servicios de AWS.

Otras herramientas

- Visual Studio es un entorno de desarrollo integrado (IDE) que incluye compiladores, herramientas de finalización de código, diseñadores gráficos y otras características que facilitan el desarrollo de software.

Código

El código de este patrón se encuentra en el repositorio de Incorporación de inquilinos en la arquitectura SaaS para el modelo silo Ejemplo APG.

Epics

Configure AWS CDK

Tarea	Descripción	Habilidades requeridas
Compruebe la instalación de Node.js.	Para comprobar que Node.js esté instalado en su equipo local, ejecute el siguiente comando. `node --version`	Administrador de AWS, AWS DevOps
Instale el kit de herramientas de AWS CDK.	Para instalar el kit de herramientas de AWS CDK en su equipo local, ejecute el siguiente comando. `npm install -g aws-cdk` Si npm no está instalado, puede instalarlo desde el sitio Node.js.	Administrador de AWS, AWS DevOps
Compruebe la versión del kit de herramientas de AWS CDK.	Para comprobar que la versión del kit de herramientas de AWS CDK esté instalada correctamente en su equipo, ejecute el siguiente comando. `cdk --version`	Administrador de AWS, AWS DevOps

Revise el código del plano de control de incorporación del inquilino

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Clone el repositorio y navegue hasta la carpeta `\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example` . Abra la solución `\src\TenantOnboardingInfra.sln` en Visual Studio 2022. Abra el archivo `TenantOnboardingInfraStack.cs` y revise el código. Los siguientes recursos se crean como parte de esta pila: • Tabla de DynamoDB • Depósito de S3 (cargue la CloudFormation plantilla en el depósito de S3). • Rol de ejecución de Lambda • Función de Lambda • API de API Gateway • Origen de eventos de la función de Lambda	Administrador de AWS, AWS DevOps
Revise la CloudFormation plantilla.	En la `\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example\template` carpetainfra.yaml , abra	Desarrollador de aplicaciones, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	y revise la CloudFormation plantilla. Esta plantilla se completará con el nombre del inquilino obtenido de la tabla de DynamoDB de incorpora ción de inquilinos. La plantilla proporciona la infraestructura específica para cada inquilino. En este ejemplo, aprovisiona la clave AWS KMS, Amazon SNS, Amazon SQS y la alarma. CloudWatch	

Tarea	Descripción	Habilidades requeridas
Revise la función de incorporación de inquilinos.	Abra `Function.cs` y revise el código de la función de incorporación de inquilinos, que se crea con la plantilla AWS Lambda Project (.NET Core- C#) de Visual Studio con el esquema .NET 6 (Imagen contenedora). Abra `Dockerfile` y revise el código. `Dockerfile` es un archivo de texto que contiene instrucciones para crear la imagen del contenedor de Lambda. Tenga en cuenta que los siguientes NuGet paquetes se añaden como dependencias al `TenantOnboardingFunction` proyecto: • `Amazon.Lambda.APIGatewayEvents` • `AWSSDK.DynamoDBv2` • `Newtonsoft.Json`	Desarrollador de aplicaciones, AWS DevOps

Tarea	Descripción	Habilidades requeridas
Revise la InfraProvisioning función Tenant.	Vaya a `\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example\src\InfraProvisioningFunction` . Abra `Function.cs` y revise el código de la función de aprovisionamiento de la infraestructura inquilina, que se crea con la plantilla AWS Lambda Project (.NET Core-C#) de Visual Studio con el esquema .NET 6 (Imagen contenedora). Abra `Dockerfile` y revise el código. Tenga en cuenta que los siguientes NuGet paquetes se agregan como dependencias al `InfraProvisioningFunction` proyecto: • `Amazon.Lambda.DynamoDBEvents` • `AWSSDK.DynamoDBv2` • `AWSSDK.Cloudformation`	Desarrollador de aplicaciones, AWS DevOps

Implementar recursos de AWS

Tarea	Descripción	Habilidades requeridas
Compilar la solución.	Para crear la solución, siga los pasos que se indican a continuación: 1. Abra la solución `\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example\src\TenantOnboardingInfra.sln` en Visual Studio 2022. 2. Abra el menú contextual (clic derecho) de la solución y elija Build solution (Compilar solución). Nota: Asegúrese de actualizar el paquete `Amazon.CDK.Lib NuGet` a la última versión del proyecto `\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example\src\TenantOnboardingInfra` antes de crear la solución.	Desarrollador de aplicaciones
Inicie el entorno de AWS CDK.	Abra la línea de comandos de Windows y vaya a la carpeta raíz de la aplicación AWS CDK donde está disponibl	Administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	e el archivo `cdk.json` (`\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example`). Ejecute el siguiente comando para el arranque. `cdk bootstrap` Si ha creado un perfil de AWS para las credenciales, utilice el comando con su perfil. `cdk bootstrap --profile <profile name>`	
Enumere las pilas de CDK de AWS.	Para obtener una lista de todas las pilas que se van a crear como parte de este proyecto, ejecute el siguiente comando. `cdk ls` `cdk ls --profile <profile name>` Si ha creado un perfil de AWS para las credenciales, utilice el comando con su perfil. `cdk ls --profile <profile name>`	Administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
Revise qué recursos de AWS se crearán.	Para revisar todos los recursos de AWS que se crearán como parte de este proyecto, ejecute el siguiente comando. `cdk diff` Si ha creado un perfil de AWS para las credenciales, utilice el comando con su perfil. `cdk diff --profile <profile name>`	Administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
Implemente todos los recursos de AWS mediante AWS CDK.	Use el siguiente comando para implementar todos los recursos de AWS. `cdk deploy --all --require-approval never` Si ha creado un perfil de AWS para las credenciales, utilice el comando con su perfil. `cdk deploy --all --require-approval never --profile <profile name>` Una vez completada la implementación, copie la URL de la API de la sección de resultados de la línea de comandos, como se muestra en el siguiente ejemplo. `Outputs: TenantOnboardingInfraStack.TenantOnboardingAPIEndpoint42E526D7 = https://j2qmp8ds21i1i.execute-api.us-west-2.amazonaws.com/prod/`	Administrador de AWS, AWS DevOps

Verificar la funcionalidad

Tarea	Descripción	Habilidades requeridas
Cree un nuevo inquilino.	Para crear el nuevo inquilino, envíe la siguiente solicitud de curl. `curl -X POST <TenantOnboardingAPIEndpoint* from CDK Output>tenant -d '{"Name":"Tenant123", "Description":"Stack for Tenant123"}'` Cambie el marcador de posición `<TenantOnboardingAPIEndpoint* from CDK Output>` por el valor real de AWS CDK, como se muestra en el siguiente ejemplo. `curl -X POST https://j2qmp8ds21i1i.execute-api.us-west-2.amazonaws.com/prod/tenant -d '{"Name": "Tenant123", "Description":"test12"}'` En el siguiente ejemplo, se muestra el resultado. `{"message": "A new tenant added - 5/4/2022 7:11:30 AM"}`	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
Compruebe los detalles del inquilino recién creado en DynamoDB.	Para comprobar los detalles del inquilino recién creado en DynamoDB, siga estos pasos. 1. Abra la consola de administración de AWS y navegue hasta el servicio Amazon DynamoDB. 2. En el menú de navegación de la izquierda, elija Explorar elementos y elija la tabla `Tenant0nboarding` . Nota: El nombre del inquilino irá precedido de `tenantcluster-` . Para obtener más información, consulte la sección Additional information (Información adicional). 3. Compruebe que se ha creado un elemento nuevo con los detalles del inquilino .	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
Verifique la creación de la pila para el nuevo inquilino.	Compruebe que la nueva pila se haya creado correctam ente y se haya aprovisionado con la infraestructura para el inquilino recién creado de acuerdo con la CloudForm ation plantilla. 1. Abre la CloudFormation consola. 2. En el menú de navegació n de la izquierda, elija Pilas y compruebe que se haya creado correctamente una pila con el nombre del inquilino. 3. Elija la pila de inquilinos de recién creada y, a continuac ión, elija la pestaña Resources (Recursos). Anote el recurso de alarma y el recurso de Amazon SQS. 4. Abra una nueva terminal con las credenciales de AWS configuradas y apunte a la región correcta. Para activar una alarma de prueba, introduzca el siguiente código, sustituye ndo `<alarm resource name>` por el nombre del recurso de alarma indicado en el paso 3.	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`aws cloudwatch set-alarm-state --alarm-name <alarm resource name> --state-value ALARM --state-reason 'Test setup'` En el siguiente ejemplo se muestra el código con un nombre de recurso de alarma. `aws cloudwatch set-alarm-state --alarm-name tenantcluster-tenant123-alarm --state-value ALARM --state-reason 'Test setup'` 5. Abra la consola y vaya a la consola de Amazon SQS. Elija el nombre del recurso de Amazon SQS identificado en el paso 3. Siga las Instrucciones de la documentación de AWS para recibir y eliminar el mensaje de prueba de la alarma que se activó en el paso 4.	

Tarea	Descripción	Habilidades requeridas
Elimine la pila de inquilinos.	Para eliminar la nueva pila de inquilinos, envíe la siguiente solicitud de curl. `curl -X DELETE <TenantOnboardingAPIEndpoint* from CDK Output>tenant/<Tenant Name from previous step>` Cambie el marcador de posición `<TenantOnboardingAPIEndpoint* from CDK Output>` por el valor real de AWS CDK y cambie `<Tenant Name from previous step>` por el valor real del paso anterior de creación del inquilino , como se muestra en el siguiente ejemplo. `curl -X DELETE https://j2qmp8ds21i1i.execute-api.us-west-2.amazonaws.com/prod/tenant/Tenant123` En el siguiente ejemplo, se muestra el resultado. `{"message": "Tenant destroyed - 5/4/2022 7:14:48 AM"}`	Desarrollador de aplicaciones, AWS DevOps, administrador de AWS

Tarea	Descripción	Habilidades requeridas
Verifique la eliminación de la pila para el inquilino existente.	Para comprobar que se ha eliminado la pila de inquilinos existente, siga estos pasos: 1. Abra la consola y navegue hasta la CloudFormation consola. 2. En el panel de navegación de la izquierda, compruebe que la pila existente con el nombre del inquilino ya no esté en la CloudForm ation consola (si la consola está configurada para mostrar solo las pilas activas) o que esté en proceso de borrarse. Si la pila ya no está en la CloudFormation consola, usa la lista desplegable para cambiar la configura ción de la consola de Activa a Eliminada para ver la pila eliminada y comprobar que la pila se ha eliminado correctamente.	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps

Limpieza

Tarea	Descripción	Habilidades requeridas
Destruya el entorno.	Antes de limpiar la pila, asegúrese de lo siguiente:	Administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	• Todos los registros de DynamoDB se han eliminado mediante la operación de eliminación de inquilinos anterior o mediante la consola o la API de DynamoDB. Cada vez que se elimine un registro de inquilino, se iniciará la limpieza de su CloudFormation homólogo de AWS. • Todas las CloudFormation pilas de AWS basadas en inquilinos se limpian (en caso de que falle la lógica de limpieza del activador de DynamoDB) en la consola de AWS. CloudFormation Una vez finalizadas las pruebas, se puede usar AWS CDK para destruir todas las pilas y los recursos relacionados mediante la ejecución del siguiente comando. `cdk destroy --all;` Si ha creado un perfil de AWS para las credenciales, utilice el perfil.	

Tarea	Descripción	Habilidades requeridas
	Confirme la solicitud de eliminación de la pila para eliminarla.	
Limpia Amazon CloudWatch Logs.	El proceso de eliminación de la pila no limpiará CloudWatch los registros (grupos de registros y registros) generados por la pila. Limpie los CloudWatch recursos manualmente mediante la CloudWatch consola o la API.	Desarrollador de aplicaciones, AWS DevOps, administrador de AWS

Recursos relacionados

- Taller sobre AWS CDK .NET
- Utilización de AWS CDK en C#
- Referencia de CDK .NET

Información adicional

Conjunto de tecnologías de plano de control

El código CDK escrito en .NET se utiliza para aprovisionar la infraestructura del plano de control, que consta de los siguientes recursos:

1. API Gateway

   Sirve como punto de entrada de la API de REST para la pila del plano de control.

2. Función de Lambda de incorporación de inquilinos

   La puerta de enlace de API inicia esta función de Lambda mediante el método m.

   Una solicitud de API del método POST hace que (`tenant name`, `tenant description`) se inserte en la tabla de DynamoDB `Tenant Onboarding`.

En este ejemplo de código, el nombre del inquilino también se usa como parte del nombre de la pila de inquilinos y de los nombres de los recursos de esa pila. Esto es para facilitar la identificación de estos recursos. El nombre de este inquilino debe ser único en la configuración para evitar conflictos o errores. La configuración detallada de la validación de entradas se explica en la documentación sobre los roles de IAM y en la sección de Limitations (Limitaciones).

El proceso de persistencia en la tabla de DynamoDB solo tendrá éxito si el nombre del inquilino no se utiliza en ningún otro registro de la tabla.

En este caso, el nombre del inquilino es la clave de partición de esta tabla, ya que solo la clave de partición se puede usar como expresión de condición `PutItem`.

Si el nombre del inquilino nunca se registró antes, el registro se guardará correctamente en la tabla.

Sin embargo, si un registro existente de la tabla ya utiliza el nombre del inquilino, la operación fallará e iniciará una excepción de DynamoDB `ConditionalCheckFailedException`. La excepción se utilizará para devolver un mensaje de error (`HTTP BadRequest`) que indique que el nombre del inquilino ya existe.

Una solicitud de API de método `DELETE` eliminará el registro de un nombre de inquilino específico de la tabla `Tenant Onboardin`.

La eliminación del registro de DynamoDB en este ejemplo se realizará correctamente aunque el registro no exista.

Si el registro de destino existe y se elimina, se creará un registro de transmisión de DynamoDB. De lo contrario, no se creará ningún registro posterior.

3. Incorporación de DynamoDB por parte del inquilino, con Amazon DynamoDB Streams habilitado

   Esto registra la información de los metadatos del inquilino y cualquier registro que se guarde o elimine enviará un flujo descendente a la función de Lambda `Tenant Infrastructure`.

4. Función de Lambda de infraestructura inquilina

   Esta función de Lambda la inicia el registro de flujo de DynamoDB del paso anterior. Si el registro corresponde a un `INSERT` evento, invoca CloudFormation a AWS para crear una nueva infraestructura de inquilinos con la CloudFormation plantilla que está almacenada en un bucket

de S3. Si el registro es para `REMOVE`, se inicia la eliminación de una pila existente en función del campo del registro de transmisión `Tenant Name`.

5. S3 bucket

   Esto sirve para almacenar la CloudFormation plantilla.

6. Funciones de IAM para cada función de Lambda y una función de servicio para CloudFormation

   Cada función de Lambda tiene su rol de IAM único con permisos de privilegio mínimo para realizar su tarea. Por ejemplo, la función de Lambda `Tenant On-boarding` tiene acceso de lectura y escritura a DynamoDB y la función de Lambda `Tenant Infrastructure` solo puede leer el flujo de DynamoDB.

   Se crea un rol CloudFormation de servicio personalizado para el aprovisionamiento de la pila de inquilinos. Esta función de servicio contiene permisos adicionales para el aprovisionamiento de CloudFormation pilas (por ejemplo, la clave de AWS KMS). Esto divide las funciones entre Lambda y CloudFormation evita todos los permisos en una sola función (función de Infraestructura Lambda).

   Los permisos que permiten realizar acciones poderosas (como crear y eliminar CloudFormation pilas) están bloqueados y solo se permiten en los recursos que comienzan con. `tenantcluster-` La excepción es AWS KMS, debido a su convención de nomenclatura de recursos. El nombre del inquilino introducido por la API irá precedido de `tenantcluster-` así como otras comprobaciones de validación (alfanuméricas solo con guiones y limitadas a menos de 30 caracteres para que quepan en la mayoría de los nombres de los recursos de AWS). Esto garantiza que el nombre del inquilino no provoque una interrupción accidental de los recursos o las pilas de la infraestructura principal.

Pila de tecnología para inquilinos

La CloudFormation plantilla se almacena en el depósito de S3. La plantilla proporciona la clave de AWS KMS específica del inquilino, una CloudWatch alarma, un tema de SNS, una cola de SQS y una política de SQS.

Amazon SNS y Amazon SQS utilizan la clave de AWS KMS para el cifrado de datos de sus mensajes. Las prácticas de seguridad de AwsSolutions-SNS2 y AwsSolutions -SQS2 recomiendan configurar Amazon SNS y Amazon SQS con cifrado. Sin embargo, CloudWatch las alarmas no funcionan con Amazon SNS cuando se utiliza una clave gestionada por AWS, por lo que debe utilizar

una clave gestionada por el cliente en este caso. Para obtener más información, consulte el Centro de conocimientos de AWS.

La política de SQS se utiliza en la cola de Amazon SQS para permitir que el tema de SNS creado entregue el mensaje a la cola. Sin la política SQS, se denegará el acceso. Para obtener más información, consulte la documentación de Amazon SNS.

Descomponga monolitos en microservicios mediante CQRS y abastecimiento de eventos

Creado por Rodolfo Jr. Cerrada (AWS), Dmitry Gulin (AWS) y Tabby Ward (AWS)

Entorno: PoC o piloto	Origen: modelo CRUD monolítico	Destino: microservicios
Tipo R: renovar arquitectura	Carga de trabajo: código abierto	Tecnologías: modernización; mensajería y comunicaciones; sin servidor
Servicios de AWS: Amazon DynamoDB; AWS Lambda; Amazon EventBridge		

Resumen

Este patrón combina dos patrones y emplea tanto el patrón de división de responsabilidad por consultas de comandos (CQRS) como el patrón de abastecimiento de eventos. El patrón CQRS divide las responsabilidades de los modelos de comando y consulta. El patrón de abastecimiento de eventos aprovecha la comunicación asincrónica basada en eventos para mejorar la experiencia general del usuario.

Puede usar servicios de CQRS y Amazon Web Services (AWS) para mantener y escalar cada modelo de datos de forma independiente y, al mismo tiempo, refactorizar su aplicación monolítica en una arquitectura de microservicios. Después, puede usar el patrón de abastecimiento de eventos para sincronizar los datos de la base de datos de comandos con la base de datos de consultas.

Este patrón emplea un código de ejemplo que incluye un archivo de solución (*.sln) que puede abrir con la versión más reciente de Visual Studio. El ejemplo contiene el código de la API Reward para mostrar el funcionamiento de CQRS y el abastecimiento de eventos en aplicaciones de AWS sin servidor y aplicaciones tradicionales o en las instalaciones.

Para obtener más información sobre CQRS y el abastecimiento de eventos, consulte la sección de Información adicional.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Amazon CloudWatch
- Tablas de Amazon DynamoDB
- Amazon DynamoDB Streams
- Clave de acceso y clave secreta de AWS Identity and Access Management (IAM); para obtener más información, consulte el vídeo de la sección de Recursos relacionados
- AWS Lambda
- Familiaridad con Visual Studio
- Familiaridad con el kit de herramientas de AWS para Visual Studio; para obtener más información, consulte el vídeo de demostración del kit de herramientas de AWS para Visual Studio en la sección de Recursos relacionados

Versiones de producto

- Microsoft Visual Studio 2019 Community Edition.
- AWS Toolkit para Visual Studio 2019.
- .NET Core 3.1. Este componente es una opción de la instalación de Visual Studio. Para incluir .NET Core durante la instalación, seleccione desarrollo multiplataforma de NET Core.

Limitaciones

- El código de ejemplo de aplicación tradicional en las instalaciones (ASP.NET Core Web API y objetos de acceso a datos) no incluye base de datos. Sin embargo, incluye el objeto en memoria `CustomerData`, que actúa como base de datos simulada. El código proporcionado es suficiente para probar el patrón.

Arquitectura

Pila de tecnología de origen

- Proyecto ASP.NET Core Web API

- Servidor web IIS
- Objeto de acceso a datos
- Modelo CRUD

Arquitectura de origen

En la arquitectura de origen, el modelo CRUD contiene interfaces de comandos y consultas en una sola aplicación. Para ver un código de ejemplo, consulte `CustomerDAO.cs` (adjunto).

Pila de tecnología de destino

- Amazon DynamoDB
- Amazon DynamoDB Streams
- AWS Lambda
- (Opcional) Amazon API Gateway
- (Opcional) Amazon Simple Notification Service (Amazon SNS)

Arquitectura de destino

En la arquitectura de destino, las interfaces de comando y consulta están separadas. La arquitectura que se muestra en el siguiente diagrama se puede ampliar con puerta de enlace API y Amazon SNS. Para obtener más información, consulte la sección Información adicional.

1. Las funciones de comandos de Lambda realizan operaciones de escritura, como crear, actualizar o eliminar, en la base de datos.
2. Las funciones de consulta de Lambda realizan operaciones de lectura, como obtener o seleccionar, en la base de datos.
3. Esta función de Lambda procesa los flujos de DynamoDB de la base de datos de comandos y actualiza la base de datos de consultas con los cambios.

Herramientas

Herramientas

- Amazon DynamoDB: Amazon DynamoDB es un servicio de base de datos NoSQL totalmente administrado que ofrece un rendimiento rápido y predecible, así como una perfecta escalabilidad.
- Amazon DynamoDB Streams: DynamoDB Streams captura una secuencia en orden cronológico de las modificaciones de los elementos en una tabla de DynamoDB. Este servicio posteriormente almacena esta información en un registro durante un máximo de 24 horas. El cifrado en reposo cifra los datos en DynamoDB streams.
- AWS Lambda: AWS Lambda es un servicio informático que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo. Solo pagará por el tiempo de computación que consuma, no se aplican cargos cuando el código no se está ejecutando.
- La consola de administración de AWS: la consola de administración de AWS es una aplicación web que engloba y hace referencia a un amplio conjunto de consolas de servicios para la administración de recursos de AWS.
- Visual Studio 2019 Community Edition: Visual Studio 2019 es un entorno de desarrollo integrado (IDE). La Community Edition es gratuita para colaboradores de código abierto. En este patrón usará Visual Studio 2019 Community Edition para abrir, compilar y ejecutar código de ejemplo. Solo con fines de visualización, puede usar cualquier editor de texto o Visual Studio Code.
- AWS Toolkit para Visual Studio: el AWS Toolkit para Visual Studio es un complemento para el IDE de Visual Studio. El AWS Toolkit para Visual Studio facilita el desarrollo, la depuración y la implementación de aplicaciones .NET que utilizan servicios de AWS.

Código

Se adjunta el código de ejemplo. Para obtener más instrucciones sobre cómo implementar el código de ejemplo, consulta la sección Epics.

Epics

Abra y cree la solución

Tarea	Descripción	Habilidades requeridas
Abra la solución.	1. Descargue el código fuente de ejemplo (`CQRS-ES Code.zip`) de la sección	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	de Adjuntos y extraiga los archivos. 2. En el IDE de Visual Studio, seleccione Archivo, Abrir, Solución de proyecto, y navegue hasta la carpeta en la que extrajo el código fuente. 3. Seleccione AWS.APG.CQRSES.sln y seleccione Abrir. La solución completa se carga en Visual Studio.	
Cree la solución.	Abra el menú contextual (clic derecho) de la solución y elija Compilar solución. Esto generará y compilará todos los proyectos de la solución. La compilación debería realizarse correctamente. Visual Studio Solution Explorer mostrará la estructura de directorios. • `CQRS On-Premises Code Sample` contiene un ejemplo del uso de CQRS en las instalaciones. • `CQRS AWS Serverless` contiene todo el código de ejemplo de CQRS y de abastecimiento de eventos mediante servicios sin servidor de AWS.	Desarrollador de aplicaciones

Cree tablas de DynamoDB

Tarea	Descripción	Habilidades requeridas
Proporcionar credenciales.	Si aún no tiene una clave de acceso, consulte el vídeo de la sección de Recursos relacionados. 1. En Solution Explorer, expanda CQRS AWS Serverless y, a continuación, expanda la carpeta Compilar solución. 2. Expanda el proyecto AwS.APG.CQRSES.Build y visualice el archivo `Program.cs` . 3. Desplácese hasta la parte superior de `Program.cs` y busque `Program()` . 4. Sustituya `YOUR ACCESS KEY` por su clave de acceso a la cuenta y sustituya `YOUR SECRET KEY` por la clave secreta de la cuenta. Tenga en cuenta que, en un entorno de producción, no debería codificar sus claves de forma rígida. En su lugar, puede usar AWS Secrets Manager para almacenar y recuperar las credenciales.	Desarrollador de aplicaciones, ingeniero de datos, administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Compilar el proyecto.	Para compilar el proyecto, abra el menú contextual (clic derecho) del proyecto AwS.APG.CQRSES.Build y seleccione Compilar.	Desarrollador de aplicaciones, ingeniero de datos, administrador de base de datos
Cree y rellene las tablas.	Para compilar las tablas y rellenarlas con datos iniciales, abra el menú contextual (clic derecho) del proyecto AwS.APG.CQRSES.Build y seleccione Depurar, Iniciar nueva instancia.	Desarrollador de aplicaciones, ingeniero de datos, administrador de base de datos
Verifique la construcción de la tabla y los datos.	Para comprobarlo, acceda al Explorador de AWS y expanda Amazon DynamoDB. Se mostrarán las tablas. Abra cada tabla para mostrar los datos de ejemplo.	Desarrollador de aplicaciones, ingeniero de datos, administrador de base de datos

Ejecute pruebas locales

Tarea	Descripción	Habilidades requeridas
Crear el proyecto CQRS.	1. Abra la solución y acceda a la carpeta de soluciones CQRS AWS Services/CQRS/Tests. 2. En el proyecto AWS.apg.cqrses.cqrslambda.tests, abra .cs y sustituya y por las claves de IAM que haya	Desarrollador de aplicaciones, ingeniero de pruebas

Tarea	Descripción	Habilidades requeridas
	creado. BaseFunctionTest AccessKeySecretKey 3. Guarde los cambios. 4. Para compilar y crear el proyecto de prueba, abra el menú contextual (clic derecho) del proyecto y seleccione Crear.	
Cree el proyecto de abastecimiento de eventos.	1. Navegue hasta la carpeta de soluciones CQRS AWS Services/Event Source/Tests. 2. En el AWS.APG.CQRSES.EventSourceLambda.Tests del proyecto, abra BaseFunctionTest.cs y sustituya AccessKeyy SecretKeypor las claves de IAM que haya creado. 3. Guarde los cambios. 4. Para compilar y crear el proyecto de prueba, abra el menú contextual (clic derecho) del proyecto y seleccione Crear.	Desarrollador de aplicaciones, ingeniero de pruebas

Tarea	Descripción	Habilidades requeridas
Ejecutar las pruebas.	Para ejecutar todas las pruebas, seleccione Ver, Explorador de pruebas y, a continuación, seleccione Ejecutar todas las pruebas a la vista. Todas las pruebas resultarán correctas. El sistema lo indicará con un icono de marca de verificación verde.	Desarrollador de aplicaciones, ingeniero de pruebas

Publique las funciones de Lambda de CQRS en AWS

Tarea	Descripción	Habilidades requeridas
Publica la primera función de Lambda.	1. En el Explorador de soluciones, abra el menú contextual (haga clic con el botón derecho) del AWS.APG.CQRSES.CommandCreateLambda proyecto y, a continuación, elija Publicar en AWS Lambda. 2. Seleccione el perfil que desee usar, la región de AWS en la que desee implementar la función de Lambda y el nombre de la función. 3. Para los campos restantes, mantenga los valores predeterminados y seleccione Next (Siguiente).	Desarrollador de aplicaciones, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	4. En la lista desplegable del nombre del rol, seleccione. AWSLambdaFullAccess 5. Para proporcionar las claves de su cuenta, seleccione Agregar e introdúzca `AcessKey` como variable y su clave de acceso como valor. A continuación, vuelva a seleccionar Agregar, introduzca `SecretKey` como variable y su clave secreta como valor. 6. Para los campos restantes , mantenga los valores predeterminados y seleccione Upload (Cargar). Una vez cargada la función de prueba de Lambda, aparecerá automáticamente en Visual Studio. 7. Repita los pasos 1 a 6 para los siguientes proyectos: • AWS.APG.CARSES. CommandDeleteLambda • AWS.APG.CARSES. CommandUpdateLambda • AWS.APG.CARSES. CommandAddRewardLa mbda	

Tarea	Descripción	Habilidades requeridas
	• AWS.APG.CARSES.CommandRedeemRewardLambda • AWS.APG.CARSES.QueryCustomerListLambda • AWS.APG.CARSES.QueryRewqardLambda	
Verifique la carga de la función.	(Opcional) Para comprobar que la función se ha cargado correctamente, acceda al Explorador de AWS y expanda AWS Lambda. Para abrir la ventana de prueba, seleccione la función de Lambda (doble clic).	Desarrollador de aplicaciones, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Pruebe la función de Lambda.	1. Introduzca los datos de la solicitud o copie los datos de la solicitud de ejemplo Datos de prueba, en la sección Información adicional. Asegúrese de seleccionar los datos correctos para la función que está probando. 2. Para ejecutar la prueba, elija Invoke (Invocar). La respuesta y cualquier error se muestran en el cuadro de texto Respuesta, y los registros se muestran en el cuadro de texto Registros o en CloudWatch Registros. 3. Para verificar los datos, en el Explorador de AWS, seleccione la tabla de DynamoDB (doble clic). Todos los proyectos Lambda de CQRS se encuentran en las carpetas de soluciones `CQRS AWS Serverless\CQRS\Command Microservice` y `CQRS AWS Serverless\CQRS\Command Microservice`. Para ver el directorio de soluciones y los proyectos, consulte el Directorio de	Desarrollador de aplicaciones, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	códigos fuente en la sección de Información adicional.	
Publique las funciones restantes.	Repita los pasos previos para los siguientes proyectos: • AWS.APG.CARSES.CommandDeleteLambda • AWS.APG.CARSES.CommandUpdateLambda • AWS.APG.CARSES.CommandAddRewardLambda • AWS.APG.CARSES.CommandRedeemRewardLambda • AWS.APG.CARSES.QueryCustomerListLambda • AWS.APG.CARSES.QueryRewqardLambda	Desarrollador de aplicaciones, DevOps ingeniero

Configure la función de Lambda como oyente de eventos

Tarea	Descripción	Habilidades requeridas
Publique los controladores de eventos Customer y Reward Lambda.	Para publicar cada controlador de eventos, siga los pasos de la épica anterior. Los proyectos se encuentran en las carpetas de soluciones `CQRS AWS Serverless\Event Source\Customer Event` y `CQRS`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`AWS Serverless\Event Source\Reward Event` . Para obtener más información, consulte Directorio de código fuente en la sección Información adicional.	

Tarea	Descripción	Habilidades requeridas
Adjunte el oyente de Lambda detector de eventos.	1. Inicie sesión en la consola de administración de AWS con la misma cuenta que usó para publicar los proyectos de Lambda. 2. En Región, seleccione US East 1 o la región en la que implementó las funciones de Lambda en la épica anterior. 3. Navegue hasta el servicio Lambda. 4. Seleccione el `EventSourceCustomer` función de Lambda. 5. Elija Add trigger (Añadir disparador). 6. En la lista desplegable Configuración de desencadenante, seleccione DynamoDB. 7. En la lista desplegable de tablas de DynamoDB, seleccione. cqrses-customer-cmd 8. En la lista desplegable Posición inicial, seleccione Recortar horizonte desde. Recortar el horizonte significa que el desencadenante de DynamoDB empezará a leer en el último registro de transmisi	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	ón (sin recortar), que es el registro más antiguo del fragmento. 9. Seleccione la casilla Enable trigger (Habilitar disparador). 10. Deje los valores predeterminados en los demás campos y seleccione Add (Agregar). Una vez que el oyente se haya adjuntado correctamente a la tabla de DynamoDB, se mostrará en la página del diseñador de Lambda.	
Publique y adjunte la EventSourceReward función Lambda.	Para publicar y adjuntar la función `EventSourceReward` Lambda, repita los pasos de las dos historias anteriores y selecciónela en la lista desplegable cqrses-reward-cmdde tablas de DynamoDB.	Desarrollador de aplicaciones

Pruebe y valide los flujos de DynamoDB y el desencadenante de Lambda

Tarea	Descripción	Habilidades requeridas
Pruebe la transmisión y el desencadenante de Lambda.	1. En Visual Studio, acceda al Explorador de AWS. 2. Amplíe AWS Lambda y elija la CommandRedeemRewar	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	dfunción (haga doble clic). Se abrirá una ventana de funciones en la que podrá probar la función. 3. En el cuadro de texto de la solicitud, introduzca los datos de la solicitud en formato de notación de JavaScript objetos (JSON). Para ver un ejemplo de solicitud, consulte Datos de prueba en la sección Información adicional. 4. Elija Invocación de .	
Valide usando la tabla de consultas de recompensas de DynamodDB.	1. Abre la cqrses-reward-queryytabla. 2. Compruebe los puntos del cliente que canjeó la recompensa. Los puntos canjeados deben restarse del total de puntos agregados del cliente.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Valide mediante CloudWatch registros.	1. Navegue hasta los grupos de registros CloudWatch y selecciónelos. 2. El grupo de registros / aws/lambda/ contiene los EventSourceReward registros del desencadenador. `EventSourceReward` Se registrarán todas las llamadas de Lambda, incluidos los mensajes que ha incluido en `context.Logger.LogLine` y `Console.Writeline` dentro del código de Lambda.	Desarrollador de aplicaciones
Valide EventSourceCustomer el disparador.	Para validar el `EventSourceCustomer` disparador, repite los pasos de esta epopeya utilizando la tabla de clientes y los CloudWatch registros respectivos del `EventSourceCustomer` disparador.	Desarrollador de aplicaciones

Recursos relacionados

Referencias

- Descargas de Visual Studio 2019 Community Edition
- Descargar AWS Toolkit para Visual Studio
- Guía del usuario de AWS Toolkit para Visual Studio

- Sin servidor en AWS
- Casos de uso y patrones de diseño de DynamoDB
- CQRS Martin Fowler
- Aprovisionamiento de eventos Martin Fowler

Vídeos

- Demo de AWS Toolkit para Visual Studio
- ¿Cómo creo una ID de clave de acceso para un nuevo usuario de IAM?

Información adicional

CQRS y abastecimiento de eventos

CQRS

El patrón CQRS separa un único modelo de operaciones conceptual, como un modelo CRUD (creación, lectura, actualización, eliminación) único de objetos de acceso a datos, en modelos de operaciones de comando y consulta. El modelo de comandos hace referencia a cualquier operación, como crear, actualizar o eliminar, que cambia el estado. El modelo de consulta hace referencia a cualquier operación que devuelva un valor.

1. El modelo CRUD del cliente incluye las siguientes interfaces:
   - `Create Customer()`
   - `UpdateCustomer()`
   - `DeleteCustomer()`
   - `AddPoints()`
   - `RedeemPoints()`
   - `GetVIPCustomers()`
   - `GetCustomerList()`
   - `GetCustomerPoints()`

Cuando sus necesidades sean más complejas, podrá superar este enfoque de modelo único. El CQRS emplea un modelo de comandos y un modelo de consulta para separar las responsabilidades de escribir y leer los datos. De esta forma, los datos se pueden mantener y gestionar de forma independiente. Con una clara separación de responsabilidades, las mejoras de cada modelo no afectan al otro. Esta separación mejora el mantenimiento y el rendimiento, y reduce la complejidad de la aplicación a medida que crece.

1. Interfaces en el modelo de comandos del cliente:
   - `Create Customer()`
   - `UpdateCustomer()`
   - `DeleteCustomer()`
   - `AddPoints()`
   - `RedeemPoints()`
2. Interfaces en el modelo de consultas del cliente:
   - `GetVIPCustomers()`
   - `GetCustomerList()`
   - `GetCustomerPoints()`
   - `GetMonthlyStatement()`

Para ver código de ejemplo, consulte el Directorio de códigos fuente.

A continuación, el patrón CQRS desacopla la base de datos. Esta disociación posibilita la independencia total de cada servicio, que es el ingrediente principal de la arquitectura de microservicios.

Al usar CQRS en la nube de AWS, puede optimizar aún más cada servicio. Por ejemplo, puede establecer diferentes configuraciones informáticas, o elegir entre un microservicio sin servidor o uno basado en contenedores. Puedes sustituir el almacenamiento en caché local por Amazon. ElastiCache Si tiene mensajería de publicación y suscripción en las instalaciones, puede reemplazarla por Amazon Simple Notification Service (Amazon SNS). Además, puede aprovechar los pay-as-you-go precios y la amplia gama de servicios de AWS, que solo paga por lo que utiliza.

CQRS ofrece los siguientes beneficios:

- Escalado independiente: la estrategia de escalado de cada modelo se puede adaptar para satisfacer los requisitos y la demanda del servicio. Al igual que en las aplicaciones de alto rendimiento, separar la lectura y la escritura permite escalar el modelo de forma independiente para satisfacer cada demanda. También puede agregar o reducir recursos de cómputo para satisfacer la demanda de escalabilidad de un modelo sin afectar al otro.
- Mantenimiento independiente: la separación de los modelos de consulta y comando mejora la capacidad de mantenimiento de los modelos. Puede realizar cambios en el código y mejoras en un modelo sin que ello afecte al otro.
- Seguridad: es más fácil aplicar los permisos y las políticas a modelos separados para lectura y escritura.
- Lecturas optimizadas: puede definir un esquema optimizado para las consultas. Por ejemplo, puede definir un esquema para datos agregados y un esquema independiente para tablas de hechos.
- Integración: CQRS se adapta bien a los modelos de programación basados en eventos.
- Complejidad gestionada: la separación en modelos de consulta y comando es adecuada para dominios complejos.

Al utilizar CQRS, tenga en cuenta lo siguiente:

- El patrón de CQRS se aplica solo a una parte específica de una aplicación, y no a su conjunto. La implementación en un dominio inadecuado para el patrón puede reducir la productividad, aumentar el riesgo e introducir complejidad.
- El patrón funciona mejor en modelos de uso frecuente que presentan un desequilibrio en las operaciones de lectura y escritura.
- En el caso de aplicaciones de lectura intensiva, como informes de gran tamaño que tardan en procesarse, CQRS le ofrece la opción de seleccionar la base de datos adecuada y crear un esquema para almacenar los datos agregados. Esto mejora el tiempo de respuesta en la lectura y visualización del informe, ya que procesa los datos del informe solo una vez y los coloca en la tabla agregada.
- En el caso de las aplicaciones de escritura intensiva, puede configurar la base de datos para operaciones de escritura y permitir que el microservicio de comandos se escale de forma independiente cuando aumente la demanda de escritura. Para ver ejemplos, consulte los microservicios `AWS.APG.CQRSES.CommandRedeemRewardLambda` y `AWS.APG.CQRSES.CommandAddRewardLambda`.

Aprovisionamiento de eventos

El siguiente paso consiste en usar el abastecimiento de eventos para sincronizar la base de datos de consultas cuando se ejecuta un comando. Por ejemplo, considere los siguientes eventos:

- Al añadir un punto de recompensa, es necesario actualizar sus puntos de recompensa totales o agregados en la base de datos de consultas.
- El apellido del cliente se actualiza en la base de datos de comandos, y es necesario actualizar la información del cliente en la base de datos de consultas.

En un modelo CRUD tradicional, se garantiza la coherencia de los datos al bloquearlos hasta que finalice la transacción. En el abastecimiento de eventos, los datos se sincronizan publicando una serie de eventos que el suscriptor utilizará para actualizar sus datos respectivos.

El patrón de abastecimiento de eventos garantiza y registra una serie completa de acciones realizadas con los datos, y las publica a través de una secuencia de eventos. Estos eventos representan un conjunto de cambios en los datos que los suscriptores de ese evento deben procesar para mantener su registro actualizado. El suscriptor consume estos eventos y sincroniza los datos en la base de datos del suscriptor. En este caso, es la base de datos de consultas.

El siguiente diagrama muestra el abastecimiento de eventos con CQRS en AWS.

1. Las funciones de comandos de Lambda realizan operaciones de escritura, como crear, actualizar o eliminar, en la base de datos.
2. Las funciones de consulta de Lambda realizan operaciones de lectura, como obtener o seleccionar, en la base de datos.
3. Esta función de Lambda procesa los flujos de DynamoDB de la base de datos de comandos y actualiza la base de datos de consultas con los cambios. También puede usar esta función para publicar un mensaje en Amazon SNS y que los suscriptores puedan procesar los datos.
4. (Opcional) El suscriptor del evento de Lambda procesa el mensaje publicado por Amazon SNS y actualiza la base de datos de consultas.
5. (Opcional) Amazon SNS envía una notificación por correo electrónico de la operación de escritura.

En AWS, DynamoDB Streams puede sincronizar la base de datos de consultas. DynamoDB captura una secuencia en orden cronológico de las modificaciones de los elementos en la tabla de

DynamoDB en tiempo casi real y almacena la información de forma duradera en un plazo máximo de 24 horas.

La activación de DynamoDB Streams permite a la base de datos publicar una secuencia de eventos que posibilita el patrón de abastecimiento de eventos. El patrón de abastecimiento de eventos añade al suscriptor del evento. La aplicación del suscriptor del evento consume el evento y lo procesa en función de la responsabilidad del suscriptor. En el diagrama anterior, el suscriptor del evento envía los cambios a la base de datos de Query DynamoDB para mantener los datos sincronizados. El uso de Amazon SNS, el agente de mensajes y la aplicación de suscripción de eventos mantiene la arquitectura desacoplada.

El abastecimiento de eventos ofrece los siguientes beneficios:

- Coherencia de los datos transaccionales
- Un registro de auditoría fiable y un historial de las acciones que permite supervisar las medidas adoptadas en los datos
- Las aplicaciones distribuidas, como los microservicios, pueden sincronizar sus datos en todo el entorno
- Publicación fiable de los eventos siempre que cambie el estado
- Reconstrucción o reproducción de estados anteriores
- Entidades con acoplamiento flexible que intercambian eventos para migrar de una aplicación monolítica a microservicios
- Reducción de los conflictos causados por actualizaciones simultáneas; el abastecimiento de eventos evita la necesidad de actualizar los objetos directamente en el almacén de datos
- Flexibilidad y extensibilidad, ya que la tarea se desvincula del evento
- Actualizaciones externas del sistema
- Gestión de múltiples tareas en un solo evento

Cuando use abastecimiento de eventos, tenga en cuenta los siguientes puntos:

- Como existe cierto retardo en la actualización de los datos entre las bases de datos de suscriptor de origen, la única forma de deshacer un cambio es añadir un evento de compensación al almacén de eventos.
- La implementación del abastecimiento de eventos tiene cierta curva de aprendizaje, ya que su estilo de programación es diferente.

Datos de prueba

Use los siguientes datos de prueba para probar la función de Lambda tras una implementación correcta.

CommandCreate ¿Cliente

```
{  "Id":1501,  "Firstname":"John",  "Lastname":"Done",  "CompanyName":"AnyCompany",
 "Address": "USA",  "VIP":true }
```

CommandUpdate Cliente

```
{  "Id":1501,  "Firstname":"John",  "Lastname":"Doe",  "CompanyName":"Example Corp.",
 "Address": "Seattle, USA",  "VIP":true }
```

CommandDelete Cliente

Introduzca la ID del cliente como dato de solicitud. Por ejemplo, si la ID de cliente es 151, introduzca 151 como dato de solicitud.

```
151
```

QueryCustomerList

Está en blanco. Cuando se invoca, devuelve a todos los clientes.

CommandAddReward

Añade 40 puntos al cliente con la ID 1 (Richard).

```
{
  "Id":10101,
  "CustomerId":1,
  "Points":40
}
```

CommandRedeemReward

Esto reducirá 15 puntos al cliente con la ID 1 (Richard).

```
{
```

```
  "Id":10110,
  "CustomerId":1,
  "Points":15
}
```

QueryReward

Introduzca la ID del cliente. Por ejemplo, introduzca 1 para Richard, 2 para Arnav y 3 para Shirley.

```
2
```

Directorio de códigos fuente

Use la siguiente tabla como guía de estructura de directorios de la solución de Visual Studio.

Ejemplo de código de muestra de directorio CQRS en las instalaciones

Modelo CRUD de cliente

Proyecto CQRS On-Premises Code Sample\CRUD Model\AWS.APG.CQRSES.DAL

Versión CQRS del modelo CRUD del cliente

- Comando del cliente: proyecto `CQRS On-Premises Code Sample\CQRS Model\Command Microservice\AWS.APG.CQRSES.Command`
- Consulta del cliente: proyecto `CQRS On-Premises Code Sample\CQRS Model\Query Microservice\AWS.APG.CQRSES.Query`

Microservicios de comando y consulta

El microservicio de comandos se encuentra en la carpeta de soluciones `CQRS On-Premises Code Sample\CQRS Model\Command Microservice`:

- El proyecto de API ASP.NET Core `AWS.APG.CQRSES.CommandMicroservice` actúa como punto de entrada desde el que los consumidores interactúan con el servicio.
- El proyecto .NET Core `AWS.APG.CQRSES.Command` es un objeto que aloja objetos e interfaces relacionados con comandos.

El microservicio de consultas se encuentra en la carpeta de soluciones `CQRS On-Premises Code Sample\CQRS Model\Query Microservice`:

- El proyecto de API ASP.NET Core `AWS.APG.CQRSES.QueryMicroservice` actúa como punto de entrada desde el que los consumidores interactúan con el servicio.
- El proyecto .NET Core `AWS.APG.CQRSES.Query` es un objeto que aloja objetos e interfaces relacionados con consultas.

Directorio de soluciones de código CQRS AWS sin servidor

Este código es la versión de AWS del código en las instalaciones que emplea los servicios sin servidor de AWS.

En C# .NET Core, cada función de Lambda está representada por un proyecto .NET Core. En el código de ejemplo de este patrón, hay un proyecto independiente para cada interfaz en los modelos de comandos y consultas.

Uso de los servicios de AWS por CQRS

Puede encontrar el directorio raíz de soluciones para CQRS con servicios sin servidor de AWS en la carpeta `CQRS AWS Serverless\CQRS`. El ejemplo incluye dos modelos: Customer y Reward.

El comando de funciones de Lambda para Customer y Reward se encuentra en las carpetas `CQRS \Command Microservice\Customer` y `CQRS\Command Microservice\Reward`. Contienen los siguientes proyectos de Lambda:

- Comando Customer: `CommandCreateLambda`, `CommandDeleteLambda` y `CommandUpdateLambda`
- Comando Reward: `CommandAddRewardLambda` y `CommandRedeemRewardLambda`

Las funciones de Lambda de consulta para Customer y Reward se encuentra en las carpetas `CQRS \Query Microservice\Customer` y `CQRS\QueryMicroservice\Reward`. Contienen los proyectos de Lambda `QueryCustomerListLambda` and `QueryRewardLambda`.

Proyecto de prueba de CQRS

El proyecto de prueba se encuentra en la carpeta `CQRS\Tests`. Este proyecto contiene un script de prueba para automatizar las pruebas de las funciones de Lambda de CQRS.

Abastecimiento de eventos mediante servicios de AWS

Las transmisiones de DynamoDB Customer y Reward inician los siguientes controladores de eventos de Lambda para procesar y sincronizar los datos de las tablas de consultas.

- La función de Lambda `EventSourceCustomer` se asigna al flujo de DynamoDB de la tabla Customer (`cqrses-customer-cmd`).
- La función de Lambda `EventSourceReward` se asigna al flujo de DynamoDB de la tabla Customer (`cqrses-reward-cmd`).

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Más patrones

- ???
- Automatice la adición o actualización de entradas de registro de Windows con AWS Systems Manager
- Automatice la conmutación por error y la conmutación por recuperación entre regiones mediante DR Orchestrator Framework
- Automatice la identificación y planificación de la estrategia de migración mediante AppScore
- Crear e implementar de forma automática una aplicación Java en Amazon EKS mediante una canalización de CI/CD
- Crear automáticamente canalizaciones de CI/CD y clústeres de Amazon ECS para microservicios mediante AWS CDK
- Realice copias de seguridad y archive los datos del mainframe en Amazon S3 mediante AMI Cloud Data de BMC
- Encadene los servicios de AWS mediante un enfoque sin servidor
- Almacenamiento en contenedores de las cargas de trabajo de mainframe que Blu Age ha modernizado
- Implemente de forma continua una aplicación web AWS Amplify moderna desde un repositorio de AWS CodeCommit
- Convierta y desempaquete datos EBCDIC a ASCII en AWS mediante Python
- Convertir archivos de datos de mainframe con diseños de registros complejos mediante Micro Focus
- ???
- Cree una canalización e implemente actualizaciones de artefactos en instancias EC2 locales mediante CodePipeline
- Implementar y depurar clústeres de Amazon EKS
- Implementar contenedores mediante Elastic Beanstalk
- Emule Oracle DR mediante una base de datos global de Aurora compatible con PostgreSQL
- Genere información de datos mediante AWS Mainframe Modernization y Amazon Q en QuickSight
- Migre gradualmente de Amazon RDS para Oracle a Amazon RDS para PostgreSQL con Oracle SQL Developer y AWS SCT
- Integrar el controlador universal Stonebranch con AWS Mainframe Modernization

- Administre los productos de AWS Service Catalog en varias cuentas y regiones de AWS
- Migración de una cuenta de miembro de AWS de AWS Organizations a AWS Control Tower
- Migre y replique archivos VSAM a Amazon RDS o Amazon MSK mediante Connect de Precisely
- Migración de SAP ASE a Amazon RDS para SQL Server utilizando AWS DMS
- Migre tablas externas de Oracle a Amazon Aurora compatible con PostgreSQL
- Modernice las cargas de trabajo de impresión por lotes de mainframe en AWS mediante Micro Focus Enterprise Server y LRS VPSX/MFI
- ???
- Modernice la administración de la producción de mainframe en AWS mediante OpenText Micro Focus Enterprise Server y LRS X PageCenter
- ???
- Optimizar imágenes de Docker generadas por AWS App2Container
- Replicar bases de datos de unidades centrales en AWS mediante Precisely Connect
- Ejecute tareas de Amazon ECS en Amazon WorkSpaces con Amazon ECS Anywhere
- Configure un repositorio de gráficos de Helm v3 en Amazon S3
- Configure la detección de CloudFormation desviaciones de AWS en una organización multirregional y multicuenta
- Estructure un proyecto de Python en una arquitectura hexagonal con AWS Lambda
- Actualizar los clústeres de SAP Pacemaker de ENSA1 a ENSA2
- Uso CloudEndure para la recuperación ante desastres de una base de datos local
- Validar Account Factory para el código Terraform (AFT) localmente

Red

Temas

Automatice la configuración del emparejamiento entre regiones con AWS Transit Gateway

Creado por Ram Kandaswamy (AWS)

Entorno: producción	Tecnologías: redes; nube híbrida	Servicios de AWS: AWS Transit Gateway; AWS Step Functions; AWS Lambda

Resumen

AWS Transit Gateway conecta las nubes privadas virtuales (VPC) y redes en las instalaciones mediante un núcleo central. El tráfico de Transit Gateway siempre permanece en la red troncal global de Amazon Web Services (AWS) y no atraviesa la Internet pública, lo que reduce los vectores de amenazas, como las vulnerabilidades más comunes y los ataques de denegación de servicio distribuido (DDoS).

Si usted necesita comunicarse entre dos o más regiones de AWS, puede utilizar el emparejamiento entre regiones de Transit Gateway para establecer conexiones de interconexión entre las puertas de enlace de tránsito de distintas regiones. Sin embargo, configurar manualmente el emparejamiento entre regiones con Transit Gateway puede ser un proceso lento que consta de varios pasos. Este patrón proporciona un proceso automatizado para eliminar estos pasos manuales mediante el uso de código para realizar el emparejamiento. Usted puede utilizar este enfoque si tiene que configurar varias regiones y cuentas de AWS de forma repetida durante la configuración de una organización multirregional.

Este patrón utiliza una CloudFormation pila de AWS que incluye el flujo de trabajo de AWS Step Functions, las funciones de AWS Lambda, las funciones de AWS Identity and Access Management (IAM) y los grupos de registros en Amazon Logs. CloudWatch A continuación, puede iniciar una ejecución de Step Functions y crear el emparejamiento entre regiones para sus puertas de enlace de tránsito.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.

- Un bucket existente de Amazon Simple Storage Service (Amazon S3)
- Puertas de enlace de tránsito, creadas y configuradas en la región solicitante y en las regiones receptoras. La región solicitante es el lugar donde se origina una solicitud de emparejamiento y las regiones receptoras aceptan la solicitud de interconexión. Para obtener más información al respecto, consulte Creación y aceptación de conexiones de emparejamiento de VPC en la documentación de Amazon VPC.
- VPC, instaladas y configuradas en las regiones receptora y solicitante. Para ver los pasos para crear una VPC, consulte Creación de VPC desde Introducción a Amazon VPC en la documentación de Amazon VPC.
- Las VPC deben usar la etiqueta `addToTransitGateway` y el valor `true`.
- Grupos de seguridad y listas de control de acceso (ACL) de red para sus VPC, configurados de acuerdo con sus requisitos. Para obtener más información al respecto, consulte Grupos de seguridad de su VPC y las ACL de red en la documentación de Amazon VPC.

Regiones y limitaciones de AWS

- Solo algunas regiones de AWS son compatibles con el emparejamiento entre regiones. Para obtener una lista completa de las regiones que admiten el emparejamiento entre regiones, consulte las preguntas frecuentes sobre AWS Transit Gateway.
- En el código de ejemplo adjunto, se supone que la región solicitante es `us-east-2` y que la región receptora `us-west-2`. Si desea configurar diferentes regiones, debe editar estos valores en todos los archivos de Python. Para implementar una configuración más compleja que incluya más de dos regiones, puede cambiar la función Step para pasar las regiones como parámetro a la función de Lambda y ejecutar la función para cada combinación.

Arquitectura

El diagrama muestra un flujo de trabajo con los siguientes pasos:

1. El usuario crea una CloudFormation pila de AWS.
2. AWS CloudFormation crea una máquina de estados Step Functions que utiliza una función Lambda. Para obtener más información al respecto, consulte Creación de una máquina de estados de Step Functions que utilice Lambda en la documentación de AWS Step Functions.

3. Step Functions llama a una función de Lambda para el emparejamiento.
4. La función de Lambda crea una conexión de emparejamiento entre puertas de enlace de tránsito.
5. Step Functions llama a una función de Lambda para modificar la tabla de enrutamiento.
6. La función de Lambda modifica las tablas de enrutamiento al agregar el bloque de enrutamiento entre dominios sin clases (CIDR) de las VPC.

Flujo de trabajo de Step Functions

El diagrama muestra el siguiente flujo de trabajo de Step Functions:

1. El flujo de trabajo de Step Functions llama a la función de Lambda para el emparejamiento de la puerta de enlace de tránsito.
2. Hay una llamada en el temporizador para esperar un minuto.
3. El estado de emparejamiento se recupera y se envía al bloque de condiciones. El bloque es responsable del bucle.
4. Si no se cumple la condición de éxito, el flujo de trabajo se codifica para entrar en la fase de temporización.
5. Si se cumple la condición de éxito, se llama a una función de Lambda para modificar las tablas de enrutamiento. Tras esta llamada, finaliza el flujo de trabajo de Step Functions.

Herramientas

- AWS CloudFormation: AWS CloudFormation es un servicio que le ayuda a modelar y configurar sus recursos de AWS.
- Amazon CloudWatch Logs: CloudWatch Logs le ayuda a centralizar los registros de todos los sistemas, aplicaciones y servicios de AWS que utilice.
- AWS Identity and Access Management (IAM): es un servicio web que lo ayuda a controlar el acceso seguro a los servicios de AWS.
- AWS Lambda: Lambda ejecuta el código en una infraestructura informática de alta disponibilidad y realiza todas las tareas de administración de los recursos informáticos.
- AWS Step Functions: Step Functions facilita la organización de los componentes de sus aplicaciones distribuidas en una serie de pasos en un flujo de trabajo visual.

Epics

Automatización del emparejamiento

Tarea	Descripción	Habilidades requeridas
Cargue los archivos adjuntos en el bucket de S3.	Inicie sesión en la consola de administración de AWS, abra la consola de Amazon S3 y, a continuación cargue los archivos `modify-transit-gateway-routes.zip` , `peer-transit-gateway.zip` , y `get-transit-gateway-peering-status.zip` (adjuntos) a el bucket de S3.	AWS general
Cree la CloudFormation pila de AWS.	Ejecute el siguiente comando para crear una CloudFormation pila de AWS mediante el `transit-gateway-peering.json` archivo (adjunto): `aws cloudformation create-stack --stack-name myteststack --template-body file://sampletemplate.json` La CloudFormation pila de AWS crea el flujo de trabajo de Step Functions, las funciones de Lambda, las funciones de IAM y CloudWatch los grupos de registros.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	Asegúrese de que la CloudFormation plantilla de AWS haga referencia al depósito de S3 que contiene los archivos que cargó anteriormente. Nota: También puede crear una pila mediante la CloudFormation consola de AWS. Para obtener más información al respecto, consulte Crear una pila en la CloudFormation consola de AWS en la CloudFormation documentación de AWS.	

Tarea	Descripción	Habilidades requeridas
Inicie una nueva ejecución en Step Functions.	Abra la consola Step Functions e inicie una nueva ejecución. Step Functions llama a la función de Lambda y crea la conexión de emparejamiento para las puertas de enlace de tránsito. No es necesario introducir un archivo JSON. Compruebe que haya un archivo adjunto disponible y que el tipo de conexión sea Peering (Emparejamiento). Para obtener más informaci ón al respecto, consulte Iniciar una nueva ejecución desde Cómo empezar con AWS Step Functions en la documenta ción de AWS Steps Functions.	DevOps ingeniero, AWS general

Tarea	Descripción	Habilidades requeridas
Verifique las rutas en las tablas de enrutamiento.	El emparejamiento entre regiones se establece entre las puertas de enlace de tránsito. Las tablas de enrutamiento se actualizan con el rango de bloques CIDR de IPv4 de la VPC de la región homóloga. Abra la consola de Amazon VPC y elija la pestaña Associations (Asociaciones) en la tabla de enrutamie nto que corresponde a la conexión de puerta de enlace de tránsito. Verifique el rango de bloques CIDR de VPC de las regiones emparejadas. Para obtener instrucciones y pasos detallados, consulte la tabla de enrutamiento Asociar una puerta de enlace de tránsito en la documentación de Amazon VPC.	Administrador de red

Recursos relacionados

- Ejecuciones en Step Functions
- Vinculaciones del emparejamiento de puerta de enlace de tránsito
- Interconexión de VPC entre regiones de AWS mediante AWS Transit Gateway: demostración (vídeo)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Centralice la conectividad de red con AWS Transit Gateway

Creado por Mydhili Palagummi (AWS) y Nikhil Marrapu (AWS)

Entorno: producción	Tecnologías: redes	Servicios de AWS: AWS Transit Gateway; Amazon VPC

Resumen

Este patrón describe la configuración más sencilla en la que se puede usar AWS Transit Gateway para conectar una red en las instalaciones a nubes privadas virtuales (VPC) en varias cuentas de AWS dentro de una región de AWS. Con esta configuración, puede establecer una red híbrida que conecte varias redes de VPC en una región y una red en las instalaciones. Esto se logra mediante el uso de una puerta de enlace de tránsito y una conexión de red privada virtual (VPN) a la red en las instalaciones.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta para alojar servicios de red, administrada como una cuenta de miembro de una organización en AWS Organizations
- VPC en varias cuentas de AWS, sin superponer bloques de enrutamiento entre dominios sin clases (CIDR)

Limitaciones

Este patrón no admite el aislamiento del tráfico entre determinadas VPC o la red en las instalaciones. Todas las redes conectadas a la puerta de enlace de tránsito podrán comunicarse entre sí. Para aislar el tráfico, debe usar tablas de enrutamiento personalizadas en la puerta de enlace de tránsito. Este patrón solo conecta las VPC y la red en las instalaciones mediante una única tabla de enrutamiento de la puerta de enlace de tránsito predeterminada, que es la configuración más sencilla.

Arquitectura

Pila de tecnología de destino

- AWS Transit Gateway
- AWS Site-to-Site VPN
- VPC
- AWS Resource Access Manager (AWS RAM)

Arquitectura de destino

Herramientas

Servicios de AWS

- AWS Resource Access Manager (AWS RAM) lo ayuda a compartir sus recursos de forma segura entre las cuentas de AWS y dentro de su organización o unidades organizativas en AWS Organizations.
- AWS Transit Gateway es un hub central que conecta las nubes privadas virtuales (VPC) y las redes en las instalaciones.

Epics

Crear una puerta de enlace de tránsito en la cuenta de servicios de red

Tarea	Descripción	Habilidades requeridas
Crear una puerta de enlace de tránsito	En la cuenta de AWS en la que desee alojar los servicios de red, cree una puerta de enlace de tránsito en la región de AWS de destino. Para obtener instrucciones, consulte Creación de una	Administrador de red

Tarea	Descripción	Habilidades requeridas
	puerta de enlace de tránsito. Tenga en cuenta lo siguiente: • Seleccione Default route table association (Asociación de tablas de enrutamiento predeterminada). • Seleccione Default route table propagation (Propagación de tablas de enrutamiento predeterminada).	

Conecte la puerta de enlace de tránsito a tu red en las instalaciones

Tarea	Descripción	Habilidades requeridas
Cambio de la puerta de enlace de cliente para una conexión de VPN.	El dispositivo de la puerta de enlace de cliente se conecta en el lado en las instalaciones de la conexión VPN de sitio a sitio entre la puerta de enlace de tránsito y su red en las instalaciones. Para obtener más información, consulte El dispositivo de la puerta de enlace de cliente en la documentación de AWS Site-to-Site VPN. Identifique o inicie un dispositivo de cliente en las instalaciones compatible y anote su dirección IP pública. La configuración de la VPN se completará más adelante en esta epopeya.	Administrador de red

Tarea	Descripción	Habilidades requeridas
En la cuenta de servicios de red, cree una conexión VPC a la puerta de enlace de tránsito.	Para configurar una conexión, cree una conexión VPN para la puerta de enlace de tránsito. Para obtener instrucciones, consulte las conexiones VPN de puerta de enlace de tránsito.	Administrador de red
Configure la VPN en el dispositivo de la puerta de enlace de cliente en las instalaciones.	Descargue el archivo de configuración de la conexión de Site-to-Site VPN asociada a la puerta de enlace de tránsito y configure los ajustes de VPN en el dispositivo de puerta de enlace de cliente. Para obtener las instrucciones, consulte Descargar el archivo de configuración.	Administrador de red

Comparta la puerta de enlace de tránsito de la cuenta de servicios de red con otras cuentas de AWS o con su organización

Tarea	Descripción	Habilidades requeridas
En la cuenta de administración de AWS Organizations, active el uso compartido.	Para compartir la puerta de enlace de tránsito con su organización o con determinadas unidades organizativas, active el uso compartido en AWS Organizations. De lo contrario, tendrá que compartir la puerta de enlace de tránsito de cada cuenta de forma individual. Para obtener	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	instrucciones, consulte Habilitar el uso compartido de recursos en AWS Organizations.	
Cree el recurso compartido de la puerta de enlace de tránsito en la cuenta de servicios de red.	Para permitir que las VPC de otras cuentas de AWS de su organización se conecten a la puerta de enlace de tránsito, en la cuenta de servicios de red, utilice la consola RAM de AWS para compartir el recurso de la puerta de enlace de tránsito. Para obtener instrucciones, consulte Crear un recurso compartido.	Administrador de sistemas de AWS

Conecte las VPC a una puerta de enlace de tránsito.

Tarea	Descripción	Habilidades requeridas
Cree adjuntos de VPC en cuentas individuales.	En las cuentas con las que se ha compartido la puerta de enlace de tránsito, cree adjuntos de VPC de la puerta de enlace de tránsito. Para obtener instrucciones, consulte Creación de una conexión de puerta de enlace de tránsito a una VPC.	Administrador de red
Acepte las solicitudes de adjuntos de la VPC.	En la cuenta de servicios de red, acepte las solicitudes de adjuntos de VPC de la puerta de enlace de tránsito.	Administrador de red

Tarea	Descripción	Habilidades requeridas
	Para obtener instrucciones, consulte Aceptar un archivo adjunto compartido.	

Configuración del enrutamiento

Tarea	Descripción	Habilidades requeridas
Configure las rutas en las VPC de cuentas individuales.	En cada VPC de cuenta individual, agregue rutas a la red en las instalaciones y a otras redes de VPC, utilizando la puerta de enlace de tránsito como destino. Para obtener instrucciones, consulte Agregar y eliminar rutas de una tabla de enrutamiento.	Administrador de red
Configure la ruta a la tabla de enrutamiento de la puerta de enlace de tránsito.	Las rutas de las VPC y de la conexión VPN deben propagarse y aparecer en la tabla de enrutamiento predeterminada de la puerta de enlace de tránsito. Si es necesario, cree cualquier ruta estática (un ejemplo son las rutas estáticas para la conexión VPN estática) en la tabla de enrutamie nto predeterminada de la puerta de enlace de tránsito. Para obtener instrucciones, consulte Crear una ruta estática.	Administrador de red

Tarea	Descripción	Habilidades requeridas
Agregar reglas de grupos de seguridad y listas de control de acceso a la red (ACL).	Para las instancias EC2 y otros recursos de la VPC, asegúrese de que las reglas del grupo de seguridad y las reglas de ACL de la red permitan el tráfico entre las VPC y la red en las instalaciones. Para obtener instrucciones, consulte Controlar el tráfico hacia los recursos mediante grupos de seguridad y Agregar y eliminar reglas de una ACL.	Administrador de red

Prueba de conectividad

Tarea	Descripción	Habilidades requeridas
Pruebe la conectividad entre las VPC.	Asegúrese de que la ACL de la red y los grupos de seguridad permitan el tráfico del Protocolo de mensajes de control de Internet (ICMP) y, a continuación, haga ping desde las instancias de una VPC a otra VPC que también esté conectada a la puerta de enlace de tránsito.	Administrador de red
Pruebe la conectividad entre las VPC y la red en las instalaciones.	Asegúrese de que las reglas ACL de la red, las reglas del grupo de seguridad y cualquier firewall permiten el tráfico ICMP y, a continuación,	Administrador de red

Tarea	Descripción	Habilidades requeridas
	haga ping entre la red local y las instancias EC2 en las VPC. La comunicación de red debe iniciarse primero desde la red en las instalaciones para que la conexión VPN recupere el estado UP.	

Recursos relacionados

- Creación de una infraestructura de red de AWS multiVPC escalable y segura (documento técnico de AWS)
- Trabajar con recursos compartidos (documentación de RAM de AWS)
- Trabajar con puertas de enlace de tránsito (documentación de AWS Transit Gateway)

Configure el cifrado HTTPS para Oracle JD Edwards EnterpriseOne en Oracle WebLogic mediante un Application Load Balancer

Entorno: producción	Tecnologías: redes, seguridad , identidad, conformidad	Carga de trabajo: Oracle
Servicios de AWS: Elastic Load Balancing (ELB); AWS Certificate Manager (ACM); Amazon Route 53		

Resumen

Este patrón explica cómo configurar el cifrado HTTPS para la descarga de SSL en las cargas de trabajo de Oracle JD Edwards EnterpriseOne en Oracle. WebLogic Este enfoque cifra el tráfico entre el navegador del usuario y un equilibrador de carga para eliminar la carga de cifrado de los servidores. EnterpriseOne

Muchos usuarios escalan el nivel de la máquina virtual EnterpriseOne JAVA (JVM) horizontalmente mediante un AWS Application Load Balancer.El equilibrador de carga sirve como un único punto de contacto para los clientes y distribuye el tráfico entrante entre múltiples JVM. Opcionalmente, el balanceador de cargas puede distribuir el tráfico entre varias zonas de disponibilidad y aumentar la disponibilidad de. EnterpriseOne

El proceso descrito en este patrón configura el cifrado entre el navegador y el equilibrador de carga en lugar de cifrar el tráfico entre el equilibrador de carga y las máquinas virtuales virtuales. EnterpriseOne Este enfoque se denomina descarga de SSL. Al transferir el proceso de descifrado SSL del servidor EnterpriseOne web o de aplicaciones al Application Load Balancer, se reduce la carga para la aplicación. Tras la finalización del SSL en el equilibrador de cargas, el tráfico no cifrado se enruta a la aplicación en AWS.

Oracle JD Edwards EnterpriseOne es una solución de planificación de recursos empresariales (ERP) para organizaciones que fabrican, construyen, distribuyen, dan servicio o gestionan productos o

activos físicos. JD Edwards EnterpriseOne es compatible con varios hardware, sistemas operativos y plataformas de bases de datos.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un rol de AWS Identity and Access Management (IAM) con permisos para realizar llamadas de servicio de AWS y administrar los recursos de AWS
- Un certificado SSL

Versiones de producto

- Este patrón se probó con Oracle WebLogic 12c, pero también puede utilizar otras versiones.

Arquitectura

Existen varios enfoques para realizar la descarga de SSL. Este patrón utiliza un equilibrador de carga de aplicación y un Oracle HTTP Server (OHS), como se ilustra en el siguiente diagrama.

El siguiente diagrama muestra el diseño de la JVM de JD Edwards EnterpriseOne, Application Load Balancer y Java Application Server (JAS).

Herramientas

Servicios de AWS

- El equilibrador de carga de aplicación distribuye el tráfico entrante de aplicaciones entre varios destinos, tales como instancias de Amazon Elastic Compute Cloud (Amazon EC2, en varias zonas de disponibilidad.
- AWS Certificate Manager (ACM) le ayuda a crear, almacenar y renovar certificados y claves SSL/TLS X.509 públicos y privados que protegen sus sitios web y aplicaciones de AWS.

- Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad.

Prácticas recomendadas

- Para conocer las prácticas recomendadas de ACM, consulte la documentación de ACM.

Epics

Configuración y OHS WebLogic

Tarea	Descripción	Habilidades requeridas
Instale y configure los componentes de Oracle.	1. Instale Fusion Middlewar e Infrastructure siguiendo el proceso de instalación estándar. Este programa le ayuda a instalar y configura r un WebLogic dominio. Para obtener instrucciones, consulte la documentación de Oracle. 2. Instale OHS siguiendo el proceso de instalación estándar. Para obtener instrucciones, consulte la documentación de Oracle. 3. Cuando se complete la instalación, inicie el asistente de configuración (archivo `config.sh`) para configurar el OHS. • Puede actualizar un dominio existente o crear uno nuevo. Este	JDE CNC, administrador WebLogic

Tarea	Descripción	Habilidades requeridas
	patrón supone que está actualizando un dominio existente. • Para ver las Plantillas disponibles, elija Oracle Enterprise Manager-R estricted JRF y Oracle HTTP Server (Restrict ed JRF). Al seleccion ar estas opciones de archivos necesarios de Java (JRF), se elimina la conexión a una base de datos externa. • En el caso de los Servidores gestionados, los clústeres, las Plantilla s de servidores, los Clústeres de coherencia, los Equipos, la Asignació n de servidores a equipos, los Destinos virtuales y las Particion es, acepte los valores de configuración predeterm inados y seleccione Siguiente para pasar a la siguiente categoría. • Complete los detalles de configuración (por ejemplo, el host y el puerto del administrador, la dirección y el puerto de escucha y el nombre del	

Tarea	Descripción	Habilidades requeridas
	servidor) de la instancia de OHS (por ejemplo, `ohs1`).	
Habilite el WebLogic complemento a nivel de dominio.	El WebLogic complemento es necesario para equilibrar la carga. Para habilitar el complemento: 1. Inicie sesión en la consola de WebLogic administración mediante el enlace: `http://<WeblogicServer>:<Adminport>/console` 2. Seleccione Bloquear y editar y, a continuación, seleccione Configuración, Aplicaciones web. 3. Seleccione el WebLogic complemento activado (casilla de verificación o opción desplegable). 4. Seleccione Guardar y activar los cambios.	JDE CNC, administrador WebLogic

Tarea	Descripción	Habilidades requeridas
Edite el archivo de configuración.	El `mod_wl_ohs.conf` archivo configura las solicitudes de proxy de OHS a. WebLogic 1. Edite este archivo. Está ubicado en: `$ORACLE_HOME/user_projects/domains/` Por ejemplo: `/home/oracle/Oracle/Middleware/Oracle_Home/user_projects/domains/base_domain/config/fmwconfig/components/OHS/instances/ohs1` 2. Agregue los valores de WebLogic host (`WebLogicHost`) y port (`WebLogicPort`) (este patrón asume localhost y el puerto 8000). 3. Agregue los valores `WLProxySSL` y `WLProxySSLPassThrough` de la siguiente manera: `<VirtualHost *:8000>` `<Location /jde>` `WLSRequest On`	JDE CNC, administrador WebLogic

Tarea	Descripción	Habilidades requeridas
	`SetHandler weblogic-handler` `WebLogicHost localhost` `WebLogicPort 8000` `WLProxySSL On` `WLProxySSLPassThrough On` `</Location>` `</VirtualHost>`	

Tarea	Descripción	Habilidades requeridas
Inicie la OHS mediante Enterprise Manager.	1. Inicie sesión en Enterprise Manager Fusion Middlewar e mediante el enlace: `http://<WeblogicSe rver>:<Adminport>/ em/` 2. En Navegación de destino, en Servidor HTTP, seleccione la instancia de OHS (por ejemplo, `ohs1`). 3. Seleccione Apagar and Arrancar para reiniciar la instancia de OHS. 4. Cuando se complete la configuración de OHS, puede conectarse al cliente EnterpriseOne HTML utilizando el nombre de host del servidor HTTP con el puerto 8000 en lugar del nombre de host del EnterpriseOne servidor. • Enlace anterior: `http:// <Webserver>:80/ jde/owhtml` • Nuevo enlace: `http:// <HTTP server or web server>:8000/jde/o whtml` Si utiliza un puerto que no sea el puerto HTTP predeterminado de Oracle,	JDE CNC, administrador WebLogic

Tarea	Descripción	Habilidades requeridas
	edite el archivo `httpd.conf` para añadir un oyente para ese puerto en dos lugares: `#[Listen] OHS_LISTEN_PORT` `Listen 8000` y: `#` `ServerName <Weblogic Server1>:8000`	

Configure el Equilibrador de carga de aplicación

Tarea	Descripción	Habilidades requeridas
Establezca un grupo de destino.	1. Cree un grupo de destino para el puerto 8000 del servidor HTTP. 2. Registre los destinos en el grupo de objetivos con el mismo puerto. 3. Compruebe el estado de los objetivos para confirmar que están en buen estado. 4. Configure los ajustes de comprobación de estado según sea necesario. Para obtener más instrucciones, consulte la documenta	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	ción de Elastic Load Balancing .	
Configure el equilibrador de carga.	1. Cree un equilibrador de carga de aplicación con los atributos predeterminados y la nube privada virtual (VPC), los grupos de seguridad y las subredes necesarios. Para obtener más instrucciones, consulte la documentación de Elastic Load Balancing. 2. Añada una entrada de oyente para HTTPS 443 y reenvíela al grupo de destino que creó en el paso anterior. (Para obtener más instrucciones, consulte la documentación de Elastic Load Balancing). Un oyente HTTPS requiere un certificado SSL. Puede elegir un certificado de ACM o cargar uno. 3. Para ambos oyentes, habilite la adherencia siguiendo las instrucciones de la documentación de equilibrador de carga elástico.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Adición un registro de DNS de Route 53	(Opcional) Puede añadir un registro DNS de Amazon Route 53 para el subdominio. Este registro apuntaría a su equilibrador de carga de aplicación. Para obtener instrucciones, consulte la documentación de Route 53.	Administrador de AWS

Resolución de problemas

Problema	Solución
El servidor HTTP no aparece.	Si el servidor HTTP no aparece en la lista de Navegación de destino de la consola de Enterprise Manager, siga estos pasos: 1. En WebLogic Dominio, Administración, elija OHS Instances. 2. Elija Crear para crear una nueva instancia de OHS. 3. Proporcione un nombre de instancia y, a continuación, elija Aceptar para crear la instancia. Cuando se haya creado la instancia y se hayan activado los cambios, podrá ver el servidor HTTP en el panel de Navegación de destino.

Recursos relacionados

Documentación de AWS

- Equilibrador de carga de aplicación
- Trabajar con zonas públicas alojadas
- Uso de zonas alojadas privadas

Documentación de Oracle:

- Descripción general del complemento Oracle WebLogic Server Proxy
- Instalación WebLogic del servidor mediante el instalador de infraestructuras
- Instalación y configuración del servidor HTTP de Oracle

Conéctese a los planos de datos y control del Servicio de Migración de Aplicaciones a través de una red privada

Creado por Dipin Jain (AWS) y Mike Kuznetsov (AWS)

Entorno: PoC o piloto	Tecnologías: redes; migración	Servicios de AWS: Servicio de migración de aplicaciones de AWS; Amazon EC2; Amazon VPC; Amazon S3

Resumen

Este patrón explica cómo puede conectarse a un plano de datos y un plano de control del AWS Servicio de migración de aplicaciones (AWS MGN) en una red privada y segura mediante puntos de conexión de VPC de interfaz.

El servicio de migración de aplicaciones es una solución altamente automatizada lift-and-shift (rehospedaje) que simplifica, agiliza y reduce el costo de la migración de aplicaciones a AWS. Permite a las empresas volver a alojar una gran cantidad de servidores físicos, virtuales o en la nube sin problemas de compatibilidad, interrupciones en el rendimiento ni periodos de transición prolongados. Servicio de migración de aplicaciones está disponible en la Consola de administración de AWS. Esto permite una integración perfecta con otros servicios de AWS, como AWS CloudTrail CloudWatch, Amazon y AWS Identity and Access Management (IAM).

Puede conectarse desde un centro de datos de origen a un plano de datos (es decir, a una subred que sirva como área de almacenamiento para la replicación de datos en la VPC de destino) a través de una conexión privada mediante los servicios de VPN de AWS, AWS Direct Connect o el emparejamiento de VPC en Servicio de migración de aplicaciones. También puede usar puntos de enlace de VPC de interfaz con tecnología de AWS PrivateLink para conectarse a un plano de control del Servicio de migración de aplicaciones a través de una red privada.

Requisitos previos y limitaciones

Requisitos previos

- Subred de área de ensayo: antes de configurar el Servicio de migración de aplicaciones, cree una subred para utilizarla como área de almacenamiento provisional para los datos replicados desde

sus servidores de origen a AWS (es decir, un plano de datos). Debe especificar esta subred en la Plantilla de configuración de replicación cuando acceda por primera vez a la consola del Servicio de migración de aplicaciones. Puede anular esta subred para servidores de origen específicos en la plantilla de configuración de replicación. Aunque puede utilizar una subred existente en su cuenta de AWS, le recomendamos que cree una nueva subred dedicada para este fin.

- Requisitos de red: Los servidores de replicación que lanza Application Migration Service en la subred del área de ensayo deben poder enviar datos al punto de conexión de la API de Application Migration Service en `https://mgn.<region>.amazonaws.com/`, donde `<region>` es el código de la región de AWS en la que se está replicando (por ejemplo, `https://mgn.us-east-1.amazonaws.com`). Se necesitan direcciones URL de servicio de Amazon Simple Storage Service (Amazon S3) para descargar el software Servicio de migración de aplicaciones.
  - El instalador del agente de replicación de AWS debe tener acceso a la URL del bucket S3 de la región de AWS que utilice con Servicio de migración de aplicaciones.
  - La subred del área de almacenamiento debe tener acceso a Amazon S3.
  - Los servidores de origen en los que está instalado el agente de replicación de AWS deben poder enviar datos a los servidores de replicación de la subred del área de ensayo y al punto de conexión de la API del Application Migration Service en `https://mgn.<region>.amazonaws.com/`.

En la siguiente tabla se muestran los puertos necesarios.

Origen	Destino	Puerto	Para obtener más información, consulte
Su centro de datos de origen	La URL del servicio Amazon S3	443 (TCP)	Comunicación a través del puerto TCP 443
Su centro de datos de origen	Dirección de consola específica de la región de AWS para el servicio de migración de aplicaciones	443 (TCP)	Comunicación entre los servidores de origen y el Servicio de migración de aplicaciones a través del puerto TCP 443

Su centro de datos de origen	Subred de área de almacenamiento	1500 (TCP)	Comunicación entre los servidores de origen y la subred del área de almacenamiento a través del puerto TCP 1500
Subred de área de almacenamiento	Dirección de consola específica de la región de AWS para el servicio de migración de aplicaciones	443 (TCP)	Comunicación entre la subred del área de ensayo y el Servicio de migración de aplicaciones a través del puerto TCP 443
Subred de área de almacenamiento	La URL del servicio Amazon S3	443 (TCP)	Comunicación a través del puerto TCP 443
Subred de área de almacenamiento	Punto de conexión Amazon EC2 de la Región de AWS de la subred	443 (TCP)	Comunicación a través del puerto TCP 443

Limitaciones

El servicio de migración de aplicaciones no está disponible actualmente en todas las regiones y sistemas operativos de AWS.

- Regiones de AWS admitidas
- Sistemas operativos compatibles

Arquitectura

El siguiente diagrama ilustra la arquitectura de red para una migración típica. Para obtener más información sobre esta arquitectura, consulte la documentación del Servicio de migración de aplicaciones y el vídeo sobre la arquitectura del servicio de migración de aplicaciones y la arquitectura de red.

La siguiente vista detallada muestra la configuración de los puntos de conexión de VPC de la interfaz en el área de ensayo para conectar Amazon S3 y Servicio de migración de aplicaciones.

Herramientas

- AWS Application Migration Service es un servicio de AWS que simplifica, acelera y reduce el costo de volver a alojar aplicaciones en AWS.
- Los puntos de enlace de VPC de interfaz le permiten conectarse a los servicios que funcionan con AWS PrivateLink sin necesidad de una puerta de enlace a Internet, un dispositivo NAT, una conexión VPN o una conexión AWS Direct Connect. Las instancias de su VPC no necesitan direcciones IP públicas para comunicarse con los recursos del servicio. El tráfico entre su VPC y el otro servicio no sale de la red de Amazon.

Epics

Cree puntos de conexión para Servicio de migración de aplicaciones, Amazon EC2 y Amazon S3

Tarea	Descripción	Habilidades requeridas
Configure el punto de conexión de la interfaz para el Servicio de migración de aplicaciones.	El centro de datos de origen y la VPC del área de ensayo se conectan de forma privada al plano de control del Servicio de migración de aplicaciones a través del punto de conexión de la interfaz que se crea en la VPC del área de almacenam iento de destino. Para crear el punto de conexión: 1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.	Líder de migración

Tarea	Descripción	Habilidades requeridas
	2. En el panel de navegación, seleccione Puntos de conexión, Crear puntos de conexión. 3. En Service category, seleccione AWS services. 4. En Nombre del servicio, escriba `com.amazonaws.<region>.mgn` . En Tipo, seleccione Interfaz. 5. En VPC, seleccione el espacio provisional de la VPC de destino en la que se va a crear el punto de conexión. 6. En Subredes, seleccione las subredes (zonas de disponibilidad) en las que se van a crear las interfaces de red de punto de conexión. 7. Para activar el DNS privado en el punto de conexión de la interfaz, en la sección Configuración adicional , seleccione Habilitar el nombre DNS. 8. Seleccione un grupo de seguridad que permita la entrada desde la subred de VPC del área de ensayo a través de TCP 443.	

Tarea	Descripción	Habilidades requeridas
	9. Seleccione Crear punto de conexión. Para obtener más información, consulte Creación de puntos de conexión de la VPC de tipo interfaz en la documentación de Amazon VPC.	
Configure el punto de conexión de interfaz para Amazon EC2.	La VPC del área de ensayo se conecta de forma privada a la API de Amazon EC2 a través del punto de conexión de interfaz que usted crea en la VPC del área de ensayo de destino. Para crear el punto de conexión, siga las instrucciones de la historia anterior. • Para Nombre del servicio, escriba `com.amazonaws.<region>.ec2`. En Tipo, seleccione Interfaz. • El grupo de seguridad debe permitir el tráfico HTTPS entrante desde la subred de VPC del área de ensayo a través del puerto 443. • En la sección Configuración adicional, seleccione Habilitar el nombre DNS.	Líder de migración

Tarea	Descripción	Habilidades requeridas
Configure el punto de conexión de interfaz para Amazon S3.	El centro de datos de origen y la VPC del área de ensayo se conectan de forma privada a la API de Amazon S3 a través del punto de conexión de interfaz que usted crea en la VPC del área de ensayo de destino. Para crear el punto de conexión, siga las instrucciones que se proporcionan en la primera historia. • En Nombre del servicio, escriba `com.amazonaws.<region>.s3` . En Tipo, seleccione Interfaz. • El grupo de seguridad de VPC debe permitir el tráfico HTTPS entrante desde la subred de VPC del área de ensayo a través del puerto 443. • En la sección Configuración adicional, desactive Habilitar nombre DNS. Los puntos de conexión de tipo interfaz de Amazon S3 no admiten nombres de DNS privados. Nota: Se utiliza un punto de conexión de interfaz porque las conexiones de punto de conexión de puerta de enlace no se pueden ampliar más	Líder de migración

Tarea	Descripción	Habilidades requeridas
	allá de la VPC. (Para obtener más información, consulte la documentación de Amazon VPC).	
Creación del punto de conexión de la puerta de enlace de Amazon S3.	Durante la fase de configuración, el servidor de replicación debe conectarse a un bucket S3 para descargar las actualizaciones de software del servidor de replicación de AWS. Sin embargo, los puntos de conexión de la interfaz Amazon S3 no admiten nombres de DNS privados y no hay forma de proporcionar un nombre de DNS de punto de conexión de Amazon S3 a un servidor de replicación. Para mitigar este problema, debe crear un punto de conexión de puerta de enlace de Amazon S3 en la VPC a la que pertenece la subred del área de ensayo y actualizar las tablas de rutas de la subred de almacenamiento provisional con las rutas pertinentes. Para obtener más información, consulte Crear un punto de enlace en la PrivateLink documentación de AWS.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Configure el DNS en las instalaciones para resolver los nombres DNS privados de los puntos de conexión.	Los puntos de conexión de la interfaz de Servicio de migración de aplicaciones y Amazon EC2 tienen nombres de DNS privados que se pueden resolver en la VPC. Sin embargo, también debe configurar los servidores en las instalaciones para resolver los nombres DNS privados de estos puntos de conexión de la interfaz. Estos servidores se pueden configurar de varias formas. En este patrón, probamos esta funcionalidad mediante el reenvío de las consultas de DNS en las instalaciones al punto de conexión de entrada Amazon Route 53 Resolver en la VPC del área de ensayo. Para obtener más informaci ón, consulte Resolución de consultas de DNS entre las VPC y su red en la documenta ción de Route 53.	Ingeniero de migraciones

Conéctese al plano de control del Servicio de migración de aplicaciones a través de un enlace privado

Tarea	Descripción	Habilidades requeridas
Instale AWS Replication Agent mediante AWS PrivateLink.	1. Descargue el agente de replicación de AWS en un bucket S3 privado de la región de destino. 2. Inicie sesión en los servidores de origen que desee migrar. El instalado r del agente de replicación de AWS necesita acceso de red al servicio de migración de aplicaciones y a los puntos de conexión de Amazon S3. Como su red local no está abierta a los puntos de enlace públicos de Application Migration Service y Amazon S3, debe instalar el agente con la ayuda de los puntos de enlace de la interfaz que creó en los pasos anteriore s mediante AWS. PrivateLi nk A continuación se muestra un ejemplo para Linux: 1. Descargar el agente mediante el comando:	Ingeniero de migraciones

Tarea	Descripción	Habilidades requeridas
	`wget -O ./aws-replication-installer-init.py \ https://aws-application-migration-service-<aws_region>.bucket.<s3-endpoint-DNS-name>/latest/linux/aws-replication-installer-init.py` Nota: `bucket` es una palabra clave estática que debe añadir antes del nombre DNS del punto de conexión de la interfaz Amazon S3. Para obtener más información, consulte la documentación de Amazon S3. Por ejemplo, si el nombre DNS del punto de conexión de la interfaz Amazon S3 es `vpce-009c8b07adb052a11-qgf8q50y.s3.us-west-1.vpce.amazonaws.com` y la región de AWS es `us-west-1`, utilizaría el comando: `wget -O ./aws-replication-installer-init.py \ https://aws-application-migration-service-us-west-1.bucket.vpce-009c8b`	

Tarea	Descripción	Habilidades requeridas
	07adb052a11-qgf8q5 0y.s3.us-west-1.vp ce.amazonaws.com/l atest/linux/aws-re plication-installer- init.py 2. Instalar el agente: • Si seleccionó Habilitar el nombre DNS al crear un punto de conexión de interfaz para el Servicio de migración de aplicaciones, ejecute el comando: sudo python3 aws- replication-installer- init.py \ --region <aws_regi on> \ --aws-access-key-i d <access-key> \ --aws-secret-acces s-key <secret-key> \ --no-prompt \ --s3-endpoint <s3- endpoint-DNS-name> • Si no seleccionó Habilitar el nombre DNS al crear el punto de conexión de la interfaz para el Servicio de migración de aplicaciones, ejecute el comando:	

Tarea	Descripción	Habilidades requeridas
	`sudo python3 aws-replication-installer-init.py \ --region <aws_region> \ --aws-access-key-id <access-key> \ --aws-secret-access-key <secret-key> \ --no-prompt \ --s3-endpoint <s3-endpoint-DNS-name> \ --endpoint <mgn-endpoint-DNS-name>` Para obtener más información, consulte las Instrucciones de instalación del AWS Replication Agent en la documentación del Servicio de migración de aplicaciones. Una vez establecida la conexión con el Servicio de migración de aplicaciones e instalado el agente de replicación de AWS, siga las instrucciones de la documentación del Servicio de migración de aplicaciones para migrar los servidores de origen a la VPC y la subred de destino.	

Recursos relacionados

Documentación del Servicio de migración de aplicaciones

- Conceptos
- Flujo de trabajo de migración
- Guía de inicio rápido
- PREGUNTAS FRECUENTES
- Solución de problemas

Recursos adicionales

- Servicio de migración de aplicaciones de AWS: Una introducción técnica (tutorial sobre AWS Training and Certification)
- Arquitectura y arquitectura de red del Servicio de migración de aplicaciones de AWS (vídeo)

Información adicional

Solución de problemas de instalaciones de AWS Replication Agent en servidores Linux

Si recibe un error gcc en un servidor Amazon Linux, configure el repositorio de paquetes y utilice el siguiente comando:

```
## sudo yum groupinstall "Development Tools"
```

Cree objetos de Infoblox con los recursos CloudFormation personalizados de AWS y Amazon SNS

Documento creado por Tim Sutton (AWS)

Entorno: PoC o piloto	Tecnologías: redes	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon SNS CloudFormation; AWS KMS; AWS Lambda; AWS Organizations		

Resumen

El sistema de nombres de dominio (DNS), el protocolo de configuración dinámica de host (DHCP) y la administración de direcciones IP (Infoblox DDI) permiten centralizar y controlar de manera eficiente un entorno híbrido complejo. Con Infoblox DDI se pueden descubrir y registrar todos los activos de la red en una base de datos de Administrador de direcciones IP (IPAM) autorizada, además de administrar el DNS en las instalaciones y en la nube de Amazon Web Services (AWS) mediante los mismos dispositivos.

Este patrón describe cómo usar un recurso CloudFormation personalizado de AWS para crear objetos de Infoblox (por ejemplo, registros DNS u objetos de IPAM) mediante una llamada a la API WAPI de Infoblox. Para obtener más información sobre la WAPI de Infoblox, consulte la documentación de la WAPI en la documentación de Infoblox.

Al utilizar el enfoque de este patrón, puede obtener una vista unificada de los registros de DNS y las configuraciones de IPAM para sus entornos de AWS y en las instalaciones, además de eliminar los procesos manuales que crean registros y aprovisionan sus redes. Se puede utilizar el enfoque de este patrón para los casos de uso siguientes:

- Agregar un registro A después de crear una instancia de Amazon Elastic Compute Cloud (Amazon EC2)
- Agregar un registro CNAME después de crear un Equilibrador de carga de aplicación
- Agregar un objeto de red después de crear una nube privada virtual (VPC)

- Proporcionar el rango de redes siguiente y usar ese rango para crear subredes

También puede ampliar este patrón y utilizar otras funciones del dispositivo Infoblox, como agregar diferentes tipos de registros DNS o configurar Infoblox vDiscovery.

El patrón usa un hub-and-spoke diseño en el que el hub requiere conectividad con el dispositivo Infoblox en la nube de AWS o en las instalaciones y usa AWS Lambda para llamar a la API de Infoblox. El radio se encuentra en la misma cuenta o en una cuenta diferente de la misma organización en AWS Organizations y llama a la función Lambda mediante un recurso CloudFormation personalizado de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Un dispositivo o una red de Infoblox existente, instalado en la nube de AWS, en las instalaciones o en ambos, y configurado con un usuario administrador que puede administrar las acciones de IPAM y DNS. Para obtener más información acerca de este tema, consulte About admin accounts (Acerca de las cuentas de administrador) en la documentación de Infoblox.
- Una zona de DNS autorizada existente a la que desee agregar registros del dispositivo Infoblox. Para obtener más información al respecto, consulte Configuring authoritative zones (Configurar zonas autorizadas) en la documentación de Infoblox.
- Dos cuentas de AWS activas en AWS Organizations. Una cuenta es la cuenta de hub y la otra es la cuenta de spoke.
- Las cuentas de hub y spoke deben estar en la misma región de AWS.
- La VPC de la cuenta de hub debe conectarse al dispositivo Infoblox; por ejemplo, mediante AWS Transit Gateway o interconexión de VPC.
- AWS Serverless Application Model (AWS SAM), instalado y configurado localmente con AWS Cloud9 o AWS. CloudShell
- Los archivos `ClientTest.yaml` y `Infoblox-Hub.zip` (adjuntos), descargados en el entorno local que contiene AWS SAM.

Limitaciones

- El token de servicio del recurso CloudFormation personalizado de AWS debe provenir de la misma región en la que se creó la pila. Se recomienda utilizar una cuenta de hub en cada región, en lugar

de crear un tema de Amazon Simple Notification Service (Amazon SNS) en una región y llamar a la función de Lambda en otra región.

Versiones de producto

- Infoblox, versión 2.7

Arquitectura

En los siguientes diagramas se muestra el flujo de este patrón.

El diagrama muestra los siguientes componentes para la solución de este patrón:

1. CloudFormation Los recursos personalizados de AWS le permiten escribir una lógica de aprovisionamiento personalizada en las plantillas que AWS CloudFormation ejecuta al crear, actualizar o eliminar pilas. Al crear una pila, AWS CloudFormation envía una `create` solicitud a un tema de SNS que supervisa una aplicación que se ejecuta en una instancia de EC2.
2. La notificación de Amazon SNS del recurso CloudFormation personalizado de AWS se cifra mediante una clave específica de AWS Key Management Service (AWS KMS) y el acceso está restringido a las cuentas de su organización en Organizations. El tema SNS inicia el recurso de Lambda que llama a la API WAPI de Infoblox.
3. Amazon SNS invoca las funciones de Lambda siguientes, que toman la URL de la WAPI de Infoblox, el nombre de usuario y la contraseña (nombre de recurso de Amazon (ARN) de AWS Secrets Manager) como variables de entorno:
   - `dnsapi.lambda_handler`— Recibe los `DNSValue` valores `DNSNameDNSType`, y del recurso CloudFormation personalizado de AWS y los utiliza para crear registros A de DNS y CNAME.
   - `ipaddr.lambda_handler`— Recibe los `Network Name` valores`VPCCIDR`, `TypeSubnetPrefix`, y del recurso CloudFormation personalizado de AWS y los utiliza para añadir los datos de la red a la base de datos de IPAM de Infoblox o para proporcionar al recurso personalizado la siguiente red disponible que se pueda utilizar para crear nuevas subredes.
   - `describeprefixes.lambda_handler`: Llama a la API de AWS `describe_managed_prefix_lists` mediante el filtro `"com.amazonaws."+Region+".s3"` para recuperar el `prefix ID` necesario.

Importante: estas funciones de Lambda están escritas en Python y son similares entre sí, pero llaman a diferentes API.

4. Puede implementar la red de Infoblox como dispositivos de red físicos, virtuales o basados en la nube. Se puede implementar en las instalaciones o como un dispositivo virtual mediante una variedad de hipervisores, incluidos VMware ESXi, Microsoft Hyper-V, Linux KVM y Xen. También puede implementar la cuadrícula de Infoblox en la nube de AWS con una Imagen de máquina de Amazon (AMI).
5. El diagrama muestra una solución híbrida para la red de Infoblox que proporciona DNS e IPAM a los recursos en la nube de AWS y en las instalaciones.

Pila de tecnología

- AWS CloudFormation
- IAM
- AWS KMS
- AWS Lambda
- SAM de AWS
- AWS Secrets Manager
- Amazon SNS
- Amazon VPC

Herramientas

- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Key Management Service (AWS KMS) facilita poder crear y controlar claves criptográficas para proteger los datos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.

- AWS Organizations es un servicio de administración de cuentas que permite agrupar varias cuentas AWS en una organización que usted crea y administra de manera centralizada.
- AWS Secrets Manager ayuda a reemplazar las credenciales codificadas en el código, incluidas las contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación.
- AWS Serverless Application Model (AWS SAM) es un marco de código abierto que permite crear aplicaciones sin servidor en la nube de AWS.
- Amazon Simple Notification Service (Amazon SNS) permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- Amazon Virtual Private Cloud (Amazon VPC) permite lanzar recursos de AWS en una red virtual que se haya definido. Esa red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Código

Puede usar la CloudFormation plantilla de AWS de `ClientTest.yaml` muestra (adjunta) para probar el centro de Infoblox. Puede personalizar la CloudFormation plantilla de AWS para incluir los recursos personalizados de la siguiente tabla.

Crear un registro A con el recurso personalizado de spoke de Infoblox	Valores devueltos: `infobloxref` : referencias de Infoblox Recurso de ejemplo: `ARECORDCustomResource:` `  Type: "Custom::InfobloxAPI"` `  Properties:` `  ServiceToken: !Sub arn:aws:sns:${AWS::Region}:${HubAccountID}:RunInfobloxDNSFunction` `  DNSName: 'arecordtest.company.com'`

```
    DNSType: 'ARecord'

    DNSValue: '10.0.0.1'
```

crear un registro de CNAME con el recurso personalizado de spoke de Infoblox

Valores devueltos:

`infobloxref` : referencias de Infoblox

Recurso de ejemplo:

```
CNAMECustomResource:

  Type: "Custom::InfobloxAPI"

  Properties:

    ServiceToken: !Sub arn:aws:sns:
${AWS::Region}:${HubAccountID}:Ru
nInfoblox

    DNSFunction

    DNSName: 'cnametest.company.com'

    DNSType: 'cname'

    DNSValue: 'aws.amazon.com'
```

crear un objeto de red utilizando el recurso personalizado de spoke de Infoblox

Valores devueltos:

`infobloxref` : referencias de Infoblox

`network`: Rango de red (igual a `VPCCIDR`)

Recurso de ejemplo:

```
VPCCustomResource:

  Type: 'Custom::InfobloxAPI'

  Properties:

    ServiceToken: !Sub  arn:aws:sns:
${AWS::Region}:${HubAccountID}:Ru
nInfobloxNextSubnetFunction

    VPCCIDR: !Ref VpcCIDR

    Type: VPC

    NetworkName: My-VPC
```

Recuperar la subred disponible siguiente mediante el recurso personalizado de spoke de Infoblox	Valores devueltos: `infobloxref` : referencias de Infoblox `network` : El rango de redes de la subred Recurso de ejemplo: `Subnet1CustomResource:` `  Type: 'Custom::InfobloxAPI'` `  DependsOn: VPCCustomResource` `  Properties:` `  ServiceToken: !Sub  arn:aws:sns:${AWS::Region}:${HubAccountID}:RunInfobloxNextSubnetFunction` `  VPCCIDR: !Ref VpcCIDR` `  Type: Subnet` `  SubnetPrefix: !Ref SubnetPrefix` `NetworkName: My-Subnet`

Epics

Crear y configurar la VPC de la cuenta de hub

Tarea	Descripción	Habilidades requeridas
Crear una VPC con una conexión al dispositivo Infoblox.	Inicie sesión en la consola de administración de AWS de su cuenta de hub y cree una VPC siguiendo los pasos de Amazon VPC en la implement	Administrador de red, administrador del sistema

Tarea	Descripción	Habilidades requeridas
	ación de referencia de inicio rápido de la nube de AWS en los inicios rápidos de AWS. Importante: La VPC debe tener conectividad HTTPS con el dispositivo Infoblox y se recomienda utilizar una subred privada para esta conexión.	

Tarea	Descripción	Habilidades requeridas
(Opcional) Cree los puntos de conexión de VPC para las subredes privadas.	Los puntos de conexión de VPC proporcionan conectividad a los servicios públicos para las subredes privadas. Se necesitan los puntos de conexión siguientes: • Un punto de enlace para Amazon Simple Storage Service (Amazon S3) que permite a Lambda comunicarse con AWS CloudFormation • Un punto de conexión de interfaz a Secrets Manager para permitir la conectividad con Secrets Manager • Un punto de conexión de interfaz a AWS KMS que permita el cifrado del tema de SNS y del secreto de Secrets Manager Para obtener más información acerca de la creación de puntos de conexión para las subredes privadas, consulte VPC endpoints (Puntos de conexión de VPC) de la documentación de Amazon VPC.	Administrador de red, administrador del sistema

Implementar el hub de Infoblox

Tarea	Descripción	Habilidades requeridas
Cree la plantilla SAM de AWS.	1. Ejecute el comando `unzip Infoblox-Hub.zip` en el entorno que contiene AWS SAM. 2. Ejecute el comando `cd Hub/` para cambiar su directorio al directorio `Hub`. 3. Ejecute el comando `sam build` para procesar el archivo de plantilla SAM de AWS, el código de la aplicación y cualquier archivo y dependencia específicos del idioma. El comando `sam build` también copia los artefactos de construcción en el formato y la ubicación esperados para la siguiente historia.	Desarrollador, administrador del sistema
Implemente la plantilla SAM de AWS.	El `sam deploy` comando toma los parámetros necesarios y los guarda en el `samconfig.toml` archivo, almacena la CloudFormation plantilla de AWS y las funciones de Lambda en un bucket de S3 y, a continuación, implementa la CloudFormation plantilla de AWS en su cuenta de hub.	Desarrollador, administrador del sistema

Tarea	Descripción	Habilidades requeridas
	El código de ejemplo siguiente muestra cómo implementar la plantilla AWS SAM: `$ sam deploy --guided` `Configuring SAM deploy` `==========` `==` `Looking for config file [samconfig.toml] : Found` `Reading default arguments : Success` `Setting default arguments for 'sam deploy'` `==========` `==========` `Stack Name [Infoblox-Hub]:` `AWS Region [eu-west-1]:` `Parameter InfobloxUsername:` `Parameter InfobloxPassword:` `Parameter InfobloxIPAddress [xxx.xxx.xx.xxx]:` `Parameter AWSOrganisationID [o-xxxxxxxxx]:` `Parameter VPCID [vpc-xxxxxxxxx]:` `Parameter VPCCIDR [xxx.xxx.xxx.xxx/16]:`	

Tarea	Descripción	Habilidades requeridas
	<pre>Parameter VPCSubnetID1 [subnet-xxx]: Parameter VPCSubnetID2 [subnet-xxx]: Parameter VPCSubnetID3 [subnet-xxx]: Parameter VPCSubnetID4 []: #Shows you resources changes to be deployed and require a 'Y' to initiate deploy Confirm changes before deploy [Y/n]: y #SAM needs permission to be able to create roles to connect to the resources in your template Allow SAM CLI IAM role creation [Y/n]: n Capabilities [['CAPABILITY_NAMED_IAM']]: Save arguments to configuration file [Y/n]: y SAM configuration file [samconfig.toml]: SAM configuration environment [default]:</pre> Importante: Debe utilizar la opción `--guided` cada vez, ya que las credenciales de inicio de sesión de Infoblox no	

Tarea	Descripción	Habilidades requeridas
	se almacenan en el archivo `samconfig.toml` .	

Recursos relacionados

- Getting started with WAPIs using Postman (Cómo empezar a utilizar las WAPI con Postman) (blog de Infoblox)
- Provisioning vNIOS for AWS Using the BYOL Model (Aprovisionar vNIOS para AWS mediante el modelo BYOL) (documentación de Infoblox)
- quickstart-aws-vpc(repositorio) GitHub
- describe_managed_prefix_lists (documentación de AWS SDK para Python)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Personalice CloudWatch las alertas de Amazon para AWS Network Firewall

Documento creado por Jason Owens (AWS)

Entorno: PoC o piloto	Tecnologías: redes, seguridad, identidad, cumplimiento	Carga de trabajo: código abierto
Servicios de AWS: Amazon CloudWatch Logs; AWS Network Firewall; AWS CLI		

Resumen

El patrón le ayuda a personalizar las CloudWatch alertas de Amazon que genera el Network Firewall de Amazon Web Services (AWS). Puede utilizar reglas predefinidas o crear reglas personalizadas que determinen el mensaje, los metadatos y la gravedad de las alertas. A continuación, puedes actuar en función de estas alertas o automatizar las respuestas de otros servicios de Amazon, como Amazon EventBridge.

En este patrón, se generan reglas de firewall compatibles con Suricata. Suricata es un motor de detección de amenazas de código abierto. Primero debe crear reglas sencillas y, a continuación, probarlas para confirmar que las CloudWatch alertas se han generado y registrado. Una vez que haya probado correctamente las reglas, las modificará para definir los mensajes personalizados, los metadatos y la gravedad y, a continuación, volverá a probarlas para confirmar las actualizaciones.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada en Linux, macOS o estación de trabajo de Windows. Para obtener más información, consulte Installing or updating the latest version of the AWS CLI (Instalar o actualizar la última versión de AWS CLI.

- AWS Network Firewall instalado y configurado para usar CloudWatch registros. Para obtener más información, consulte Logging network traffic from AWS Network Firewall (Registrar el tráfico de red desde AWS Network Firewall).
- Una instancia de Amazon Elastic Compute Cloud (Amazon EC2) en una subred privada de una nube privada virtual (VPC) que esté protegida por Network Firewall.

Versiones de producto

- Para la versión 1 de AWS CLI, utilice 1.18.180 o una versión posterior. Para la versión 2 de AWS CLI, utilice 2.1.2 o una versión posterior.
- El archivo classification.config de la versión 5.0.2 de Suricata. Para obtener una copia de este archivo de configuración, consulte la sección Información adicional.

Arquitectura

Pila de tecnología de destino

- Network Firewall
- Amazon CloudWatch Logs

Arquitectura de destino

El diagrama de la arquitectura muestra el flujo de trabajo siguiente:

1. Una instancia de EC2 de una subred privada realiza una solicitud mediante curl o Wget.
2. Network Firewall procesa el tráfico y genera una alerta.
3. Network Firewall envía las alertas registradas a CloudWatch Logs.

Herramientas

Servicios de AWS

- Amazon le CloudWatch ayuda a supervisar las métricas de sus recursos de AWS y las aplicaciones que ejecuta en AWS en tiempo real.

- Amazon CloudWatch Logs le ayuda a centralizar los registros de todos sus sistemas, aplicaciones y servicios de AWS para que pueda supervisarlos y archivarlos de forma segura.
- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que permite interactuar con los servicios de AWS mediante comandos en el intérprete de comandos de línea de comandos.
- AWS Network Firewall es un servicio de detección y prevención de intrusiones y de firewall de red con estado y administrado para nubes privadas virtuales (VPC) en la nube de AWS.

Otras herramientas y servicios

- curl: curl es una herramienta y biblioteca de línea de comandos de código abierto.
- Wget: GNU Wget es una herramienta de línea de comandos gratuita.

Epics

Crear las reglas y el grupo de reglas del firewall

Tarea	Descripción	Habilidades requeridas
Crear reglas.	1. En un editor de texto, cree una lista de reglas que desee agregar al firewall. Cada regla debe estar en una línea independiente. El valor del parámetro `classtype` proviene del archivo de configuración de clasificación predeterminado de Suricata. Para obtener el archivo de configuración completo, consulte la sección Información adicional. A continuación se muestran dos ejemplos de reglas.	Administrador de sistemas de AWS, administrador de red

Tarea	Descripción	Habilidades requeridas
	`` alert http any any -> any any (content:"badstuff "; classtype:misc- activity; sid:3; rev:1;) alert http any any -> any any (content: "morebadstuff"; classtype:bad-unkn own; sid:4; rev:1;) ``` 2. Guarde las reglas en un archivo denominado `custom.rules` .	

Tarea	Descripción	Habilidades requeridas
Cree un grupo de reglas.	En la AWS CLI, ingrese el comando siguiente. De este modo se crea el grupo de reglas. `# aws network-firewall create-rule-group \ --rule-group-name custom --type STATEFUL \ --capacity 10 --rules file://custom.rules \ --tags Key=environment,Value=development` El siguiente es un ejemplo de salida. Anote el `RuleGroup Arn` , que necesitará en un paso posterior. `{ "UpdateToken": "4f998d72-973c-490a-bed2-fc3460547e23", "RuleGroupResponse": { "RuleGroupArn": "arn:aws:network-firewall:us-east-2:1234567890:stateful-rulegroup/custom", "RuleGroupName": "custom", "RuleGroupId": "238a8259-9eaf-48bb-90af-5e690cf8c48b",`	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	<pre>"Type": "STATEFUL", "Capacity": 10, "RuleGroupStatus": "ACTIVE", "Tags": [{ "Key": "environment", "Value": "development" }] }</pre>	

Actualizar la política de firewall

Tarea	Descripción	Habilidades requeridas
Obtenga el ARN de la política de firewall.	En la AWS CLI, ingrese el comando siguiente. Esto devuelve el nombre de recurso de Amazon (ARN) de la política de firewall. Registre el ARN para su uso posterior en este patrón. <pre># aws network-firewall describe-firewall \ --firewall-name aws-network-firewall-anfw \ --query 'Firewall.FirewallPolicyArn'</pre>	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	A continuación se muestra un ejemplo de ARN que devuelve este comando. `"arn:aws:network-firewall:us-east-2:1234567890:firewall-policy/firewall-policy-anfw"`	

Tarea	Descripción	Habilidades requeridas
Actualice la política de firewall.	En un editor de texto, copie y pegue el siguiente código. Reemplace `<RuleGroupArn>` por el valor que registró en la sección Epics anterior. Guarde el archivo como `firewall-policy-anfw.json` . `{` `  "StatelessDefaultActions": [` `  "aws:forward_to_sfe"` `  ],` `  "StatelessFragmentDefaultActions": [` `  "aws:forward_to_sfe"` `  ],` `  "StatefulRuleGroupReferences": [` `  {` `  "ResourceArn": "<RuleGroupArn>"` `  }` `  ]` `}` En la AWS CLI, ingrese el comando siguiente. Este comando requiere un update token (actualizar token) para agregar las nuevas reglas. El token se usa para confirmar que la política no ha cambiado	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	desde la última vez que se recuperó. `UPDATETOKEN=(`aws network-firewall describe-firewall-policy \ --firewall-policy-name firewall-policy-anfw \ --output text --query UpdateToken`)` `aws network-firewall update-firewall-policy \ --update-token $UPDATETOKEN \ --firewall-policy-name firewall-policy-anfw \ --firewall-policy file://firewall-policy-anfw.json`	

Tarea	Descripción	Habilidades requeridas
Confirme las actualizaciones de la política.	(Opcional) Si desea confirmar que se agregaron las reglas y ver el formato de la política, ingrese el comando siguiente en la AWS CLI. `# aws network-firewall describe-firewall-policy \ --firewall-policy-name firewall-policy-anfw \ --query FirewallPolicy` El siguiente es un ejemplo de salida. `{ "StatelessDefaultActions": [ "aws:forward_to_sfe" ], "StatelessFragmentDefaultActions": [ "aws:forward_to_sfe" ], "StatefulRuleGroupReferences": [ { "ResourceArn": "arn:aws:network-firewall:us-east-2:1234567890:stateful-rulegroup/custom" }`	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	<pre>] }</pre>	

Probar la funcionalidad de las alertas

Tarea	Descripción	Habilidades requeridas
Genere alertas para las pruebas.	1. Inicie sesión en una estación de trabajo de prueba dentro de la subred del firewall. 2. Ingrese los comandos que deberían generar alertas. Puede utilizar, por ejemplo `wget` o `curl`. <pre>wget -U "badstuff" http://www.amazon. com -o /dev/null</pre> <pre>curl -A "morebads tuff" http://ww w.amazon.com -o / dev/null</pre>	Administrador de sistemas de AWS
Valide que las alertas estén registradas.	1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/ 2. Navegue hasta el grupo de registros y el flujo correctos. Para obtener más información, consulte Ver los datos de registro	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	enviados a CloudWatch Logs (documentación de CloudWatch Logs). 3. Confirme que los eventos de registro son similares a los ejemplos siguientes. Los ejemplos muestran solo la parte relevante de la alerta. Ejemplo 1 `"alert": { "action": "allowed", "signature_id": 3, "rev": 1, "signature": "", "category": "Misc activity", "severity": 3 }` Ejemplo 2 `"alert": { "action": "allowed", "signature_id": 4, "rev": 1, "signature": "", "category": "Potentially Bad Traffic",`	

Tarea	Descripción	Habilidades requeridas
	<pre>"severity ": 2 } </pre>	

Actualizar las reglas y el grupo de reglas del firewall

Tarea	Descripción	Habilidades requeridas
Actualice las reglas del firewall.	1. Abra el archivo `custom.rules` en un editor de texto. 2. Cambie la primera regla para que sea similar a la siguiente. Esta regla debe escribirse en una sola línea del archivo. <pre>alert http any any -> any any (msg:"Watch out - Bad Stuff!!"; content:"badstuff" ; classtype:misc-activity; priority: 2; sid:3; rev:2; metadata:custom-field-2 Danger!, custom-field More Info;)</pre> De este modo, se realizan los siguientes cambios en la regla: • Se agrega una cadena msg (sitio web de Suricata) que proporciona información textual sobre la firma o la alerta. En la	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	alerta generada, esto se asigna a la firma. • Se ajusta la prioridad predeterminada (sitio web de Suricata) de `misc-activity` , que pasa de 3 a 2. Para ver los valores predeterminados de los distintos `classtypes` , consulte la sección Información adicional. • Se agregan metadatos personalizados (sitio web de Suricata) a la alerta. Se trata de información adicional que se agrega a la firma. Se recomienda utilizar pares clave-valor. • Se cambia la rev (sitio web de Suricata) de 1 a 2. Esto representa la versión de la firma.	

Tarea	Descripción	Habilidades requeridas
Actualice el grupo de reglas.	Ejecute los comandos siguientes en la AWS CLI. Utilice el ARN de su política de firewall. Estos comandos obtienen un token de actualización y actualizan el grupo de reglas con los cambios de las reglas. `# UPDATETOKEN=(`aws network-firewall \ describe-rule-group \ --rule-group-arn arn:aws:network-firewall:us-east-2:123457890:stateful-rulegroup/custom \ --output text --query UpdateToken`)` `# aws network-firewall update-rule-group \ --rule-group-arn arn:aws:network-firewall:us-east-2:1234567890:stateful-rulegroup/custom \ --rules file://custom.rules \ --update-token $UPDATETOKEN` El siguiente es un ejemplo de salida. `{`	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	"UpdateToken": "7536939f-6a1d-414c-96d1-bb28110996ed", "RuleGroupResponse": { "RuleGroupArn": "arn:aws:network-firewall:us-east-2:1234567890:stateful-rulegroup/custom", "RuleGroupName": "custom", "RuleGroupId": "238a8259-9eaf-48bb-90af-5e690cf8c48b", "Type": "STATEFUL", "Capacity": 10, "RuleGroupStatus": "ACTIVE", "Tags": [{ "Key": "environment", "Value": "development" }] } }	

Probar la funcionalidad de la alerta actualizada

Tarea	Descripción	Habilidades requeridas
Genere una alerta para probarla.	1. Inicie sesión en una estación de trabajo de prueba dentro de la subred del firewall.	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	2. Ingrese un comando que genere una alerta. Por ejemplo, puede utilizar `curl`. `curl -A "badstuff" http://www.amazon.com -o /dev/null`	

Tarea	Descripción	Habilidades requeridas
Valide la alerta modificada.	1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/ 2. Navegue hasta el grupo de registros y el flujo correctos. 3. Confirme que el evento de registro sea similar al ejemplo siguiente. El ejemplo solo muestra la parte pertinente de la alerta. `"alert": { "action": "allowed", "signature_id": 3, "rev": 2, "signature": "Watch out - Bad Stuff!!", "category": "Misc activity", "severity": 2, "metadata": { "custom-field": [ "More Info" ], "custom-field-2": [ "Danger!" ] } }`	Administrador de sistemas de AWS

Recursos relacionados

Referencias

- Send alerts from AWS Network Firewall to a Slack channel (Enviar alertas desde AWS Network Firewall a un canal de Slack) (Recomendaciones de AWS)
- Scaling threat prevention on AWS with Suricata (Escalar la prevención de amenazas en AWS con Suricata) (entrada del blog de AWS)
- Deployment models for AWS Network Firewall (Modelos de implementación para AWS Network Firewall) (entrada del blog de AWS)
- Suricata meta keyworks (Claves meta de Suricata) (documentación de Suricata)

Tutoriales y videos

- Taller de AWS Network Firewall

Información adicional

A continuación se muestra el archivo de configuración de clasificación de Suricata 5.0.2. Estas clasificaciones se utilizan al crear las reglas de firewall.

```
# config classification:shortname,short description,priority

config classification: not-suspicious,Not Suspicious Traffic,3
config classification: unknown,Unknown Traffic,3
config classification: bad-unknown,Potentially Bad Traffic, 2
config classification: attempted-recon,Attempted Information Leak,2
config classification: successful-recon-limited,Information Leak,2
config classification: successful-recon-largescale,Large Scale Information Leak,2
config classification: attempted-dos,Attempted Denial of Service,2
config classification: successful-dos,Denial of Service,2
config classification: attempted-user,Attempted User Privilege Gain,1
config classification: unsuccessful-user,Unsuccessful User Privilege Gain,1
config classification: successful-user,Successful User Privilege Gain,1
config classification: attempted-admin,Attempted Administrator Privilege Gain,1
config classification: successful-admin,Successful Administrator Privilege Gain,1

# NEW CLASSIFICATIONS
config classification: rpc-portmap-decode,Decode of an RPC Query,2
```

```
config classification: shellcode-detect,Executable code was detected,1
config classification: string-detect,A suspicious string was detected,3
config classification: suspicious-filename-detect,A suspicious filename was detected,2
config classification: suspicious-login,An attempted login using a suspicious username
 was detected,2
config classification: system-call-detect,A system call was detected,2
config classification: tcp-connection,A TCP connection was detected,4
config classification: trojan-activity,A Network Trojan was detected, 1
config classification: unusual-client-port-connection,A client was using an unusual
 port,2
config classification: network-scan,Detection of a Network Scan,3
config classification: denial-of-service,Detection of a Denial of Service Attack,2
config classification: non-standard-protocol,Detection of a non-standard protocol or
 event,2
config classification: protocol-command-decode,Generic Protocol Command Decode,3
config classification: web-application-activity,access to a potentially vulnerable web
 application,2
config classification: web-application-attack,Web Application Attack,1
config classification: misc-activity,Misc activity,3
config classification: misc-attack,Misc Attack,2
config classification: icmp-event,Generic ICMP event,3
config classification: inappropriate-content,Inappropriate Content was Detected,1
config classification: policy-violation,Potential Corporate Privacy Violation,1
config classification: default-login-attempt,Attempt to login by a default username and
 password,2

# Update
config classification: targeted-activity,Targeted Malicious Activity was Detected,1
config classification: exploit-kit,Exploit Kit Activity Detected,1
config classification: external-ip-check,Device Retrieving External IP Address
 Detected,2
config classification: domain-c2,Domain Observed Used for C2 Detected,1
config classification: pup-activity,Possibly Unwanted Program Detected,2
config classification: credential-theft,Successful Credential Theft Detected,1
config classification: social-engineering,Possible Social Engineering Attempted,2
config classification: coin-mining,Crypto Currency Mining Activity Detected,2
config classification: command-and-control,Malware Command and Control Activity
 Detected,1
```

Migrar registros DNS de forma masiva a una zona alojada privada de Amazon Route 53

Creado por Ram Kandaswamy (AWS)

Entorno: producción	Tecnologías: redes; nativas de la nube; infraestructura DevOps	Servicios de AWS: AWS Cloud9; Amazon Route 53; Amazon S3

Resumen

Los ingenieros de redes y los administradores de la nube necesitan una forma eficaz y sencilla de añadir registros del Sistema de nombres de dominio (DNS) a las zonas alojadas privadas en Amazon Route 53. El uso de un enfoque manual para copiar las entradas de una hoja de cálculo de Microsoft Excel a las ubicaciones adecuadas de la consola de Route 53 es tedioso y propenso a errores. Este patrón describe un enfoque automatizado que reduce el tiempo y el esfuerzo necesarios para añadir varios registros. También proporciona un conjunto de pasos repetibles para la creación de varias zonas alojadas.

Este patrón utiliza el entorno de desarrollo integrado (IDE) AWS Cloud9 para el desarrollo y las pruebas, y Amazon Simple Storage Service (Amazon S3) para almacenar registros. Para trabajar con los datos de manera eficiente, el patrón usa el formato JSON debido a su simplicidad y su capacidad para admitir un diccionario de Python (tipo de datos `dict`).

Nota: si puede generar un archivo de zona desde su sistema, considere utilizar la característica de importación de Route 53 en su lugar.

Requisitos previos y limitaciones

Requisitos previos

- Una hoja de cálculo de Excel que contiene registros de zonas alojadas privadas
- Familiaridad con distintos tipos de registros DNS, como el registro A, el registro Name Authority Pointer (NAPTR) y el registro SRV (consulte Tipos de registros DNS compatibles)
- Familiaridad con el lenguaje Python y sus bibliotecas

Limitaciones

- El patrón no proporciona una cobertura amplia para todos los escenarios de casos de uso. Por ejemplo, la llamada change_resource_record_sets no usa todas las propiedades disponibles de la API.
- En la hoja de cálculo de Excel, se supone que el valor de cada fila es único. Se espera que aparezcan varios valores para cada nombre completo del dominio (FQDN) en la misma fila. Si eso no es cierto, debe modificar el código proporcionado en este patrón para realizar la concatenación necesaria.
- El patrón utiliza AWS SDK para Python (Boto3) para llamar directamente al servicio Route 53. Puede mejorar el código para utilizar un CloudFormation contenedor de AWS para los `update_stack` comandos `create_stack` y, además, utilizar los valores de JSON para rellenar los recursos de la plantilla.

Arquitectura

Pila de tecnología

- Zonas alojadas privadas de Route 53 para enrutar el tráfico
- IDE de AWS Cloud9 para desarrollo y pruebas
- Amazon S3 para almacenar el archivo JSON de salida

El flujo de trabajo consta de los siguientes pasos, tal como se ilustra en el diagrama anterior y se describe en la sección Epics:

1. Cargue una hoja de cálculo de Excel que contenga la información del conjunto de registros en un bucket de S3.
2. Cree y ejecute un script de Python que convierta los datos de Excel al formato JSON.
3. Lea los registros del bucket de S3 y limpie los datos.
4. Cree conjuntos de registros en su zona alojada privada.

Herramientas

- Route 53: Amazon Route 53 es un servicio web de DNS escalable y de alta disponibilidad que se utiliza para gestionar el registro de dominio, enrutamiento de DNS y comprobación de estado.
- AWS Cloud9: AWS Cloud9 es un IDE que ofrece una completa experiencia de edición de código, compatible con varios lenguajes de programación y depuradores de tiempo de ejecución, además de un terminal integrado. Contiene una colección de herramientas que se utilizan para codificar, compilar, ejecutar, probar y depurar software, y le ayuda a lanzar software en la nube.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet. Puede utilizar Amazon S3 para almacenar y recuperar cualquier cantidad de datos en cualquier momento y desde cualquier parte de la web.

Epics

Prepare los datos para la automatización

Tarea	Descripción	Habilidades requeridas
Cree un archivo de Excel para sus registros.	Utilice los registros que ha exportado desde su sistema actual para crear una hoja de cálculo de Excel que contenga las columnas necesarias para un registro, como el nombre de dominio completo (FQDN), el tipo de registro, el tiempo de vida (TTL) y el valor. En el caso de los registros NAPTR y SRV, el valor es una combinación de varias propiedades, por lo que debe utilizar el método de Excel `concat` para combinar estas propiedades.	Ingeniero de datos, con conocimientos de Excel

Tarea	Descripción	Habilidades requeridas
	FqdnN Recor e Valor TTL somet .exam org A 1.1.1.1 900	
Verifique el entorno de trabajo.	En el IDE de AWS Cloud9, cree un archivo Python para convertir la hoja de trabajo de entrada de Excel al formato JSON. (En lugar de AWS Cloud9, también puede usar un SageMaker bloc de notas de Amazon para trabajar con código Python). Compruebe que la versión de Python que está utilizando sea la 3.7 o posterior. `python3 --version` Instale el paquete pandas. `pip3 install pandas --user`	AWS general

Tarea	Descripción	Habilidades requeridas
Convierta los datos de la hoja de cálculo de Excel a JSON.	Cree un archivo Python que contenga el siguiente código para convertirlo de Excel a JSON. `import pandas as pd` `data=pd.read_excel('./Book1.xls')` `data.to_json(path_or_buf='my.json', orient='records')` donde `Book1` es el nombre de la hoja de cálculo de Excel y `my.json` el nombre del archivo JSON de salida.	Ingeniero de datos, con conocimientos de Python
Cargue el archivo JSON en un bucket de S3.	Cargue el archivo `my.json` en un bucket de S3. Para obtener más información, consulte Creación de un bucket en la documentación de Amazon S3.	Desarrollador de aplicaciones

Insertar registros

Tarea	Descripción	Habilidades requeridas
Cree una zona alojada privada.	Use la API create_hosted_zone y el siguiente código de ejemplo de Python para crear una zona alojada privada. Sustituya los parámetros `hostedZoneName` , `vpcRegion`	Ingeniero en la nube, administrador de redes, con habilidades de Python

Tarea	Descripción	Habilidades requeridas
	y `vpcId` por sus propios valores. `import boto3` `import random` `hostedZoneName ="xxx"` `vpcRegion = "us-east-1"` `vpcId="vpc-xxxx"` `route53_client = boto3.client('route53')` `response = route53_client.create_hosted_zone(` `Name= hostedZoneName,` `VPC={` `'VPCRegion: vpcRegion,` `'VPCId': vpcId` `},` `CallerReference=str(random.random()*100000),` `HostedZoneConfig={` `'Comment': "private hosted zone created by automation",` `'PrivateZone': True` `}` `)` `print(response)` También puede usar una herramienta de infraestructura	

Tarea	Descripción	Habilidades requeridas
	como código (IaC), como AWS, CloudFormation para reemplazar estos pasos por una plantilla que cree una pila con los recursos y propiedad es adecuados.	
Recupere detalles en formato de diccionario de Amazon S3.	Use el siguiente código para leer el bucket de S3 y obtener los valores de JSON como un diccionario de Python. `fileobj = s3_client .get_object( Bucket=bu cket_name, Key='my.json' ) filedata = fileobj[' Body'].read() contents = filedata. decode('utf-8') json_content=json. loads(contents) print(json_content )` donde `json_content` contiene el diccionario de Python.	Desarrollador de aplicaciones, con conocimientos de Python

Tarea	Descripción	Habilidades requeridas
Limpie los valores de datos para los espacios y caracteres Unicode.	Como medida de seguridad para garantizar la exactitud de los datos, utilice el siguiente código para realizar una operación de extracción de los valores incluidos en `json_content` . Este código elimina los caracteres de espacio al principio y al final de cada cadena. También utiliza el método `replace` para eliminar los espacios duros (que no se rompan) (los caracteres `\xa0`). `for item in json_cont ent:` `fqn_name = unicodeda ta.normalize("NFKD ",item["FqdnName"] .replace("u'", "'").replace('\xa0', '').strip())` `rec_type = item["Rec ordType"].replace( '\xa0', '').strip()` `res_rec = {` `'Value': item["Val ue"].replace('\xa0', '').strip()` `}`	Desarrollador de aplicaciones, con conocimientos de Python

Tarea	Descripción	Habilidades requeridas
Insertar registros.	Use el siguiente código como parte del bucle `for` anterior. `change_response = route53_client.change_resource_record_sets( HostedZoneId="xxxxxxxx", ChangeBatch={ 'Comment': 'Created by automation', 'Changes': [ { 'Action': 'UPSERT', 'ResourceRecordSet': { 'Name': fqn_name, 'Type': rec_type, 'TTL': item["TTL"], 'ResourceRecords': res_rec } } ] } )`	Desarrollador de aplicaciones, con conocimientos de Python

Tarea	Descripción	Habilidades requeridas
	Dónde xxxxxxx es el ID de la zona alojada del primer paso de esta épica.	

Recursos relacionados

Referencias

- Creación de registros mediante la importación de un archivo de zona (documentación de Amazon Route 53)
- método create_hosted_zone (documentación de Boto3)
- método change_resource_record_sets (documentación de Boto3)

Tutoriales y videos

- El tutorial de Python (documentación de Python)

- Diseño de DNS con Amazon Route 53 (YouTube vídeo, charlas técnicas en línea de AWS)

Modificar los encabezados HTTP al migrar de F5 a un equilibrador de carga de aplicación en AWS

Creado por Sachin Trivedi (AWS)

Entorno: PoC o piloto	Origen: En las instalaciones	Destino: Nube de AWS
Tipo R: redefinir la plataforma	Carga de trabajo: todas las demás cargas de trabajo	Tecnologías: Redes; nube híbrida; migración
Servicios de AWS: Amazon CloudFront; Elastic Load Balancing (ELB); AWS Lambda		

Resumen

Cuando migra una aplicación que utiliza un equilibrador de carga de F5 a Amazon Web Services (AWS) y quiere usar un equilibrador de carga de aplicación en AWS, la migración de las reglas de F5 para las modificaciones de encabezados es un problema habitual. Un Application Load Balancer no admite modificaciones de encabezados, pero puedes usar Amazon CloudFront como red de entrega de contenido (CDN) y Lambda @Edge para modificar encabezados.

Este patrón describe las integraciones necesarias y proporciona un código de muestra para la modificación del encabezado mediante AWS CloudFront y Lambda @Edge.

Requisitos previos y limitaciones

Requisitos previos

- Aplicación en las instalaciones que usa un equilibrador de carga de F5 con una configuración que reemplaza el valor del encabezado HTTP mediante el uso de `if, else`. Para obtener más información sobre esta configuración, consulte Encabezado HTTP en la documentación del producto de F5.

Limitaciones

- Este patrón se aplica a la personalización del encabezado del equilibrador de carga de F5. Para otros equilibradores de carga de terceros, por favor consulte la documentación del equilibrador de carga para obtener información de soporte.
- Las funciones de Lambda que utilice para Lambda@Edge deben estar en la región Este de EE. UU. (Norte de Virginia).

Arquitectura

El siguiente diagrama muestra la arquitectura de AWS, incluyendo el flujo de integración entre la CDN y otros componentes de AWS.

Herramientas

Servicios de AWS

- Equilibrador de carga de aplicación – Un equilibrador de carga de aplicación es un servicio de equilibrio de carga totalmente gestionado por AWS que funciona en la séptima capa del modelo de interconexión de sistemas abiertos (OSI). Equilibra el tráfico entre varios destinos y admite solicitudes de enrutamiento avanzadas basadas en encabezados y métodos HTTP, cadenas de consulta y enrutamiento basado en el host o en la ruta.
- Amazon CloudFront: Amazon CloudFront es un servicio web que acelera la distribución de su contenido web estático y dinámico, como .html, .css, .js y archivos de imagen, a sus usuarios. CloudFront entrega su contenido a través de una red mundial de centros de datos denominados ubicaciones perimetrales para reducir la latencia y mejorar el rendimiento.
- Lambda @Edge – Lambda @Edge es una extensión de AWS Lambda que le permite ejecutar funciones para personalizar el contenido que se entrega. CloudFront Puede crear funciones en la región EE.UU. Este (Virginia del Norte) y, después, asociarlas a una CloudFront distribución para replicar automáticamente el código en todo el mundo, sin aprovisionar ni administrar servidores. Esto reduce la latencia y mejora la experiencia del usuario.

Código

El siguiente código de ejemplo proporciona un plan para modificar los encabezados de CloudFront respuesta. Siga las instrucciones de la sección Epics para implementar el código.

```
exports.handler = async (event, context) => {
    const response = event.Records[0].cf.response;
    const headers = response.headers;


    const headerNameSrc = 'content-security-policy';
    const headerNameValue = '*.xyz.com';


    if (headers[headerNameSrc.toLowerCase()]) {
        headers[headerNameSrc.toLowerCase()] = [{
            key: headerNameSrc,
            value: headerNameValue,
        }];
        console.log(`Response header "${headerNameSrc}" was set to ` +
                    `"${headers[headerNameSrc.toLowerCase()][0].value}"`);
    }
    else {
            headers[headerNameSrc.toLowerCase()] = [{
            key: headerNameSrc,
            value: headerNameValue,
            }];
    }
    return response;
};
```

Epics

Crear una distribución

Tarea	Descripción	Habilidades requeridas
Cree una distribución CloudFront web.	En este paso, crea una CloudFront distribución para indicar desde CloudFront dónde quiere que se entregue el contenido y los detalles sobre cómo realizar el seguimiento y gestionar la entrega del contenido.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	Para crear una distribución mediante la consola, inicie sesión en la consola de administración de AWS, abra la CloudFront consola y, a continuación, siga los pasos de la CloudFront documentación.	

Creación e implementación de la funcion Lambda@Edge

Tarea	Descripción	Habilidades requeridas
Crear e implementar la funcion Lambda@Edge.	Puede crear una función Lambda @Edge mediante un esquema para modificar CloudFront los encabezados de respuesta. (Hay otros blueprints disponibles para diferentes casos de uso; para obtener más información, consulte las funciones de ejemplo de Lambda @Edge en CloudFront la documentación). Para crear una función de Lambda@Edge: 1. Inicie sesión en la consola de administración de AWS y abra la consola de AWS Lambda en https://console.aws.amazon.com/lambda/.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	2. Asegúrese de estar en la región EE.UU. Este (Norte de Virginia). CloudFront los planos solo están disponibles en esta región. 3. Elija Crear función. 4. Seleccione Usar un esquema y, a continuación, introduzca cloudfront en el campo de búsqueda Esquemas. 5. Elija el cloudfront-modify-response-headerplano y, a continuación, elija Configurar. 6. En la página Información básica, facilite la siguiente información: a. Escriba un nombre de función. b. Para Execution Role (Rol de ejecución), elija Create a new role from AWS policy templates (Crear un rol a partir de las plantillas de políticas de AWS). c. Asocie el nombre del rol de AWS Identity and Access Management (IAM) correspondiente. 7. Elija Crear función.	

Tarea	Descripción	Habilidades requeridas
	8. En la sección Diseñador de la página, elija el nombre de la función. 9. En la sección Código de función, sustituya el código de plantilla por el código de muestra proporcio nado anteriormente en este patrón, en la sección Código. 10. En el código de muestra, reemplace `xyz.com` por el nombre de su dominio. 11. Seleccione Guardar.	
Implemente la función de Lambda@Edge.	Siga las instrucciones del paso 4 del tutorial: Creación de una función Lambda @Edge sencilla de la CloudFront documentación de Amazon para configura r el CloudFront activador e implementar la función.	Administrador de AWS

Recursos relacionados

CloudFront documentación

- Comportamiento de solicitudes y respuestas para orígenes personalizados
- Trabajo con distribuciones
- Funciones de ejemplo de Lambda@Edge
- Personalización en la periferia con Lambda@Edge
- Tutorial: Creación de una función de Lambda@Edge sencilla

Acceda de forma privada a un punto de conexión de servicio central de AWS desde varias VPC

Creado por Martin Guenthner (AWS) y Samuel Gordon (AWS)

Repositorio de código: VPC Endpoint Sharing	Entorno: producción	Tecnologías: redes; infraestructura
Servicios de AWS: AWS RAM; Amazon Route 53; Amazon SNS; AWS Transit Gateway; Amazon VPC		

Resumen

Los requisitos de seguridad y conformidad de su entorno pueden especificar que el tráfico a los servicios o puntos de conexión de Amazon Web Services (AWS) no debe atravesar la Internet pública. Este patrón es una solución diseñada para una hub-and-spoketopología en la que una VPC de hub central está conectada a varias VPC de radios distribuidos. En esta solución, utiliza AWS PrivateLink para crear un punto de enlace de VPC de interfaz para el servicio de AWS en la cuenta hub. A continuación, utiliza puertas de enlace y una regla de sistema de nombres de dominio (DNS) distribuido para resolver las solicitudes a la dirección IP privada del punto de conexión en todas las VPC conectadas.

Este patrón describe cómo usar AWS Transit Gateway, un punto de conexión entrante de Amazon Route 53 Resolver y una regla de reenvío de Route 53 compartida para resolver las consultas de DNS de los recursos de las VPC conectadas. El punto de conexión, la puerta de enlace, Resolver y la regla de reenvío se crean en la cuenta central. A continuación, debe utilizar AWS Resource Access Manager (AWS RAM) para compartir la puerta de enlace y la regla de reenvío con las VPC radiales. CloudFormation Las plantillas de AWS proporcionadas le ayudan a implementar y configurar los recursos en las VPC centrales y en las VPC radiales.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta central y una o más cuentas radiales, administradas en la misma organización en AWS Organizations. Para obtener más información, consulte Creación y administración de una organización.
- AWS Resource Access Manager (AWS RAM) se ha configurado como un servicio de confianza en AWS Organizations. Para obtener más información, consulte Uso de AWS Organizations con otros servicios de AWS.
- La resolución de DNS debe estar habilitada en las VPC centrales y radiales. Para más información, consulte la atributos DNS para su VPC (documentación de Amazon Virtual Private Cloud).

Limitaciones

- Este patrón conecta las cuentas centrales y radiales en la misma región de AWS. Para las implementaciones en varias regiones, debe repetir este patrón para cada región.
- El servicio de AWS debe integrarse PrivateLink como punto final de la VPC como interfaz. Para obtener una lista completa, consulte los servicios de AWS que se integran con AWS PrivateLink (PrivateLink documentación).
- No se garantiza la afinidad entre zonas de disponibilidad. Por ejemplo, las consultas de la zona de disponibilidad A pueden responder con una dirección IP de la zona de disponibilidad B.
- La interfaz de red elástica asociada al punto final de la VPC tiene un límite de 10 000 consultas por segundo.

Arquitectura

Pila de tecnología de destino

- Una VPC central en la cuenta de AWS central
- Una o más VPC radiales en una cuenta de AWS radial
- Uno o más puntos de conexión de interfaz de la VPC en la cuenta central
- Resolvers de Route 53 entrantes y salientes en la cuenta central
- Una regla de reenvío de Route 53 Resolver implementada en la cuenta central y compartida con la cuenta radial
- Una puerta de enlace implementada en la cuenta central y compartida con la cuenta radial
- AWS Transit Gateway que conecta las VPC centrales y radiales

Arquitectura de destino

En la siguiente imagen se muestra un ejemplo de arquitectura para esta solución. En esta arquitectura, la regla de reenvío del Route 53 Resolver de la cuenta central tiene la siguiente relación con los demás componentes de la arquitectura:

1. La regla de reenvío se comparte con la VPC radial mediante la RAM de AWS.
2. La regla de reenvío está asociada al Resolver saliente en la VPC central.
3. La regla de reenvío se dirige al Resolver entrante en la VPC central.

En la siguiente imagen se muestra el flujo de tráfico a través de la arquitectura de muestra:

1. Un recurso, como una instancia de Amazon Elastic Compute Cloud (Amazon EC2), en la VPC radial, realiza una solicitud de DNS a `<service>.<region>.amazonaws.com`. La solicitud es recibida por la Amazon DNS Resolver radial.
2. La regla de reenvío de Route 53, que se comparte desde la cuenta central y se asocia a la VPC radial, intercepta la solicitud.
3. En la VPC central, el Resolver saliente usa la regla de reenvío para reenviar la solicitud al Resolver entrante.
4. El Resolver entrante utiliza el Resolver de Amazon DNS de la VPC central para resolver la dirección IP de `<service>.<region>.amazonaws.com` para la dirección IP privada de un punto de conexión de VPC. Si no hay un punto de conexión de VPC, se resuelve en la dirección IP pública.

Herramientas

Herramientas y servicios de AWS

- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.

- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Resource Access Manager (AWS RAM) le ayuda a compartir sus recursos de forma segura entre las cuentas de AWS para reducir los gastos operativos y brindar visibilidad y auditabilidad.
- Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad.
- AWS Systems Manager le permite administrar las aplicaciones y la infraestructura que se ejecutan en la nube de AWS. Simplifica la administración de aplicaciones y recursos, reduce el tiempo requerido para detectar y resolver problemas operativos y ayuda a utilizar y administrar los recursos de AWS a escala de manera segura.
- AWS Transit Gateway es un concentrador central que conecta las VPC y las redes en las instalaciones.
- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esta red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Otras herramientas y servicios

- nslookup es una herramienta de línea de comandos que se utiliza para consultar registros DNS. En este patrón, se utiliza esta herramienta para probar la solución.

Repositorio de código

El código de este patrón está disponible en GitHub, en el vpc-endpoint-sharingrepositorio. Este patrón proporciona dos CloudFormation plantillas de AWS:

- Una plantilla para implementar los siguientes recursos en la cuenta central:
  - `rSecurityGroupEndpoints`: el grupo de seguridad que controla el acceso al punto de conexión de VPC.
  - `rSecurityGroupResolvers`: el grupo de seguridad que controla el acceso al Resolver de Route 53.
  - `rKMSEndpoint`, `rSSMMessagesEndpoint`, `rSSMEndpoint` y `rEC2MessagesEndpoint`: ejemplos de puntos de conexión de VPC de interfaz en la cuenta central. Personalice estos punto de conexión para su caso de uso.

  - `rInboundResolver`:un Resolver de Route 53 que resuelve las consultas de DNS en el Resolver de Amazon DNS central.
  - `rOutboundResolver`: un Resolver de Route 53 saliente que reenvía las consultas al Resolver entrante.
  - `rAWSApiResolverRule`: la regla de reenvío de Resolver de Route 53 que se comparte con todas las VPC radiales.
  - `rRamShareAWSResolverRule`: el recurso compartido de RAM de AWS que permite a las VPC radiales utilizar la regla de reenvío `rAWSApiResolverRule`.
  - *`rVPC`: la VPC central, utilizada para modelar los servicios compartidos.
  - *`rSubnet1`: una subred privada que se utiliza para alojar los recursos centrales.
  - *`rRouteTable1`: la tabla de enrutamiento de la VPC central.
  - *`rRouteTableAssociation1`: para la tabla de enrutamiento `rRouteTable1` de la VPC central, la asociación de la subred privada.
  - *`rRouteSpoke`: la ruta desde la VPC central a la VPC radial.
  - *`rTgw`: la puerta de enlace que se comparte con todas las VPC radiales.
  - *`rTgwAttach`: la conexión que permite a la VPC central enrutar el tráfico a la puerta de enlace `rTgw`.
  - *`rTgwShare`: el recurso compartido de RAM de AWS que permite a las cuentas radiales utilizar la puerta de enlace `rTgw`.
- Una plantilla para implementar los siguientes recursos en las cuentas centrales:
  - `rAWSApiResolverRuleAssociation`: una asociación que permite a la VPC radial utilizar la regla de reenvío compartido en la cuenta central.
  - *`rVPC`: la VPC radial.
  - *`rSubnet1, rSubnet2, rSubnet3`: una subred para cada zona de disponibilidad, que se utiliza para alojar los recursos privados radiales.
  - *`rTgwAttach`: la conexión que permite a la VPC central enrutar el tráfico a la puerta de enlace de tránsito `rTgw`.
  - *`rRouteTable1`: la tabla de enrutamiento de la VPC central.
  - *`rRouteEndpoints`: la ruta desde los recursos de la VPC radial hasta la puerta de enlace de tránsito.
  - *`rRouteTableAssociation1/2/3`: para la tabla de enrutamiento `rRouteTable1` de la VPC central, las asociaciones de las subredes privadas.

- *`rInstanceRole`: el rol de IAM utilizado para probar la solución.
- *`rInstancePolicy`: la política de IAM utilizada para probar la solución.
- *`rInstanceSg`: el grupo de seguridad utilizado para probar la solución.
- *`rInstanceProfile`: el perfil de instancia de IAM utilizado para probar la solución.
- *`rInstance`: una instancia EC2 preconfigurada para el acceso a través de AWS Systems Manager. Utilice esta instancia para probar la solución.

* Estos recursos son compatibles con la arquitectura de muestra y es posible que no sean necesarios al implementar este patrón en una zona de aterrizaje existente.

Epics

Prepare las CloudFormation plantillas

Tarea	Descripción	Habilidades requeridas
Clone el repositorio de código.	1. En una interfaz de la línea de comandos, cambie el directorio de trabajo a la ubicación en la que desee almacenar los archivos de muestra. 2. Escriba el siguiente comando: `git clone https://github.com/aws-samples/vpc-endpoint-sharing.git`	Administrador de redes, arquitecto de la nube
Modifique las plantillas.	1. En el repositorio clonado, abra los archivos hub.yml y spoke.yml. 2. Revise los recursos creados por estas plantillas y ajuste las plantillas	Administrador de redes, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	según sea necesario para su entorno. Para obtener una lista completa, consulte la sección Repositorio de código en Herramientas. Si sus cuentas ya tienen algunos de estos recursos, elimínelos de la CloudFormation plantilla. Para obtener más información, consulte Trabajar con plantillas (CloudFormation documentación). 3. Guarde y cierre los archivos hub.yml y spoke.yml.	

Implemente los recursos en las cuentas de destino

Tarea	Descripción	Habilidades requeridas
Implementación de recursos centrales.	Con la plantilla hub.yml, crea una pila. CloudFormation Cuando se le indique, proporcione los valores de los parámetros de la plantilla .. Para obtener más información, consulte Creación de una pila (documentación)CloudFormation .	Arquitecto de la nube, administrador de redes
Implemente los recursos radiales.	Con la plantilla spoke.yml , cree una pila. CloudFormation Cuando se le indique, proporcione los valores de	Arquitecto de la nube, administrador de redes

Tarea	Descripción	Habilidades requeridas
	los parámetros de la plantilla.. Para obtener más información, consulte Creación de una pila (documentación). CloudFormation	

Pruebe la solución

Tarea	Descripción	Habilidades requeridas
Pruebe las consultas de DNS privadas en el servicio de AWS.	1. Conéctese a la instancia EC2 `rInstance` mediante Session Manager, una funcionalidad de AWS Systems Manager. Para obtener más información, consulte Conexión a la instancia de Linux mediante Session Manager (documentación de Amazon EC2). 2. En el caso de un servicio de AWS que tenga un punto de conexión de VPC en la cuenta central, utilice `nslookup` para confirmar que se devuelven las direcciones IP privadas del Resolver de Route 53 entrante. A continuación, se muestra un ejemplo de uso de `nslookup` para obtener	Administrador de red

Tarea	Descripción	Habilidades requeridas
	acceso a un punto de conexión de Amazon Systems Manager. `nslookup ssm.<region>.amazonaws.com` 3. En la Interfaz de la línea de comandos de AWS (CLI de AWS), introduzc a un comando que pueda ayudarlo a confirmar que los cambios no afectaron a la funcionalidad del servicio. Para obtener una lista de los comandos, consulte Referencia de comandos de la CLI de AWS. Por ejemplo, el siguiente comando debería mostrar una lista de documentos de Amazon Systems Manager. `aws ssm list-documents`	

Tarea	Descripción	Habilidades requeridas
Pruebe las consultas de DNS públicas en un servicio de AWS.	1. En el caso de un servicio de AWS que no tenga un punto de conexión de VPC en la cuenta central, utilice `nslookup` para confirmar que se devuelven las direcciones IP públicas. A continuación, se muestra un ejemplo de uso de `nslookup` para obtener acceso a un punto de conexión de Amazon Simple Notification Service (Amazon SNS). `nslookup sns.<region>.amazonaws.com` 2. En la CLI de AWS, introduzca un comando que pueda ayudarlo a confirmar que los cambios no afectaron a la funcionalidad del servicio. Para obtener una lista de los comandos, consulte Referencia de comandos de la CLI de AWS. Por ejemplo, si hay algún tema de Amazon SNS en la cuenta central, el siguiente comando debería devolver una lista de temas.	Administrador de red

Tarea	Descripción	Habilidades requeridas
	`aws sns list-topics`	

Recursos relacionados

- Creación de una infraestructura de red de AWS multiVPC escalable y segura (documento técnico de AWS)
- Trabajar con recursos compartidos (documentación de RAM de AWS)
- Cómo trabajar con puertas de enlace de tránsito (documentación de AWS Transit Gateway)

Crear un informe con los resultados del Analizador de acceso a la red sobre el acceso entrante a Internet en varias cuentas de AWS

Creado por Mike Virgilio (AWS)

Repositorio de código: Análisis de cuentas múltiples de Network Access Analyzer	Entorno: producción	Tecnologías: redes, seguridad, identidad, conformidad
Servicios de AWS: AWS CloudFormation; Amazon S3; Amazon VPC; AWS Security Hub		

Resumen

El acceso entrante no intencionado a los recursos de AWS a través de Internet puede suponer un riesgo para el perímetro de datos de una organización. El Analizador de acceso a la red es una característica de Amazon Virtual Private Cloud (Amazon VPC) que ayuda a identificar el acceso de red no deseado a sus recursos en Amazon Web Services (AWS). Puede utilizar el Analizador de acceso a la red para especificar sus requisitos de acceso a la red e identificar posibles rutas de red que no cumplan los requisitos especificados. Puede utilizar el Analizador de acceso a la red para hacer lo siguiente:

1. Identifique los recursos de AWS que son accesibles a Internet a través de las puertas de enlace de Internet.
2. Compruebe que sus nubes privadas virtuales (VPC) estén segmentadas adecuadamente, por ejemplo, aislando los entornos de producción y desarrollo y separando las cargas de trabajo transaccionales.

El analizador de acceso a la end-to-end red analiza las condiciones de accesibilidad de la red y no solo un componente. Para determinar si un recurso es accesible desde Internet, el Analizador de acceso a la red evalúa la puerta de enlace de Internet, las tablas de enrutamiento de VPC, las listas de control de acceso (ACL) a la red, las direcciones IP públicas en las interfaces de red elásticas y los grupos de seguridad. Si alguno de estos componentes impide el acceso a Internet, en Analizador

de acceso a la red no genera ningún resultado. Por ejemplo, si una instancia de Amazon Elastic Compute Cloud (Amazon EC2) tiene un grupo de seguridad abierto que permite el tráfico desde `0/0`, pero la instancia se encuentra en una subred privada que no se puede enrutar desde ninguna puerta de enlace de Internet, el Analizador de acceso a la red no generará ningún resultado. Esto proporciona resultados de alta fidelidad para que pueda identificar los recursos a los que realmente se puede acceder desde Internet.

Cuando ejecuta el Analizador de acceso a la red, utiliza los Ámbitos de acceso a la red para especificar sus requisitos de acceso a la red. Esta solución identifica las rutas de red entre una puerta de enlace de Internet y una interfaz de red elástica. En este patrón, usted implementa la solución en una cuenta de AWS centralizada en su organización, administrada por AWS Organizations, y esta analiza todas las cuentas de cualquier región de AWS de la organización.

Esta solución se diseñó teniendo en cuenta lo siguiente:

- CloudFormation Las plantillas de AWS reducen el esfuerzo necesario para implementar los recursos de AWS en este patrón.
- Puede ajustar los parámetros de las CloudFormation plantillas y del script naa-script.sh en el momento de la implementación para personalizarlos para su entorno.
- Los scripts de Bash aprovisionan y analizan automáticamente los alcances de acceso a la red para varias cuentas, en paralelo.
- Un script de Python procesa los resultados, extrae los datos y, a continuación, consolida los resultados. Puede optar por revisar el informe consolidado de los resultados del Analizador de acceso a la red en formato CSV o en AWS Security Hub. Un ejemplo del informe CSV está disponible en la sección de Información adicional de este patrón.
- Puede corregir los resultados o excluirlos de futuros análisis agregándolos al archivo naa-exclusions.csv.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS para alojar servicios y herramientas de seguridad, administrada como una cuenta de miembro de una organización en AWS Organizations. En este patrón, esta cuenta se denomina cuenta de seguridad.
- En la cuenta de seguridad, debe tener una subred privada con acceso saliente a Internet. Para obtener instrucciones, consulte Crear una subred en la documentación de Amazon VPC. Puede

establecer el acceso a Internet mediante una puerta de enlace NAT o un punto de conexión de VPC de interfaz.

- Acceso a la cuenta de administración de AWS Organizations o a una cuenta para CloudFormation la que se hayan delegado permisos de administrador. Para obtener instrucciones, consulte Registrar un administrador delegado en la CloudFormation documentación.
- Habilite un acceso confiable entre AWS Organizations y CloudFormation. Para obtener instrucciones, consulte Habilitar el acceso de confianza con AWS Organizations en la CloudFormation documentación.
- Si va a subir los resultados a Security Hub, Security Hub debe estar habilitado en la cuenta y la región de AWS en las que se aprovisiona la instancia EC2. Para obtener más información, consulte Configuración de AWS Security Hub.

Limitaciones

- Las rutas de red entre cuentas no se analizan actualmente debido a las limitaciones de las característica del Analizador de acceso a la red.
- Las cuentas de AWS de destino deben administrarse como una organización en AWS Organizations. Si no utiliza AWS Organizations, puede actualizar la CloudFormation plantilla naa-execrole.yaml y el script naa-script.sh para su entorno. En su lugar, usted proporciona una lista de las regiones y los ID de las cuentas de AWS en las que desea ejecutar el script.
- La CloudFormation plantilla está diseñada para implementar la instancia EC2 en una subred privada con acceso saliente a Internet. AWS Systems Manager Agent (SSM Agent) requiere acceso saliente para llegar al punto de conexión del servicio Systems Manager, y usted necesita acceso saliente para clonar el repositorio de código e instalar las dependencias. Si desea utilizar una subred pública, debe modificar la plantilla naa-resources.yaml para asociar una Dirección IP elástica a la instancia EC2.

Arquitectura

Pila de tecnología de destino

- Analizador de acceso a la red
- Instancia de Amazon EC2
- Roles de AWS Identity and Access Management (IAM)
- Bucket de Amazon Simple Storage Service (Amazon S3)

- Tema de Amazon Simple Notification Service (Amazon SNS)
- AWS Security Hub (solo opción 2)

Arquitectura de destino

Opción 1: Acceder a los resultados de un bucket de Amazon S3

El diagrama muestra el proceso siguiente:

1. Si ejecuta la solución manualmente, el usuario se autentica en la instancia EC2 mediante Session Manager y, a continuación, ejecuta el script naa-script.sh. Este script del intérprete de comandos lleva a cabo los pasos del 2 al 7.

   Si ejecuta la solución automáticamente, el script naa-script.sh se iniciará automáticamente según la programación que haya definido en la expresión cron. Este script del intérprete de comandos lleva a cabo los pasos del 2 al 7. Para obtener más información, consulte Automatizar y escalar al final de esta sección.
2. La instancia EC2 descarga el archivo naa-exception.csv más reciente del bucket de S3. Este archivo se utiliza más adelante en el proceso, cuando el Script de Python procesa las exclusiones.
3. La instancia EC2 asume el rol de IAM de `NAAEC2Role`, que concede permisos para acceder al bucket de S3 y para asumir los roles de IAM de `NAAExecRole` en las demás cuentas de la organización.
4. La instancia EC2 asume el rol de IAM de `NAAExecRole` en la cuenta de administración de la organización y genera una lista de las cuentas de la organización.
5. La instancia EC2 asume el rol de IAM `NAAExecRole` en las cuentas de los miembros de la organización (denominadas cuentas de carga de trabajo en el diagrama de arquitectura) y realiza una evaluación de seguridad en cada cuenta. Los resultados se almacenan como archivos JSON en la instancia EC2.
6. La instancia EC2 utiliza un script de Python para procesar los archivos JSON, extraer los campos de datos y crear un informe CSV.
7. La instancia EC2 carga el archivo CSV en el bucket de S3.
8. Una EventBridge regla de Amazon detecta la carga del archivo y utiliza un tema de Amazon SNS para enviar un correo electrónico en el que se notifica al usuario que el informe está completo.

9. El usuario descarga el archivo CSV del bucket de S3. El usuario importa los resultados a la plantilla de Excel y revisa los resultados.

Opción 2: Acceder a los resultados en AWS Security Hub

El diagrama muestra el proceso siguiente:

1. Si ejecuta la solución manualmente, el usuario se autentica en la instancia EC2 mediante Session Manager y, a continuación, ejecuta el script naa-script.sh. Este script del intérprete de comandos lleva a cabo los pasos del 2 al 7.

   Si ejecuta la solución automáticamente, el script naa-script.sh se iniciará automáticamente según la programación que haya definido en la expresión cron. Este script del intérprete de comandos lleva a cabo los pasos del 2 al 7. Para obtener más información, consulte Automatizar y escalar al final de esta sección.
2. La instancia EC2 descarga el archivo naa-exception.csv más reciente del bucket de S3. Este archivo se utiliza más adelante en el proceso, cuando el Script de Python procesa las exclusiones.
3. La instancia EC2 asume el rol de IAM de `NAAEC2Role`, que concede permisos para acceder al bucket de S3 y para asumir los roles de IAM de `NAAExecRole` en las demás cuentas de la organización.
4. La instancia EC2 asume el rol de IAM de `NAAExecRole` en la cuenta de administración de la organización y genera una lista de las cuentas de la organización.
5. La instancia EC2 asume el rol de IAM `NAAExecRole` en las cuentas de los miembros de la organización (denominadas cuentas de carga de trabajo en el diagrama de arquitectura) y realiza una evaluación de seguridad en cada cuenta. Los resultados se almacenan como archivos JSON en la instancia EC2.
6. La instancia EC2 utiliza un script de Python para procesar los archivos JSON y extraer los campos de datos para importarlos a Security Hub.
7. La instancia EC2 importa los resultados del Analizador de acceso a la red a Security Hub.
8. Una EventBridge regla de Amazon detecta la importación y utiliza un tema de Amazon SNS para enviar un correo electrónico en el que se notifica al usuario que el proceso se ha completado.
9. El usuario ve los resultados en Security Hub.

Automatizar y escalar

Puede programar esta solución para que ejecute el script naa-script.sh automáticamente según una programación personalizada. Para establecer una programación personalizada, modifique el parámetro en la plantilla naa-resources.yaml. CloudFormation `CronScheduleExpression` Por ejemplo, el valor predeterminado de `0 0 * * 0` ejecuta la solución todos los domingos a medianoche. Un valor de `0 0 * 1-12 0` ejecutaría la solución a medianoche del primer domingo de cada mes. Para obtener más información sobre el uso de expresiones cron, consulte Expresiones cron y de frecuencia en la documentación de Systems Manager.

Si desea ajustar la programación una vez implementada la pila `NAA-Resources`, puede editarla manualmente en `/etc/cron.d/naa-schedule`.

Herramientas

Servicios de AWS

- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, las funciones de Lambda de AWS, los puntos de conexión de invocación HTTP que utilizan destinos de API o los buses de eventos de otras cuentas de AWS.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Organizations es un servicio de administración de cuentas que le permite agrupar varias cuentas de AWS en una organización que usted crea y administra de manera centralizada.
- AWS Security Hub proporciona una visión completa de su estado de seguridad en AWS. También le permite comprobar si su entorno de AWS cumple con los estándares y las prácticas recomendadas del sector de seguridad.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Systems Manager le permite administrar las aplicaciones y la infraestructura que se ejecutan en la nube de AWS. Simplifica la administración de aplicaciones y recursos, reduce el tiempo

requerido para detectar y resolver problemas operativos y ayuda a utilizar y administrar los recursos de AWS a escala de manera segura. Este patrón utiliza Session Manager, una capacidad de Systems Manager.

Repositorio de código

El código de este patrón está disponible en el repositorio de análisis de cuentas múltiples de GitHub Network Access Analyzer. El repositorio de código contiene los siguientes archivos:

- naa-script.sh – Este bash script se utiliza para iniciar un análisis del Analizador de acceso a la red de varias cuentas de AWS, en paralelo. Como se define en la CloudFormation plantilla naa-resources.yaml, este script se implementa automáticamente en la carpeta de la instancia EC2. `/usr/local/naa`
- naa-resources.yaml: usa esta CloudFormation plantilla para crear una pila en la cuenta de seguridad de la organización. Esta plantilla implementa todos los recursos necesarios para esta cuenta a fin de respaldar la solución. Esta pila debe implementarse antes que la plantilla naa-execrole.yaml.

  Nota: Si esta pila se elimina y se vuelve a implementar, debe volver a crear el conjunto de pilas `NAAExecRole` para recuperar las dependencias entre cuentas entre los roles de IAM.

- naa-execrole.yaml: usa esta CloudFormation plantilla para crear un conjunto de pilas que despliegue la función de IAM en todas las cuentas de la organización, incluida la cuenta de administración. `NAAExecRole`
- naa-processfindings.py – El script naa-script.sh llama automáticamente a este script de Python para procesar las salidas JSON del Analizador de acceso a la red, excluir cualquier recurso de funcionalidad comprobada en el archivo naa-exclusions.csv y, a continuación, generar un archivo CSV con los resultados consolidados o importar los resultados a Security Hub.

Epics

Preparación para la implementación

Tarea	Descripción	Habilidades requeridas
Clone el repositorio de código.	1. En una interfaz de la línea de comandos, cambie el directorio de trabajo a la ubicación en la que desee almacenar los archivos de muestra. 2. Escriba el siguiente comando. `git clone https://github.com/aws-samples/network-access-analyzer-multi-account-analysis.git`	AWS DevOps
Revise las plantillas.	1. En el repositorio clonado, abra los archivos naa-resources.yaml y naa-execrole.yaml. 2. Revise los recursos creados por estas plantillas y ajuste las plantillas según sea necesario para su entorno. Para obtener más información, consulte Trabajar con plantillas en la CloudFormation documentación.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	3. Guarde y cierre los archivos naa-resources.yaml y naa-execrole.yaml.	

Crea las CloudFormation pilas

Tarea	Descripción	Habilidades requeridas
Aprovisione recursos en la cuenta de seguridad.	Con la plantilla naa-resources.yaml, se crea una CloudFormation pila que despliega todos los recursos necesarios en la cuenta de seguridad. Para obtener instrucciones, consulta Cómo crear una pila en la documentación. CloudFormation Tenga en cuenta lo siguiente al implementar esta plantilla: 1. En la página Especificar plantilla, seleccione la Plantilla está lista y, a continuación, cargue el archivo naa-resources.yaml . 2. En la página Especificar detalles de pila, en Nombre de la pila, introduzca `NAA-Resources` . 3. En la sección Parámetros, introduzca lo siguiente:	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	• `VPCId`: seleccione una VPC en la cuenta. • `SubnetId`: seleccione una subred privada que tenga acceso a Internet. Nota: Si selecciona una subred pública, es posible que a la instancia EC2 no se le asigne una dirección IP pública porque la CloudForm ation plantilla, de forma predeterminada, no aprovisiona ni adjunta una dirección IP elástica. • `InstanceType` —– Deje el tipo de instancia predeterminado. • `InstanceImageId` : deje el valor predeterm inado. • `KeyPairName` : si utiliza SSH para acceder, especifique el nombre de un par de claves existente. • `PermittedSSHInboun d` : si utiliza SSH para el acceso, especifiq ue un bloque CIDR permitido. Si no utiliza SSH, mantenga el valor	

Tarea	Descripción	Habilidades requeridas
	predeterminado de `127.0.0.1` . • `BucketName` : El valor predeterminado es `naa-<accountID>-<region>` . Puede modificarlo según sea necesario. Si especifica un valor personalizado, el ID de cuenta y la región se añaden automátic amente al valor especific ado. • `EmailAddress` —– Especifique una dirección de correo electrónico para una notificación de Amazon SNS cuando se complete el análisis. Nota: La configura ción de la suscripción a Amazon SNS debe confirmarse antes de completar el análisis o no se enviará ninguna notificación. • `NAAEC2Role` : mantenga el nombre predeterminado a menos que sus convenciones de nomenclatura requieran un nombre diferente para este rol de IAM.	

Tarea	Descripción	Habilidades requeridas
	• `NAAExecRole` —– Mantenga el nombre predeterminado a menos que se utilice otro nombre al implementar naa-execrole.yaml • `Parallelism` : especifique el número de evaluaciones paralelas que se van a realizar. • `Regions` –– Especifique las regiones de AWS que desea analizar. • `ScopeNameValue` —– Especifique la etiqueta que se asignará al ámbito. Esta etiqueta se utiliza para determinar el alcance de acceso a la red. • `ExclusionFile` —– Especifique el nombre del archivo de exclusión . Las entradas de este archivo se excluirán de los resultados. • `FindingsToCSV` – Especifique si los resultados deben enviarse a CSV. Los valores aceptados son: `true` y `false`.	

Tarea	Descripción	Habilidades requeridas
	• `FindingsToSecurityHub` – Especifique si los resultados deben importarse a Security Hub. Los valores aceptados son: `true` y `false`. • `EmailNotificationsForSecurityHub` – Especifique si la importación de los resultados a Security Hub debe generar notificaciones por correo electrónico. Los valores aceptados son: `true` y `false`. • `ScheduledAnalysis` –– Si desea que la solución se ejecute automáticamente según una programación, introduzca `true` y, a continuación, personalice la programación en el parámetro `CronScheduleExpression`. Si no desea ejecutar la solución automáticamente, introduzca `false`. • `CronScheduleExpression` –– Si ejecuta la solución automátic	

Tarea	Descripción	Habilidades requeridas
	amente, introduzca una expresión cron para definir la programac ión. Para obtener más información, consulte Automatizar y escalar en la sección Arquitectura de este patrón. 1. En la página de revisión, seleccione Los siguiente s recursos requieren capacidades: [AWS::IAM ::Role] y, a continuación, elija Create Stack. 2. Una vez que la pila se haya creado correctamente, en la CloudFormation consola, en la pestaña Outputs, copia el `NAAEC2Role` Amazon Resource Name (ARN). Este ARN se utiliza más adelante al implementar el archivo naa-execrole.yaml.	

Tarea	Descripción	Habilidades requeridas
Facilitar el rol de IAM en las cuentas de los miembros.	En la cuenta de administración de AWS Organizations o en una cuenta con permisos de administrador delegados CloudFormation, utilice la plantilla naa-execrole.yaml para crear un conjunto de pilas. CloudFormation El conjunto de pilas implementa el rol de IAM de `NAAExecRole` para todas las cuentas de miembros de la organización. Para obtener instrucciones, consulte Crear un conjunto de pilas con permisos administrados por el servicio en la documentación. CloudFormation Tenga en cuenta lo siguiente al implementar esta plantilla: 1. En Preparación de la plantilla, seleccione La plantilla está lista y, a continuación, cargue el archivo naa-execrole.yaml. 2. En la página Especificar StackSet detalles, asigne un nombre al conjunto de pilas. `NAA-ExecRole` 3. En la sección Parámetros, introduzca lo siguiente: • `AuthorizedARN` : introduzca el ARN de	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`NAAEC2Role` que copió al crear la pila de `NAA-Resources`. • `NAARoleName` —— Mantenga el valor predeterminado de `NAAExecRole` a menos que se haya utilizado otro nombre al implementar el archivo naa-resources.yaml. 4. En Permisos, seleccione Permisos administrados por servicios. 5. En la página Cómo establecer opciones de implementación, en Destinos de implementación, seleccione Implementación en organización y acepte todos los parámetros predeterminados. Nota: Si quiere que las pilas se implementen en todas las cuentas de los miembros de forma simultánea, establezca un valor alto en el Número máximo de cuentas simultáneas y en la Tolerancia a errores, por ejemplo 100.	

Tarea	Descripción	Habilidades requeridas
	6. En Regiones de implementación, seleccione la región en la que está implementada la instancia EC2 del Analizador de acceso a la red. Como los recursos de IAM son globales y no regionales, se implementa el rol de IAM en todas las regiones activas. 7. En la página de revisión, seleccione Acepto que AWS CloudFormation podría crear recursos de IAM con nombres personalizados y, a continuación, elija Crear StackSet. 8. Supervise la pestaña Instancias de pila (para ver el estado de las cuentas individuales) y la pestaña Operaciones (para ver el estado general) para determinar cuándo se ha completado la implementación.	

Tarea	Descripción	Habilidades requeridas
Facilite el rol de IAM en la cuenta de administración.	Con la plantilla naa-execrole.yaml, se crea una CloudFormation pila que implementa la función de `NAAExecRole` IAM en la cuenta de administración de la organización. El conjunto de pilas que creó anteriormente no implementa el rol de IAM en la cuenta de administración. Para obtener instrucciones, consulta Cómo crear una pila en la documentación. CloudFormation Tenga en cuenta lo siguiente al implementar esta plantilla: 1. En la página Especificar plantilla, seleccione La plantilla está lista y, a continuación, cargue el archivo naa-execrole.yaml. 2. En la página Especificar detalles de pila, en Nombre de la pila, introduzca `NAA-ExecRole` . 3. En la sección Parámetros, introduzca lo siguiente: • `AuthorizedARN` : introduzca el ARN de `NAAEC2Role` que copió al crear la pila de `NAA-Resources` .	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	• `NAARoleName` —— Mantenga el valor predeterminado de `NAAExecRole` a menos que se haya utilizado otro nombre al implement ar el archivo naa-resou rces.yaml. 4. En la página de revisión, seleccione Los siguiente s recursos requieren capacidades: [AWS::IAM ::Role] y, a continuación, elija Crear pila.	

Realice el análisis

Tarea	Descripción	Habilidades requeridas
Personalice el script del intérprete de comandos.	1. Inicie sesión en la cuenta de seguridad de la organización. 2. Con Session Manager, conéctese a la instancia EC2 de analizador de acceso a la red que aprovisionó anteriormente. Para obtener instrucciones, consulte Conexión a la instancia de Linux mediante Session Manager. Si no puede conectarse, consulte la sección de Solución de problemas de este patrón.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	3. Introduzca los siguientes comandos para abrir el archivo naa-script.sh para editarlo. `sudo -i` `cd /usr/local/naa` `vi naa-script.sh` 4. Revise y modifique los parámetros y variables ajustables de este script según sea necesario para su entorno. Para obtener más información sobre las opciones de personalización, consulte los comentarios al principio del script. Por ejemplo, en lugar de obtener una lista de todas las cuentas de los miembros de la organización desde la cuenta de administración, puede modificar el script para especificar los ID de las cuentas de AWS o las regiones de AWS que desea escanear, o puede hacer referencia a un archivo externo que contenga estos parámetros.	

Tarea	Descripción	Habilidades requeridas
	5. Guarde y cierre el archivo naa-script.sh.	

Tarea	Descripción	Habilidades requeridas
Analice las cuentas de destino.	1. Introduzca los comandos siguientes. Esto ejecuta el script naa-script.sh. `sudo -i` `cd /usr/local/naa` `screen` `./naa-script.sh` Tenga en cuenta lo siguiente: • El comando `screen` permite que el script continúe ejecutándose en caso de que se agote el tiempo de espera de la conexión o se pierda el acceso a la consola. • Cuando comience el escaneo, puede forzar la separación de la pantalla pulsando Ctrl+A D. La pantalla se separa y puede cerrar la conexión de la instancia mientras se realiza el análisis. • Para reanudar una sesión separada, conéctese a la instancia, introduzca `sudo -i` y, a continuación, introduzca `screen -r`. 2. Supervise el resultado en busca de errores para	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	asegurarse de que el script funciona correctamente. Para ver un ejemplo de producción, consulte la sección de Información adicional de este patrón. 3. Espere a que el análisis finalice. Si configuró las notificaciones por correo electrónico, recibirá un correo electrónico cuando los resultados se carguen en el bucket de S3 o se importen a Security Hub.	
Opción 1: Recupere los resultados del bucket de S3.	1. Descargue el archivo CSV del bucket `naa-<accountID>-<region>` . Para obtener instrucciones, consulte Descargar un objeto en la documentación de Amazon S3. 2. Elimine el archivo CSV del bucket de S3. Esta es una práctica recomendada para la optimización de costos. Para obtener instrucciones, consulte Eliminar objetos en la documentación de Amazon S3.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Opción 2: Revise los resultados en Security Hub.	1. Abra la consola de Security Hub en https://console.aws.amazon.com/securityhub/. 2. En el panel de navegación, seleccione Findings (Resultados). 3. Revise los resuñtados del Analizador de acceso a la red. Para obtener instrucciones, consulte Visualización de listas de resultados y detalles en la documentación de Security Hub. Nota: Para buscar resultados, añada un título que empiece por filtrar e introducir `Network Access Analyzer`.	AWS DevOps

Corregir y excluir los resultados

Tarea	Descripción	Habilidades requeridas
Corrija los resultados.	Corrija cualquier resultado que desee abordar. Para obtener más información y prácticas recomendadas sobre cómo crear un perímetro alrededor de sus identidades, recursos y redes de AWS, consulte Creación de un perímetro de	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	datos en AWS (documento técnico de AWS).	

Tarea	Descripción	Habilidades requeridas
Excluya los recursos con rutas de red de funcionalidad comprobada.	Si el Analizador de acceso a la red genera resultados sobre los recursos a los que se debería acceder desde Internet, puede agregar estos recursos a una lista de exclusión. La próxima vez que se ejecute el Analizador de acceso a la red, no generará ningún resultado para ese recurso. 1. Navegue hasta `/usr/local/naa` y, a continuación, abra el script naa-script.sh. Anote el valor de la variable `S3_EXCLUSION_FILE` . 2. Si el valor de la variable `S3_EXCLUSION_FILE` es `true`, descargue el archivo naa-exclusions.csv del bucket `naa-<accountID>-<region>` . Para obtener instrucciones, consulte Descargar un objeto en la documentación de Amazon S3. Si el valor de la variable `S3_EXCLUSION_FILE` es `false`, navegue hasta `/usr/local/naa` y, a continuación, abra el archivo naa-exclusions.csv.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	Nota: Si el valor de la variable `S3_EXCLUSION_FILE` es `false`, el script utiliza una versión local del archivo de exclusiones. Si más adelante cambia el valor a `true`, el script sobrescribirá la versión local con el archivo del bucket de S3. 3. En el archivo naa-exclusions.csv, introduzca los recursos que desee excluir. Introduzca un recurso en cada línea y utilice el siguiente formato. `<resource_id>,<secgroup_id>,<sgrule_cidr>,<sgrule_portrange>,<sgrule_protocol>` El siguiente es un recurso de ejemplo. `eni-1111aaaaa2222bbbb,sg-3333ccccc4444dddd,0.0.0.0/0,80 to 80,tcp` 4. Guarde y cierre el archivo naa-exclusions.csv. 5. Si descargó el archivo naa-exclusions.csv del bucket	

Tarea	Descripción	Habilidades requeridas
	de S3, cargue la nueva versión. Para más instrucciones, consulte Cargar objetos en la documentación de Amazon S3.	

(Opcional) Actualizar el script naa-script.sh

Tarea	Descripción	Habilidades requeridas
Actualice el script naa-script.sh.	Si quiere actualizar el script naa-script.sh a la última versión del repositorio, haga lo siguiente: 1. Conectarse a la instancia de EC2 mediante Session Manager. Para obtener instrucciones, consulte Conexión a la instancia de Linux mediante Session Manager. 2. Introduzca el siguiente comando. `sudo -i` 3. Navegue hasta el directorio de scripts naa-script.sh. `cd /usr/local/naa` 4. Introduzca el siguiente comando para guardar el script local de forma	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	que pueda combinar los cambios personalizados en la versión más reciente. `git stash` 5. Introduzca el siguiente comando para obtener la versión más reciente del script. `git pull` 6. Introduzca el siguiente comando para combinar el script personalizado con la versión más reciente del script. `git stash pop`	

(Opcional) Limpieza

Tarea	Descripción	Habilidades requeridas
Elimine todos los recursos implementados.	Puede dejar los recursos implementados en las cuentas. Si desea desaprovisionar todos los recursos, haga lo siguiente: 1. Elimine la pila `NAA-ExecRole` aprovisionada en la cuenta de administración.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	Para obtener instrucciones, consulte Eliminar una pila en la CloudFormation documentación. 2. Elimine el conjunto de pilas `NAA-ExecRole` aprovisionado en la cuenta de administración de la organización o en la cuenta de administrador delegado. Para obtener instrucciones, consulte Eliminar un conjunto de pilas en la CloudFormation documentación. 3. Elimine todos los objetos del bucket de S3 `naa-<accountID>-<region>` . Para obtener instrucciones, consulte Eliminar objetos en la documentación de Amazon S3. 4. Elimine la pila `NAA-Resources` aprovisionada en la cuenta de seguridad . Para obtener instrucciones, consulte Eliminar una pila en la CloudFormation documentación.	

Solución de problemas

Problema	Solución
No se puede conectar a la instancia de EC2 mediante Session Manager.	El agente SSM debe poder comunicarse con el punto de conexión de Systems Manager. Haga lo siguiente: 1. Valide que la subred en la que se implement a la instancia EC2 tenga acceso a Internet. 2. Reinicie la instancia EC2.
Al implementar el conjunto de pilas, la CloudFormation consola le solicitará que lo haga`Enable trusted access with AWS Organizations to use service-managed permissions` .	Esto indica que no se ha habilitado el acceso de confianza entre AWS Organizations y CloudFormation. Se requiere acceso de confianza para implementar el conjunto de pilas gestionado por servicios. Seleccione el botón para activar el acceso de confianza. Para obtener más información, consulte Habilitar el acceso confiable en la CloudFormation documentación.

Recursos relacionados

- Nuevo – Analizador de acceso a la red de Amazon VPC (entrada del blog de AWS)
- AWS re:Inforce 2022 - Validar los controles efectivos de acceso a la red en AWS (NIS202) (video)
- Demostración - Análisis de la ruta de datos de ingreso a Internet en toda la organización mediante un Analizador de acceso a la red (video)

Información adicional

Ejemplo de salida de consola

En el siguiente ejemplo se muestra el resultado de generar la lista de cuentas de destino y analizar las cuentas de destino.

```
[root@ip-10-10-43-82 naa]# ./naa-script.sh
download: s3://naa-<account ID>-us-east-1/naa-exclusions.csv to ./naa-exclusions.csv

AWS Management Account: <Management account ID>

AWS Accounts being processed...
<Account ID 1> <Account ID 2> <Account ID 3>

Assessing AWS Account: <Account ID 1>, using Role: NAAExecRole
Assessing AWS Account: <Account ID 2>, using Role: NAAExecRole
Assessing AWS Account: <Account ID 3>, using Role: NAAExecRole
Processing account: <Account ID 1> / Region: us-east-1
Account: <Account ID 1> / Region: us-east-1 - Detecting Network Analyzer scope...
Processing account: <Account ID 2> / Region: us-east-1
Account: <Account ID 2> / Region: us-east-1 - Detecting Network Analyzer scope...
Processing account: <Account ID 3> / Region: us-east-1
Account: <Account ID 3> / Region: us-east-1 - Detecting Network Analyzer scope...
Account: <Account ID 1> / Region: us-east-1 - Network Access Analyzer scope detected.
Account: <Account ID 1> / Region: us-east-1 - Continuing analyses with Scope ID.
 Accounts with many resources may take up to one hour
Account: <Account ID 2> / Region: us-east-1 - Network Access Analyzer scope detected.
Account: <Account ID 2> / Region: us-east-1 - Continuing analyses with Scope ID.
 Accounts with many resources may take up to one hour
Account: <Account ID 3> / Region: us-east-1 - Network Access Analyzer scope detected.
Account: <Account ID 3> / Region: us-east-1 - Continuing analyses with Scope ID.
 Accounts with many resources may take up to one hour
```

Ejemplos de informes CSV

Las siguientes imágenes son ejemplos de la producción de CSV.

Etiquete automáticamente las conexiones de puerta de enlace de tránsito con AWS Organizations

Creado por Richard Milner-Watts (AWS), Haris Bin Ayub (AWS) y John Capps (AWS)

Repositorio de códigos: Transit Gateway Attachment Tagger	Entorno: producción	Tecnologías: redes, infraestructura; gestión y gobernanza; operaciones
Servicios de AWS: AWS Step Functions; AWS Transit Gateway; Amazon VPC; AWS Lambda		

Resumen

En Amazon Web Services (AWS), puede usar AWS Resource Access Manager para compartir AWS Transit Gateway entre los límites de las cuentas de AWS. Sin embargo, cuando crea conexiones de puerta de enlace de tránsito más allá de los límites de la cuenta, los archivos adjuntos se crean sin una etiqueta de nombre. Esto puede hacer que la identificación de los archivos adjuntos lleve mucho tiempo.

Esta solución proporciona un mecanismo automatizado para recopilar información sobre cada conexión de puerta de enlace de tránsito para las cuentas de una organización gestionada por AWS Organizations. El proceso incluye buscar el rango de enrutamiento entre dominios sin clase (CIDR) en la tabla de enrutamiento de puerta de enlace de tránsito. Luego, la solución aplica una etiqueta con el nombre en forma de `<CIDR-range>-<AccountName>` a la conexión de la cuenta que contiene la puerta de enlace de tránsito.

Esta solución se puede usar junto con una solución como Orquestador de red de tránsito sin servidor desde la Biblioteca de soluciones de AWS. El Orquestador de red de tránsito sin servidor permite la creación automática de conexiones de puerta de enlace de tránsito a escala.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una organización de AWS Organizations que contiene todas las cuentas relacionadas
- Acceso a la cuenta de gestión de la organización, en la raíz de la organización, para crear el rol de AWS Identity and Access Management (IAM) necesario
- Una cuenta de miembro de una red compartida que contiene una o más puertas de enlace de tránsito que se comparten con la organización y tienen archivos adjuntos

Arquitectura

La siguiente captura de pantalla de la consola de administración de AWS muestra ejemplos de conexiones de puerta de enlace de tránsito sin etiqueta de nombre asociada y dos conexiones de puerta de enlace de tránsito con etiquetas de nombre generados por esta solución. La estructura de la etiqueta de nombre generada es `<CIDR-range>-<AccountName>`.

Esta solución utiliza AWS CloudFormation para implementar un flujo de trabajo de AWS Step Functions que gestiona la creación de etiquetas de nombres de Transit Gateway en todas las regiones configuradas. El flujo de trabajo invoca las funciones de Lambda de AWS, que realizan las tareas subyacentes.

Una vez que la solución haya obtenido los nombres de las cuentas de AWS Organizations, el equipo de estados de Step Functions obtiene todos los identificadores de la conexión de puerta de enlace de tránsito. La región de AWS las procesa en paralelo. Este procesamiento incluye la búsqueda del rango de CIDR para cada archivo adjunto. El rango CIDR se obtiene buscando en las tablas de enrutamiento de puerta de enlace de tránsito de la región un identificador de la conexión de puerta de enlace de tránsito coincidente. Si toda la información requerida está disponible, la solución aplica una etiqueta con el nombre al archivo adjunto. La solución no sobrescribirá ninguna etiqueta de nombre existente.

La solución se ejecuta según un cronograma controlado por un EventBridge evento de Amazon. El evento inicia la solución todos los días a las 6:00 UTC.

Pila de tecnología de destino

- Amazon EventBridge
- AWS Lambda

- AWS Organizations
- AWS Transit Gateway
- Amazon Virtual Private Cloud (Amazon VPC)
- AWS X-Ray

Arquitectura de destino

La arquitectura de la solución y el flujo de trabajo se muestran en el siguiente diagrama.

1. El evento programado inicia la regla.
2. La EventBridge regla inicia la máquina de estados Step Functions.
3. La máquina de estados invoca la función de Lambda `tgw-tagger-organizations-account-query`.
4. La función de Lambda `tgw-tagger-organizations-account-query` asume la función en la cuenta de administración de la organización.
5. La función de Lambda `tgw-tagger-organizations-account-query` llama a la API Organizations para devolver los metadatos de las cuentas de AWS.
6. La máquina de estados invoca la función de Lambda `tgw-tagger-attachment-query`.
7. Para cada región, en paralelo, la máquina de estados invoca la función de Lambda `tgw-tagger-rtb-query` para leer el rango CIDR de cada adjunto.
8. Para cada región, en paralelo, la máquina de estados invoca la función de Lambda para `tgw-tagger-attachment-tagger`
9. Las etiquetas de nombre se crean para las conexiones de puerta de enlace de tránsito en la cuenta Shared Networking.

Automatizar y escalar

La solución procesa cada región en paralelo para reducir la duración total de la ejecución.

Herramientas

Servicios de AWS

- AWS CloudFormation: AWS CloudFormation proporciona una forma de modelar un conjunto de recursos relacionados de AWS y de terceros, aprovisionarlos de forma rápida y coherente y gestionarlos a lo largo de sus ciclos de vida, tratando la infraestructura como código.
- Amazon EventBridge: Amazon EventBridge es un servicio de bus de eventos sin servidor que puede utilizar para conectar sus aplicaciones con datos de diversas fuentes. EventBridge recibe un evento, un indicador de un cambio en el entorno, y aplica una regla para enrutar el evento a un objetivo. Las reglas hacen coincidir los eventos con los objetivos o bien en función de la estructura del evento, llamado un patrón de evento, o bien de una programación.
- AWS Lambda: AWS Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo. Solo paga por el tiempo de proceso que consume. No se aplican cargos cuando su código no se está ejecutando.
- AWS Organizations: AWS Organizations le ayuda a administrar y gobernar su entorno de manera centralizada a medida que hace crecer y escalar sus recursos de AWS. Con AWS Organizations, puede crear nuevas cuentas de AWS y asignar recursos mediante programación, agrupar cuentas para organizar sus flujos de trabajo, aplicar políticas a cuentas o grupos para la gobernanza y simplificar la facturación mediante un único método de pago para todas sus cuentas.
- AWS Step Functions: AWS Step Functions es un servicio de flujo de trabajo visual de bajo código que se utiliza para orquestar los servicios de AWS, automatizar los procesos empresariales y crear aplicaciones sin servidor. Los flujos de trabajo gestionan los errores, los reintentos, la paralelización, las integraciones de servicios y la observabilidad para que los desarrolladores puedan centrarse en una lógica empresarial de mayor valor.
- AWS Transit Gateway conecta las VPC y las redes en las instalaciones a través de un concentrador central. Esto simplifica su red y pone fin a las complejas relaciones de interconexión. Actúa como un router en la nube, de modo que cada nueva conexión se realiza solo una vez.
- Amazon Virtual Private Cloud (Amazon VPC) es un servicio que le permite lanzar recursos de AWS en una red virtual lógicamente aislada que usted defina.
- AWS X-Ray recopila datos sobre las solicitudes que su atiende su aplicación y proporciona herramientas que puede utilizar para consultar, filtrar y obtener información sobre dichos datos para identificar problemas y oportunidades de optimización.

Código

El código fuente de esta solución está disponible en el GitHub repositorio Transit Gateway Attachment Tagger. El repositorio incluye los siguientes archivos:

- `tgw-attachment-tagger-main-stack.yaml` crea todos los recursos necesarios para respaldar esta solución en la cuenta Shared Networking.
- `tgw-attachment-tagger-organizations-stack.yaml` crea un rol en la cuenta de administración de la organización.

Epics

Implemente el conjunto principal de soluciones

Tarea	Descripción	Habilidades requeridas
Reúna la información necesaria sobre los requisitos previos.	Para configurar el acceso entre cuentas desde la función de Lambda a la API de AWS Organizations, necesita el ID de cuenta de la cuenta de administración de la organización. Nota: El orden en el que se crean las dos CloudFormation pilas es importante. Primero debe implementar los recursos en la cuenta de red compartida. El rol en la cuenta Shared Networking ya debe existir antes de implementar los recursos en la cuenta de administración de la organización. Para obtener más información, consulte la documentación de AWS.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Inicie la CloudFormation plantilla para la pila de soluciones principal.	La plantilla de la pila de soluciones principal implementará las funciones de IAM, el flujo de trabajo de Step Functions, las funciones de Lambda y CloudWatch el evento. Abra la consola de administración de AWS para la cuenta de red compartida y, a continuación, abra la CloudFormation consola. Cree la pila con la plantilla `tgw-attachment-tagger-main-stack.yaml` y los siguientes valores: • Nombre de la pila: tgw-attachment-tagger-main-stack • awsOrganizationsRootAccountId— ID de cuenta de la cuenta de administración de la organización • Parámetro TGWRegions: regiones de AWS para la solución, introducidas como una cadena delimitada por comas • Parámetro TGWList: identificadores de las puertas de enlace de tránsito que se van a excluir de la solución, introducidos	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	en una cadena delimitada por comas Para obtener más información sobre el lanzamiento de una CloudFormation pila, consulte la documentación de AWS.	
Compruebe que la solución se haya lanzado correctamente.	Espere a que la CloudForm ation pila alcance el estado CREATE_COMPLETE. Este proceso no debería tardar más de un minuto. Abra la consola Step Functions y compruebe que se ha creado una nueva máquina de estados con el nombre tgw-attachment-tagger-state-machine.	DevOps ingeniero

Implemente el paquete de AWS Organizations

Tarea	Descripción	Habilidades requeridas
Reúna la información necesaria sobre los requisitos previos.	Para configurar el acceso entre cuentas desde la función de Lambda a la API de AWS Organizations, necesita el ID de cuenta de la cuenta Shared Networking.	DevOps ingeniero
Lance la CloudFormation plantilla para la pila Organizat ions	En la plantilla de AWS Organizations stack, se implementará el rol de IAM	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	en la cuenta de gestión de la organización. Acceda a la consola de AWS de la cuenta de administración de la organización y, a continuación, abra la CloudFormation consola. Cree la pila con la plantilla `tgw-attachment-tagger-organizations-stack.yaml` y los siguientes valores: • Nombre de la pila: tgw-attachment-tagger-organizations-stack • NetworkingAccountIdparámetro: ID de cuenta de la cuenta de red compartida Para las demás opciones de creación de pilas, usa los valores predeterminados.	

Tarea	Descripción	Habilidades requeridas
Compruebe que la solución se haya lanzado correctamente.	Espere a que la CloudFormation pila alcance el estado CREATE_COMPLETE. Este proceso no debería tardar más de un minuto. Abra la consola de Identity and Access Management (IAM) y compruebe que se haya creado un nuevo rol con el nombre -query-role. tgw-attachment-tagger-organization	DevOps ingeniero

Verificación de la solución

Tarea	Descripción	Habilidades requeridas
Ejecuta la máquina de estado.	Abra la consola Step Functions de la cuenta Shared Networking y elija Equipos de estado en el panel de navegación. Seleccione el estado machine tgw-attachment-tagger-state-machine y elija Iniciar ejecución. Como la solución no utiliza la entrada de esta máquina de estados, puede utilizar el valor predeterminado. `{`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	<pre>"Comment": "Insert your JSON here" }</pre> Seleccione Iniciar ejecución.	
Vigile la máquina de estados hasta su finalización.	En la nueva página que se abre, puede ver cómo funciona la máquina de estados. La duración dependerá de la cantidad de conexiones de puerta de enlace de tránsito que se procesen. En esta página, puede examinar cada paso de la máquina de estados. Puede ver las distintas tareas de la máquina de estados y seguir los enlaces a los CloudWatch registros de las funciones de Lambda. Para las tareas que se ejecutan en paralelo dentro del mapa, puede usar la lista desplegable del Índice para ver las implementaciones específicas de cada región.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Compruebe las etiquetas de conexión de puerta de enlace de tránsito.	Abra la consola de VPC de la cuenta Shared Networking y elija Conexiones de puerta de enlace de tránsito. En la consola, se proporcio na una etiqueta de nombre para los archivos adjuntos que cumplen los criterios (el archivo adjunto se propaga a una tabla de enrutamiento de puerta de enlace de tránsito y el propietario del recurso es miembro de la organización).	DevOps ingeniero
Verifique el inicio CloudWatch del evento.	Espere a que se inicie el CloudWatch evento. Está programado para las 06:00 UTC. Abra la consola Step Functions de la cuenta Shared Networking y elija State machines (Máquinas de estado) en el panel de navegación. Seleccione el estado machine tgw-attachment-tagger-state-machine. Compruebe que la solución se haya ejecutado a las 06:00 UTC.	DevOps ingeniero

Recursos relacionados

- AWS Organizations

- AWS Resource Access Manager
- Orquestador de redes de tránsito sin servidor
- Creación de roles de IAM
- Creación de una pila en la CloudFormation consola de AWS

Verifique que los equilibradores de carga ELB requieran la terminación de TLS

Creado por Priyanka Chaudhary (AWS)

Entorno: producción	Tecnologías: redes, seguridad, identidad, cumplimiento	Servicios de AWS: Amazon CloudWatch Events; Elastic Load Balancing (ELB); AWS Lambda

Resumen

En la nube de Amazon Web Services (AWS), Elastic Load Balancing (ELB) distribuye automáticamente el tráfico entrante de las aplicaciones entre varios destinos, como instancias de Amazon Elastic Compute Cloud (Amazon EC2), contenedores, direcciones IP y funciones de AWS Lambda. Los equilibradores de carga emplean oyentes para definir los puertos y protocolos que usa el equilibrador de carga para aceptar el tráfico de los usuarios. Los equilibradores de carga de aplicación toman las decisiones de enrutamiento en la capa de aplicación y emplean protocolos HTTP/HTTPS. Los equilibradores de carga clásicos toman las decisiones de enrutamiento en la capa de transporte, mediante los protocolos TCP o Secure Sockets Layer (SSL), o en la capa de aplicación, mediante HTTP/HTTPS.

Este patrón proporciona un control de seguridad que examina varios tipos de eventos para los equilibradores de carga de aplicaciones y los equilibradores de carga clásicos. Cuando se invoca la función, AWS Lambda inspecciona el evento y se asegura de que el equilibrador de carga sea compatible.

La función inicia un evento de Amazon CloudWatch Events en las siguientes llamadas a la API: CreateLoadBalancerCreateLoadBalancerListeners, DeleteLoadBalancerListeners, CreateLoadBalancerPolicy, SetLoadBalancerPoliciesOfListener, CreateListenerDeleteListener, y ModifyListener. Cuando el evento detecta una de estas API, llama a AWS Lambda, que ejecuta un script de Python. El script de Python evalúa si el oyente contiene un certificado SSL y si la política que se aplica utiliza seguridad de la capa de transporte (TLS). Si se determina que la política de SSL es distinta de TLS, la función envía una notificación de Amazon Simple Notification Service (Amazon SNS) al usuario con la información pertinente.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa

Limitaciones

- Este control de seguridad no comprueba los equilibradores de carga existentes, a menos que se realice una actualización en los dispositivos de escucha del equilibrador de carga.
- Este control de seguridad es regional. Debe implementarlo en cada región de AWS que desee supervisar.

Arquitectura

Arquitectura de destino

Automatizar y escalar

- Si utiliza AWS Organizations, puede utilizar AWS Cloudformation StackSets para implementar esta plantilla en varias cuentas que desee supervisar.

Herramientas

Servicios de AWS

- AWS CloudFormation: AWS le CloudFormation ayuda a modelar y configurar sus recursos de AWS, a aprovisionarlos de forma rápida y coherente y a gestionarlos durante todo su ciclo de vida. Facilita poder usar una plantilla para describir los recursos y sus dependencias, y lanzarlos y configurarlos juntos como una pila, en lugar de administrarlos de forma individual.
- Amazon CloudWatch Events: Amazon CloudWatch Events ofrece una transmisión casi en tiempo real de los eventos del sistema que describen los cambios en los recursos de AWS.
- AWS Lambda: AWS Lambda es un servicio informático que permite ejecutar código sin aprovisionar ni administrar servidores.

- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos altamente escalable que se puede utilizar para una amplia gama de soluciones de almacenamiento, incluidos sitios web, aplicaciones móviles, copias de seguridad y lagos de datos.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) coordina y gestiona la entrega o el envío de mensajes entre publicadores y clientes, incluyendo los servidores web y las direcciones de correo electrónico. Los suscriptores reciben todos los mensajes publicados de los temas a los que están suscritos y todos los suscriptores de un tema reciben los mismos mensajes.

Código

Este patrón incluye los siguientes archivos adjuntos:

- `ELBRequirestlstermination.zip`: el código Lambda para el control de seguridad.
- `ELBRequirestlstermination.yml`— La CloudFormation plantilla que configura el evento y la función Lambda.

Epics

Configure el bucket de S3

Tarea	Descripción	Habilidades requeridas
Elimine el bucket de S3.	En la consola Amazon S3, elija o cree un bucket de S3 para alojar el archivo .zip de código Lambda. Este bucket de S3 debe estar en la misma región de AWS que el equilibrador de carga que desea evaluar. Un nombre de bucket de S3 es globalmente único y todas las cuentas de AWS comparten el espacio de nombres. El nombre de bucket de S3 no puede incluir barras a la izquierda.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Cargue el código Lambda.	Cargue el código Lambda (archivo `ELBRequirestlstermination.zip`) que se proporciona en la sección Adjuntos en el bucket de S3.	Arquitecto de la nube

Implemente la plantilla CloudFormation

Tarea	Descripción	Habilidades requeridas
Lance la CloudFormation plantilla de AWS.	Abra la CloudFormation consola de AWS en la misma región de AWS que su bucket de S3 e implemente la plantilla adjunta `ELBRequirestlstermination.yml`. Para obtener más información sobre la implementación de CloudFormation plantillas de AWS, consulte Crear una pila en la CloudFormation consola de AWS en la CloudFormation documentación.	Arquitecto de la nube
Complete los parámetros de la plantilla.	Al lanzar la plantilla, se le solicitará la siguiente información: • Bucket de S3: especifique el bucket creado o seleccionado en la primera Epic. Aquí es donde cargó el código	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	Lambda adjunto (archivo `ELBRequirestlstermination.zip`). • Clave S3: especifique la ubicación del archivo .zip de Lambda en el bucket de S3 (por ejemplo, `ELBRequirestlstermination.zip` o). `controls/ELBRequirestlstermination.zip` No incluya barras a la izquierda . • Correo de notificación: proporcione una dirección de email activa en la que desea recibir las notificaciones de Amazon SNS. • Nivel de registro Lambda: especifique el nivel y la frecuencia de registro de la función de Lambda. Utilice Info para registrar mensajes informativos detallados sobre el progreso, Error para los eventos de error que pudieran continuar con la implementación y Advertencia en caso de situaciones potencialmente dañinas.	

Confirmar la suscripción

Tarea	Descripción	Habilidades requeridas
Confirmar la suscripción.	Cuando la CloudFormation plantilla se implementa correctamente, envía un correo electrónico de suscripción a la dirección de correo electrónico que proporcionó. Debe confirmar esta suscripción de correo electrónico para recibir las notificaciones de infracciones.	Arquitecto de la nube

Recursos relacionados

- Creación de una pila en la CloudFormation consola de AWS (CloudFormation documentación de AWS)
- ¿Qué es AWS Lambda? (documentación de AWS Lambda)
- ¿Qué es un equilibrador de carga clásico? (documentación del ELB)
- ¿Qué es un equilibrador de carga de aplicación? (documentación del ELB)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Vea los registros y las métricas de AWS Network Firewall mediante Splunk

Creado por Ivo Pinto

Entorno: PoC o piloto	Tecnologías: redes; nativas de la nube; entrega de contenido ; operaciones; seguridad, identidad y cumplimiento	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon CloudWatch; Amazon CloudWatch Logs; AWS Network Firewall		

Resumen

Muchas organizaciones utilizan Splunk Enterprise como una herramienta centralizada de agregación y visualización de registros y métricas de diferentes fuentes. Este patrón le ayuda a configurar Splunk para obtener registros y métricas de AWS Network Firewall de Amazon CloudWatch Logs mediante el complemento Splunk para AWS.

Para lograrlo, debe crear un rol de AWS Identity and Access Management (IAM) de solo lectura. El complemento Splunk para AWS utiliza esta función para acceder CloudWatch. Debe configurar el complemento Splunk para que AWS extraiga métricas y registros. CloudWatch Por último, debe crear visualizaciones en Splunk a partir de los datos de registro y las métricas recuperados.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de Splunk
- Una instancia de Splunk Enterprise, versión 8.2.2 o posterior
- Una cuenta de AWS activa
- Network Firewall, instalado y configurado para enviar CloudWatch registros a Logs

Limitaciones

- Splunk Enterprise debe implementarse como un clúster de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la nube de AWS.
- La recopilación de datos mediante una función de IAM detectada automáticamente para Amazon EC2 no está permitida en las regiones de AWS en China.

Arquitectura

En el siguiente diagrama se ilustra lo siguiente:

1. Network Firewall publica CloudWatch registros en Logs.
2. Splunk Enterprise recupera métricas y registros de. CloudWatch

Para rellenar métricas y registros de ejemplo en esta arquitectura, una carga de trabajo genera tráfico que pasa a través del punto final de Network Firewall para ir a Internet. Esto se logra mediante el uso de tablas de enrutamiento. Si bien este patrón utiliza una única instancia de Amazon EC2 como carga de trabajo, se puede aplicar a cualquier arquitectura siempre que Network Firewall esté configurado para enviar registros a CloudWatch Logs.

Esta arquitectura también utiliza una instancia de Splunk Enterprise en otra nube privada virtual (VPC). Sin embargo, la instancia de Splunk puede estar en otra ubicación, por ejemplo, en la misma VPC que la carga de trabajo, siempre que pueda acceder a CloudWatch las API.

Herramientas

Servicios de AWS

- Amazon CloudWatch Logs le ayuda a centralizar los registros de todos sus sistemas, aplicaciones y servicios de AWS para que pueda supervisarlos y archivarlos de forma segura.
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- AWS Network Firewall es un servicio de detección y prevención de intrusiones y de firewall de red con estado y administrado para nubes privadas virtuales (VPC) en la nube de AWS.

Otras herramientas

- Splunk le permite monitorear, visualizar y analizar los datos de registro.

Epics

Creación de un rol de IAM

Tarea	Descripción	Habilidades requeridas
Cree la política de IAM.	Siga las instrucciones de Creación de políticas mediante el editor JSON para crear la política de IAM que conceda acceso de solo lectura a los datos y las métricas de CloudWatch Logs. CloudWatch Pegue la siguiente política de en el editor JSON. { "Statement": [{ "Action": ["cloudwatch:List*", "cloudwatch:Get*", "network-firewall:List*", "logs:Describe*", "logs:Get*", "logs:List*", "logs:StartQuery",	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	<pre>"logs:StopQuery", "logs:TestMetricFi lter", "logs:FilterLogEve nts", "network-firewall: Describe*"], "Effect": "Allow", "Resource": "*" }], "Version": "2012-10-17" }</pre>	
Crea un nuevo rol de IAM.	Siga las instrucciones de Crear un rol para delegar permisos a un servicio de AWS para crear el rol de IAM al que utiliza el complemento Splunk para AWS para acceder. CloudWatch Para las políticas de permisos, elija la política que creó anteriormente.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Asigne la función de IAM a las instancias EC2 del clúster de Splunk.	1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/. 2. En el panel de navegación, seleccione Instancias. 3. Seleccione las instancias EC2 en el clúster de Splunk. 4. Elija Acciones, Seguridad y, a continuación, Modificar la función de IAM. 5. Seleccione el rol de IAM que creó anteriormente y, a continuación, elija Guardar.	Administrador de AWS

Instalación del complemento Splunk para AWS

Tarea	Descripción	Habilidades requeridas
Instale el complemento.	1. En el panel de control de Splunk, dirígete a Splunk Apps. 2. Busca el complemento Splunk para Amazon Web Services. 3. Elija Instalar. 4. Proporcione sus credenciales de Splunk.	Administrador de Splunk
Configure las credenciales de AWS.	1. En el panel de control de Splunk, vaya al complemento Splunk para AWS.	Administrador de Splunk

Tarea	Descripción	Habilidades requeridas
	2. Elija Configuration (Configuración). 3. En la columna Función de IAM detectada automáticamente, seleccione la función de IAM que creó anteriormente. Para obtener más información, consulte Buscar un rol de IAM en su instancia de plataforma Splunk en la documentación de Splunk.	

Configure el acceso de Splunk a CloudWatch

Tarea	Descripción	Habilidades requeridas
Configure la recuperación de los registros de Network Firewall desde los CloudWatch registros.	1. En el panel de control de Splunk, vaya al complemento Splunk para AWS. 2. Elija Entrada. 3. Elija Crear nueva entrada. 4. En la lista, elija Tipo de datos personalizado y, a continuación, seleccione CloudWatch Registros. 5. Proporcione el nombre, la cuenta de AWS, la región de AWS y el grupo de registros de sus registros de Network Firewall. 6. Seleccione Guardar.	Administrador de Splunk

Tarea	Descripción	Habilidades requeridas
	De forma predeterminada, Splunk recupera los datos del registro cada 10 minutos. Se trata de un parámetro configurable en los ajustes avanzados. Para obtener más información, consulte Configurar una entrada de CloudWatch registros mediante Splunk Web en la documentación de Splunk.	

Tarea	Descripción	Habilidades requeridas
Configure la recuperación de las métricas de Network Firewall desde CloudWatch.	1. En el panel de control de Splunk, vaya al complemento Splunk para AWS. 2. Elija Entrada. 3. Elija Crear nueva entrada. 4. En la lista, elija CloudWatch. 5. Proporcione el nombre, la cuenta de AWS y la región de AWS para sus métricas de Network Firewall. 6. Junto a Configuración métrica, selecciona Editar en modo avanzado. 7. (Opcional) Elimine todos los espacios de nombres preconfigurados. 8. Elija Agregar espacio de nombres y, a continuación, asígnele el nombre AWS/. NetworkFirewall 9. En Dimension Value, añada lo siguiente. `[{"AvailabilityZone":[".*"],"Engine":[".*"],"FirewallName":[".*"]}]` 10. En Métricas, elija Todas. 11. En Estadísticas métricas, elija Suma. 12. Seleccione Aceptar.	Administrador de Splunk

Tarea	Descripción	Habilidades requeridas
	13. Seleccione Guardar. De forma predeterminada, Splunk recupera los datos de las métricas cada 5 minutos. Se trata de un parámetro configurable en los ajustes avanzados. Para obtener más información, consulte Configurar una CloudWatch entrada mediante Splunk Web en la documentación de Splunk.	

Cree visualizaciones de Splunk mediante consultas

Tarea	Descripción	Habilidades requeridas
Vea las direcciones IP de origen principal.	1. En el panel de control de Splunk, vaya a Search & Reporting. 2. En el cuadro Introduzca «Buscar aquí», introduzca lo siguiente. `sourcetype="aws:cloudwatchlogs" | top event.src_ip` Esta consulta muestra una tabla de las direcciones IP de origen con más tráfico, en orden descendente.	Administrador de Splunk

Tarea	Descripción	Habilidades requeridas
	3. Para obtener una representación gráfica, elija Visualización.	
Ver las estadísticas de los paquetes.	1. En el panel de control de Splunk, vaya a Search & Reporting. 2. En el cuadro Introduzca «Buscar aquí», introduzca lo siguiente. `sourcetype="aws:cloudwatch"| timechart sum(Sum) by metric_name` Esta consulta muestra una tabla con las métricas `DroppedPackets` y `ReceivedPackets` por minuto. `PassedPackets` 3. Para obtener una representación gráfica, elija Visualización.	Administrador de Splunk

Tarea	Descripción	Habilidades requeridas
Vea los puertos de origen más utilizados.	1. En el panel de control de Splunk, vaya a Search & Reporting. 2. En el cuadro Introduzca «Buscar aquí», introduzca lo siguiente. `sourcetype="aws:cloudwatchlogs" | top event.dest_port` Esta consulta muestra una tabla de los puertos de origen con más tráfico, en orden descendente. 3. Para obtener una representación gráfica, elija Visualización.	Administrador de Splunk

Recursos relacionados

Documentación de AWS

- Creación de un rol para delegar permisos a un servicio de AWS (documentación de IAM)
- Creación de políticas de IAM (documentación de IAM)
- Registro y supervisión en AWS Network Firewall (documentación de Network Firewall)
- Configuraciones de tablas de enrutamiento para AWS Network Firewall (documentación de Network Firewall)

Publicaciones del blog de AWS

- Modelos de implementación de AWS Network Firewall

AWS Marketplace

- Imagen de máquina de Amazon (AMI) de Splunk Enterprise

Más patrones

- Acceder a un host bastión mediante Session Manager y Amazon EC2 Instance Connect
- Acceda a las aplicaciones de contenedores de forma privada en Amazon ECS mediante AWS Fargate PrivateLink, AWS y un Network Load Balancer
- Acceda a las aplicaciones de contenedores de forma privada en Amazon ECS mediante AWS PrivateLink y un Network Load Balancer
- ???
- Compruebe si hay entradas de red de un solo host en las reglas de ingreso de grupos de seguridad para IPv4 e IPv6
- Implemente un firewall con AWS Network Firewall y AWS Transit Gateway
- Implemente una API de Amazon API Gateway en un sitio web interno mediante puntos de conexión privados y un Equilibrador de carga de aplicación
- Implemente controles de acceso basados en atributos de detección para subredes públicas mediante AWS Config
- ???
- Habilite conexiones cifradas para instancias de base de datos de PostgreSQL en Amazon RDS
- Amplíe las VRF a AWS mediante AWS Transit Gateway Connect
- Migración de una carga de trabajo de F5 BIG-IP a F5 BIG-IP VE en la nube de AWS
- Preserve el espacio IP enrutable en los diseños de VPC de varias cuentas para subredes que no son de carga de trabajo
- Impida el acceso a Internet a nivel de cuenta mediante una política de control de servicios
- Enviar alertas desde AWS Network Firewall a un canal de Slack
- Sirva contenido estático en un bucket de Amazon S3 a través de una VPC mediante Amazon CloudFront
- Configure la recuperación ante desastres para Oracle JD Edwards EnterpriseOne con AWS Elastic Disaster Recovery
- Configure la resolución de DNS para redes híbridas en un entorno de AWS de varias cuentas
- Utilice las consultas de BMC Discovery para extraer datos de migración para planificar la migración
- Utilice Network Firewall para capturar los nombres de dominio DNS de la indicación del nombre del servidor (SNI) para el tráfico saliente

Sistemas operativos

Temas

Migración de los sistemas BYOL de RHEL a instancias con licencia incluida de AWS mediante AWS MGN

Creado por Mike Kuznetsov (AWS)

Entorno: producción	Origen: instancia BYOL de RHEL (local o en cualquier otro entorno de nube)	Destino: instancia de RHEL con licencia AWS incluida
Tipo R: volver a alojar	Carga de trabajo: todas las demás cargas de trabajo	Tecnologías: sistemas operativos; infraestructura; migración
Servicios de AWS: Servicio de migración de aplicaciones de AWS		

Resumen

Al migrar sus cargas de trabajo a AWS mediante el AWS Application Migration Service (AWS MGN), es posible que tenga que migrar mediante lift-and-shift (volver a alojar) sus instancias de Red Hat Enterprise Linux (RHEL) y cambiar la licencia del modelo traiga su propia licencia (BYOL) predeterminado a un modelo AWS License Included (LI) durante la migración. AWS MGN admite un enfoque escalable que utiliza los Identificadores de imagen de máquina de Amazon (AMI). Este patrón describe cómo realizar el cambio de licencia en los servidores de RHEL durante la migración de volver a alojar a escala. También explica cómo cambiar la licencia de un sistema RHEL que ya se ejecuta en Amazon Elastic Compute Cloud (Amazon EC2).

Requisitos previos y limitaciones

Requisitos previos

- Acceso a la cuenta de AWS de destino
- AWS MGN se inicializó en la cuenta y región de AWS de destino para la migración (no es obligatorio si ya ha migrado de su sistema en las instalaciones a AWS)
- Un servidor RHEL de origen con una licencia RHEL válida

Arquitectura

Este patrón cubre dos escenarios:

- Migración de un sistema en las instalaciones directamente a una instancia de AWS LI mediante AWS MGN. Para este escenario, siga las instrucciones de la primera epopeya (Migración a una instancia de LI: opción 1) y de la tercera epopeya.
- Cambie el modelo de licencias de BYOL a LI para un sistema RHEL migrado anteriormente que ya se ejecuta en Amazon EC2. Para este escenario, siga las instrucciones de la segunda epopeya (migrar a una instancia de LI: opción 2) y de la tercera epopeya.

Nota: La tercera epopeya implica la reconfiguración de la nueva instancia de RHEL para utilizar los servidores Red Hat Update Infrastructure (RHUI) proporcionados por AWS. Este proceso es el mismo en ambos escenarios.

Herramientas

Servicios de AWS

- El AWS Application Migration Service (AWS MGN) le ayuda a volver a alojar (migrar mediante lift-and-shift) las aplicaciones a la nube de AWS sin cambios y con un tiempo de inactividad mínimo.

Epics

Migración a una instancia LI: opción 1 (para un sistema RHEL en las instalaciones)

Tarea	Descripción	Habilidades requeridas
Busque el Identificador de AMI de la instancia de RHEL AWS LI en la región de destino.	Visite AWS Marketplace o utilice la consola Amazon EC2 para buscar el Identificador de AMI de RHEL que coincida con la versión del sistema fuente de RHEL (por ejemplo, RHEL-7.7) y anote el ID de AMI. En la consola Amazon EC2, puede filtrar las AMI	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	mediante uno de los siguientes términos de búsqueda: • Descripción = Proporcionada por Red Hat, Inc. • Nombre de la AMI = RHEL-7.7	

Tarea	Descripción	Habilidades requeridas
Configure los ajustes de lanzamiento de AWS MGN.	1. En la consola de AWS MGN, añada el sistema RHEL de origen: instale el agente de replicación de AWS y añada el servidor de origen siguiendo las instrucciones de la documentación de AWS MGN. 2. En la página Servidores de origen, elija el sistema RHEL de origen y, a continuación, elija la pestaña Configuración de lanzamiento. 3. En la sección Configuración de las opciones generales de lanzamiento, seleccion e Editar. Para deshabilitar la selección automática y especificar manualmen te el tipo de instancia de destino, cambie el Tamaño correcto del tipo de instancia a Ninguno y, a continuación, seleccion e Guardar configuración. Esto le permite usar el tipo de instancia que haya configurado en su plantilla de lanzamiento de Amazon EC2. Para obtener más información, consulte la	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	documentación de AWS MGN. 4. En la sección Plantilla de lanzamiento de EC2, elija Modificar. En el cuadro de diálogo Acerca de la modificación de las plantillas de lanzamiento de EC2, vuelva a seleccion ar Modificar. Esto abre la consola Amazon EC2 para que pueda cambiar la plantilla de esta instancia. 5. Consulte las considera ciones clave en la documentación de AWS MGN. Nota: Puede hacer caso omiso de la advertencia de no elegir su propia AMI. 6. En la consola Amazon EC2, en la nueva plantilla de lanzamiento, modifique lo siguiente: • Para AMI, especifiq ue el Identificador de AMI que identificó anteriormente o busque RHEL-x y especifique la versión que necesita (por ejemplo, RHEL-7.7).	

Tarea	Descripción	Habilidades requeridas
	• En Tipo de instancia, defina el tipo de instancia de destino deseado. • No modifique las siguientes secciones: par de claves (inicio de sesión), Configuración de red (a menos que desee especificar una subred y grupos de seguridad de destino), Almacenamiento y Etiquetas de recursos (a menos que desee añadir o modificar alguna etiqueta). • (Opcional) En la sección Detalles avanzados, especifique el rol del perfil de instancia de IAM, si es necesario para que AWS Systems Manager lo administre en el futuro. 7. Seleccione Crear versión de plantilla y, a continuación, elija el enlace que aparece en el mensaje de confirmación para ver la plantilla de lanzamiento. 8. Seleccione Acciones y Cómo establecer la versión predeterminada. En la Versión de plantilla, seleccione la versión más reciente (versión 2 para	

Tarea	Descripción	Habilidades requeridas
	un sistema nuevo) y, a continuación, elija Cómo establecer como versión predeterminada. AWS MGN utilizará ahora esta versión de la plantilla de lanzamiento para lanzar instancias de prueba o de transición. Para obtener más información, consulte la documentación de AWS MGN.	

Tarea	Descripción	Habilidades requeridas
Valide la configuración.	1. En la consola MGN de AWS, en la página Servidores de origen, elija su servidor de origen y, a continuación, elija la pestaña Configuración de lanzamiento. 2. En la sección Plantilla de lanzamiento de EC2, compruebe que los parámetros del Tipo de instancia, la subred y los Grupos de seguridad estén configurados correctam ente. Nota: En esta sección no se muestra el Identificador de AMI que ha seleccion ado. Para ver el Identific ador, puede abrir la consola Amazon EC2 en la vista Plantillas de lanzamiento y buscar el Identificador de plantilla que se muestra en esta sección.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Lance la nueva instancia de LI.	1. Cuando se complete la sincronización inicial, la columna Ciclo de vida de la migración del servidor en la página Servidores de origen de la consola AWS MGN cambia a Listo para la prueba. Para lanzar la nueva instancia de prueba, elija su servidor de origen, abra el menú Prueba y transición y, a continuac ión, elija Lanzar instancia s de prueba. Seleccione Ver detalles del trabajo para supervisar el estado del trabajo de lanzamiento. Para obtener más informaci ón, consulte la documenta ción de AWS MGN. 2. Espere a que se complete el trabajo de lanzamien to y, a continuación, abra la página de detalles de la instancia EC2 lanzada. Seleccione la pestaña Detalles y compruebe que la sección de Detalles de la instancia contiene lo siguiente: • Datos de plataforma: “Red Hat Enterprise Linux”	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	• Nombre de la AMI: el nombre de la AMI que especificó en la plantilla de lanzamiento de EC2 3. Realizar la transición a la nueva instancia de LI siguiendo las instrucciones de la documentación de AWS MGN. 4. Vuelva a configurar la nueva instancia para usar los servidores RHUI proporcionados por AWS siguiendo los pasos de la última epopeya.	

Migración a una instancia LI: opción 2 (para una instancia RHEL BYOL EC2)

Tarea	Descripción	Habilidades requeridas
Migre una instancia de RHEL BYOL EC2 a una instancia de AWS LI.	Puede cambiar los sistemas RHEL que anteriormente migró a AWS como BYOL a instancias de AWS LI moviendo sus discos (volúmenes de Amazon Elastic Block Store) y adjuntándolos a una nueva instancia de LI. Para realizar este cambio, siga estos pasos: 1. Lance una nueva instancia de RHEL de destino desde una AMI de RHEL LI.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	Asegúrese de que la AMI que ha seleccionado: • Utiliza la misma versión de RHEL que la instancia de RHEL actual. • Tiene el mismo proceso de arranque (BIOS o UEFI) que la instancia de RHEL actual. Por ejemplo, si el servidor de origen está basado en BIOS, utilice la AMI RHEL de AWS Marketplace que también esté basada en BIOS; para los sistemas basados en UEFI, elija la AMI basada en UEFI. 2. Detenga ambas instancias: la nueva instancia de LI y la instancia de origen original. 3. Separe todos los volúmenes de EBS (incluido el disco raíz) de la nueva instancia de LI y elimínelos. 4. Separe todos los volúmenes de EBS (incluido el disco raíz) de la antigua instancia de origen y adjúntelos a la nueva instancia de LI. Mantenga la misma asignación de volúmenes a los dispositivos. (Por ejemplo, el	

Tarea	Descripción	Habilidades requeridas
	volumen de EBS que estaba conectado anteriormente a la unidad de `/dev/sda` debe estar conectado como `/dev/sda` a la nueva instancia). 5. Elimine la instancia de origen (ahora sin disco). 6. Inicie la nueva instancia de LI. Inicie sesión en la instancia y vuelva a configurarla para usar los servidores RHUI proporcionados por AWS siguiendo los pasos de la siguiente epopeya.	

Reconfigurar el sistema operativo RHEL para usar la RHUI proporcionada por AWS (ambas opciones)

Tarea	Descripción	Habilidades requeridas
Anule el registro del sistema operativo de la suscripción y la licencia de Red Hat.	Tras la migración y la transición exitosa, es necesario eliminar el sistema RHEL de la suscripción a Red Hat para dejar de consumir la licencia de Red Hat y evitar la doble facturación. Para eliminar el sistema operativo RHEL de la suscripción a Red Hat, siga el proceso descrito en la documentación	Administrador de sistemas o Linux

Tarea	Descripción	Habilidades requeridas
	sobre la gestión de suscripciones de Red Hat (RHSM). Utilice el comando CLI: `subscription-manager unregister` También puede deshabilitar el complemento del administrador de suscripciones para dejar de comprobar el estado de la suscripción en cada llamada de yum. Para ello, edite el archivo de configuración `/etc/yum/pluginconf.d/subscription-manager.conf` y cambie el parámetro `enabled=1` a `enabled=0` .	

Tarea	Descripción	Habilidades requeridas
Sustituya la configuración de actualización anterior (RHUI, red Red Hat Satellite, repositorios yum) por la RHUI proporcionada por AWS.	Debe volver a configurar el sistema RHEL migrado para utilizar los servidores RHUI proporcionados por AWS. Esto le da acceso a los servidores RHUI dentro de las regiones de AWS sin necesidad de una infraestr uctura de actualización externa. El proceso consta de los pasos siguientes: 1. Realice una copia de seguridad de la configura ción actual de yum. 2. Elimine la configuración y los paquetes antiguos de RHUI (repositorios yum). 3. Añada los nuevos paquetes de certificados y configura ción de RHUI proporcio nados por AWS. Debe recuperarlos de otra instancia de RHEL en AWS, ya que estos paquetes de configuración solo están disponibles en los servidore s RHUI proporcionados por AWS. Estos son los pasos y comandos detallados:	Administrador de sistemas o Linux

Tarea	Descripción	Habilidades requeridas
	1. Haga una copia de seguridad de la configuración y los certificados de yum existentes copiando todas las carpetas `/etc/yum*` y `/etc/pki/*` en una ubicación de copia de seguridad. Por ejemplo: `mkdir yum-backup` `cp -ra /etc/yum* /etc/pki ./yum-backup` `tar czf yum-backup.tgz ./yum-backup` 2. Elimine la configuración y los paquetes de RHUI anteriores: a. Encuentre todos los paquetes RHUI instalados: `sudo rpm -qa | grep rhui` b. Elimine estos paquetes: `sudo yum remove $(rpm -qa | grep rhui)` c. Elimine el archivo `/etc/yum/vars/releasever`, si existe. 3. Añada los nuevos paquetes de certificados y RHUI proporcionados por AWS.	

Tarea	Descripción	Habilidades requeridas
	Debe recuperarlos de otra instancia de RHEL en AWS. Puede hacer esto de varias formas. Por ejemplo, puede seguir las instrucciones que se proporcionan en el artículo de la base de conocimiento de Red Hat: a. Lance otra instancia de RHEL (RHEL-EC2) desde AWS Marketplace. b. Descargue dos paquetes de esta instancia: el paquete de configuración del cliente RHUI más reciente y los certifica dos de la autoridad de certificación (CA). Por ejemplo, ejecute este comando desde el escritorio: `ssh RHEL-EC2 "sudo yumdownloader ca-certificates rh-amazon-rhui-cli ent"` c. Copie los paquetes de la instancia RHEL-EC2 al nuevo sistema migrado. Por ejemplo: `scp RHEL-EC2:rh-amazon-rhui-cli`	

Tarea	Descripción	Habilidades requeridas
	ent* RHEL-EC2:ca-certificates* . ssh <migrated-instance> "mkdir /tmp/amazon" scp rh-amazon-rhui-client* ca-certificates* <migrated-instance>:/tmp/amazon d. Instale los nuevos paquetes de configuración de RHUI y CA en la instancia migrada: ssh <migrated-instance> "sudo rpm -Uhv /tmp/amazon/*"	
Valide la configuración.	En la instancia migrada de destino, compruebe que la nueva configuración es correcta: sudo yum clean all sudo yum repolist	Administrador de sistemas o Linux

Recursos relacionados

- Guía del usuario del Servicio de migración de aplicaciones de AWS (AWS MGN)
- Obtenga un paquete de cliente RHUI de AWS compatible con IMDSv2 (artículo de la base de conocimiento de Red Hat)
- Plantillas de lanzamiento de Amazon EC2 (documentación de Amazon EC2)

Resolver los errores de conexión después de migrar Microsoft SQL Server a la nube de AWS

Creado por Premkumar Chelladurai (AWS)

Entorno: producción	Tecnologías: sistemas operativos; migración	Carga de trabajo: Microsoft
Servicios de AWS: Amazon EC2		

Resumen

Tras migrar el Microsoft SQL Server que se ejecuta en Windows Server 2008 R2, 2012 o 2012 R2 a instancias de Amazon Elastic Compute Cloud (Amazon EC2) en la nube de Amazon Web Services (AWS), se produce un error en la conexión con SQL Server y aparecen los siguientes errores:

- `[Microsoft][ODBC SQL Server Driver][DBNETLIB] General Network error`
- `ERROR [08S01] [Microsoft][SQL Native Client]Communication link failure. System.Data.SqlClient.SqlException: A transport-level error has occurred when sending the request to the server. (provider: TCP Provider, error: 0 - An existing connection was forcibly closed by the remote host.)`
- `TCP Provider: The semaphore timeout period has expired`

Este patrón describe cómo puede resolver estos errores si desactiva las características del paquete de redes escalables (SNP) de Windows en el nivel del sistema operativo (SO) y de la interfaz de red para SQL Server que se ejecuta en Windows Server 2008 R2, 2012 o 2012 R2.

Requisitos previos y limitaciones

Requisitos previos

- Privilegios de administrador para Windows Server.
- Si utilizó AWS Application Migration Service como herramienta de migración, necesitará una de las siguientes versiones de Windows Server:

  - Windows Server 2008 R2 Service Pack 1, 2012 o 2012 R2
- Si utilizó CloudEndure Migration como herramienta de migración, necesitará una de las siguientes versiones de Windows Server:
  - Windows Server 2003 R2 Service Pack 3, 2008, 2008 R2 Service Pack 1, 2012 o 2012 R2.

Herramientas

- Amazon EC2: Amazon Elastic Compute Cloud (Amazon EC2) brinda capacidad de computación escalable en la nube de AWS. Puede utilizar Amazon EC2 para lanzar tantos servidores virtuales como necesite, y puede escalar horizontalmente o reducir horizontalmente.
- Windows Server: Windows Server es una plataforma para crear una infraestructura de aplicaciones, redes y servicios web conectados.

Epics

Desactivar las características de SNP a nivel del sistema operativo y de la interfaz de red elástica

Tarea	Descripción	Habilidades requeridas
Desactive las características de SNP a nivel del sistema operativo.	1. Inicie sesión en Windows Server y abra un símbolo del sistema como administrador. 2. Ejecute el comando `netsh int tcp show global`. 3. En el resultado, compruebe si `Receive-Side Scaling` o `Chimney Offload` está en modo `enabled`. Si alguno es `enabled`, ejecute los siguientes comandos: • `netsh int tcp set global chimney=disabled`	Administrador de AWS, administrador de sistemas de AWS, ingeniero de migraciones, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	• `netsh int tcp set global rss=disabled`	
Desactive las características de SNP a nivel de la interface de red elástica.	1. Seleccione Inicio, introduzca `ncpa.cpl` y, a continuación, presione Intro. 2. Haga clic con el botón secundario en Elastic Network Adapter. 3. En el menú emergente, seleccione Properties. 4. En la ventana Ethernet Adapter Properties, seleccione Configure. 5. En la ventana emergente Amazon Elastic Network Adapter Properties, seleccione la pestaña Advanced. 6. En la sección Property, desactive todas las descargas y RSS.	Administrador de AWS, administrador de la nube, administrador de sistemas de AWS

Recursos relacionados

- Solución de problemas de características avanzadas de rendimiento de red, como RSS y NetDMA

Más patrones

- Realice copias de seguridad de los servidores Sun SPARC en el emulador Stromasys Charon-SSP en la nube de AWS
- ???
- Migre una base de datos de Microsoft SQL Server en las instalaciones a Amazon RDS para SQL Server mediante métodos nativos de copia de seguridad y restauración
- Migración de Db2 para LUW a Amazon EC2 con recuperación de desastres de alta disponibilidad
- Supervise los clústeres de SAP RHEL Pacemaker mediante los servicios de AWS
- ???
- Reinicie el agente de replicación de AWS automáticamente sin deshabilitar SELinux después de reiniciar un servidor fuente de RHEL

Operaciones

Temas

- Crear automáticamente una RFC en AMS mediante Python
- Crear una matriz RACI o RASCI para un modelo operativo en la nube
- Crear un IDE de AWS Cloud9 que utilice volúmenes de Amazon EBS con cifrado predeterminado
- Crea automáticamente CloudWatch paneles de Amazon basados en etiquetas
- Encuentre los recursos de AWS en función de su fecha de creación mediante las consultas avanzadas de AWS Config.
- Vea los detalles de la instantánea de EBS de su cuenta u organización de AWS
- Más patrones

Crear automáticamente una RFC en AMS mediante Python

Creado por Gnanasekaran Kailasam (AWS)

Entorno: producción	Tecnologías: operaciones; nativas en la nube	Servicios de AWS: AWS Managed Services

Resumen

AWS Managed Services (AMS) facilita poder operar la infraestructura basada en la nube de forma más eficiente y segura proporcionándole una gestión continua de su infraestructura de Amazon Web Services (AWS). Para realizar un cambio en su entorno administrado, debe crear y enviar una solicitud de cambio (RFC) que incluya un ID de tipo de cambio (CT) para una operación o acción concreta.

Sin embargo, la creación manual de una RFC puede tardar unos cinco minutos y es posible que los equipos de su organización tengan que enviar varias RFC todos los días. Este patrón lo ayuda a automatizar el proceso de creación de las RFC, a reducir el tiempo de creación de cada RFC y a eliminar los errores manuales.

En este patrón, se describe cómo utilizar el código Python para crear automáticamente la RFC `Stop EC2 instance` que detenga las instancias de Amazon Elastic Compute Cloud (Amazon EC2) en su cuenta de AMS. A continuación, puede aplicar el enfoque de este patrón y la automatización de Python a otros tipos de RFC.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AMS Advanced. Para obtener más información al respecto, consulte los planes de operaciones de AMS en la documentación de AWS Managed Services.
- Al menos una instancia de EC2 existente en su cuenta de AMS.
- Conocimiento de cómo crear y enviar las RFC en AMS.
- Conocimientos básicos sobre Python.

Limitaciones

- Solo puede usar los RFC para realizar cambios en su cuenta de AMS. Su cuenta de AWS utiliza procesos diferentes para realizar cambios similares.

Arquitectura

Pila de tecnología

- AMS
- Interfaz de la línea de comandos de AWS (AWS CLI)
- AWS SDK para Python (Boto3)
- Python y sus paquetes necesarios (JSON y Boto3)

Automatizar y escalar

Este patrón proporciona un código de muestra para automatizar la RFC `Stop EC2 instance`, pero puede utilizar el código y el enfoque de muestra de este patrón para otras RFC.

Herramientas

- AWS Managed Services (AMS) facilita poder utilizar la infraestructura de AWS de forma más eficiente y segura.
- AWS CLI: la interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta unificada para administrar los servicios de AWS. En AMS, la API de administración de cambios proporciona operaciones para crear y administrar las RFC.
- AWS SDK para Python (Boto3): el SDK para Python facilita la integración de su aplicación, biblioteca o script de Python con los servicios de AWS.

Código

El archivo `AMS Stop EC2 Instance.zip` (adjunto) contiene el código Python para crear una RFC `Stop EC2 instance`. También puede configurar este código para enviar un único RFC para varias instancias de EC2.

Epics

Opción 1: configurar el entorno para macOS o Linux

Tarea	Descripción	Habilidades requeridas
Instale y valide Python.	1. Abra una ventana de terminal y ejecute el comando `brew install python3`. 2. Valide que Python esté correctamente instalado ejecutando el comando `python --version` . 3. Valide que `pip` esté correctamente instalado ejecutando el comando `pip --version` .	Administrador de sistemas de AWS
Instale la CLI de AWS.	Para instalar la CLI de AWS, ejecute el comando `pip install awscli --upgrade –user` .	Administrador de sistemas de AWS
Instalación de Boto3.	Para instalar Boto3, ejecute el comando `pip install boto3`	Administrador de sistemas de AWS
Instale JSON.	Para instalar JSON, ejecute el comando `pip install json`.	Administrador de sistemas de AWS
Configure la CLI de AWS.	Inicie sesión en la consola de administración de AWS, abra la consola de AMS y, a continuación, seleccione Documentación. Descargue	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	el archivo .zip que contiene la CLI de AMS, descomprímalo e instálelo en su máquina local. Después de instalar AMS CLI, ejecute el comando `aws amscm help`. El resultado proporciona información sobre el proceso de gestión de cambios de AMS.	

Opción 2: configurar el entorno para Windows

Tarea	Descripción	Habilidades requeridas
Instale y valide Python.	1. Abra la página de Versiones de Python para Windows, descargue la última versión y, a continuación, instale Python. 2. Valide que Python esté correctamente instalado ejecutando el comando `python --version` . 3. Valide que `pip` esté correctamente instalado ejecutando el comando `pip --version` .	Administrador de sistemas de AWS
Instale la CLI de AWS.	Para instalar la CLI de AWS, ejecute el comando `pip install awscli --upgrade –user`.	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
Instalación de Boto3.	Para instalar Boto3, ejecute el comando `pip install boto3`	Administrador de sistemas de AWS
Instale JSON.	Para instalar JSON, ejecute el comando `pip install json`.	Administrador de sistemas de AWS
Configure la CLI de AWS.	Inicie sesión en la consola de administración de AWS, abra la consola de AMS y, a continuación, seleccione Documentación. Descargue el archivo .zip que contiene la CLI de AMS, descomprímalo e instálelo en su máquina local. Después de instalar AMS CLI, ejecute el comando `aws amscm help`. El resultado proporciona información sobre el proceso de gestión de cambios de AMS.	Administrador de sistemas de AWS

Extraiga el ID de CT y los parámetros de ejecución del RFC

Tarea	Descripción	Habilidades requeridas
Extraiga el ID de CT, la versión y los parámetros de ejecución del RFC	Cada RFC tiene un ID de CT, una versión y unos parámetro s de ejecución diferentes. Puede utilizar alguna de las siguientes opciones para extraer esta información:	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	1. Siga las instrucciones de la sección de Búsqueda de una solicitud de cambio (RFC) con la CLI en los Ejemplos de uso de la RFC de la documentación de AWS Managed Services. 2. Abra un RFC existente de un tipo similar o cree un RFC nuevo como prueba a través de la consola AMS. Utilice el ID de CT y los parámetros de ejecución del RFC. Para obtener más información al respecto, consulte Búsqueda de una RFC con la consola en la documentación de AWS Managed Services. Nota: Para adaptar la automatización de Python de este patrón a otras RFC, sustituya el tipo de CT y los valores de los parámetros del archivo de código Python `ams_stop_ec2_instance` del archivo `AMS Stop EC2 Instance.zip` (adjunto) por los que extrajo.	

Ejecute la automatización de Python

Tarea	Descripción	Habilidades requeridas
Ejecute la automatización de Python.	1. Descargue el archivo `AMS Stop EC2 Instance.zip` (adjunto) en el equipo local y extraiga el archivo. 2. Actualice `input_instances` con la información de su instancia EC2. 3. Abra una terminal y navegue hasta la ruta del código extraído 4. Ejecute el comando `pythonams_stop_ec2_instance.py` .	Administrador de sistemas de AWS

Recursos relacionados

- ¿Qué son los tipos de cambios?
- Tutorial de CLI: pila de dos niveles de alta disponibilidad (Linux/RHEL)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Crear una matriz RACI o RASCI para un modelo operativo en la nube

Creado por Teddy Germade (AWS), Jerome Descreux (AWS), Josselin LE MINEUR (AWS) y Florian Leroux (AWS)

Entorno: producción	Tecnologías: Operaciones; gestión y gobierno

Resumen

El centro de excelencia en la nube (CCoE) o CEE (motor de habilitación de la nube) es un equipo capacitado y responsable que se centra en la preparación operativa para la nube. Su objetivo principal es transformar la organización de TI de la información de un modelo operativo en las instalaciones a un modelo operativo en la nube. El CCoE debe ser un equipo multifuncional que incluya representantes de la infraestructura, las aplicaciones, las operaciones y la seguridad.

Uno de los componentes clave de un modelo operativo de nube es una matriz RACI o una matriz RASCI. Esto se utiliza para definir las funciones y responsabilidades de todas las partes involucradas en las actividades de migración y las operaciones en la nube. El nombre de la matriz se deriva de los tipos de responsabilidad definidos en la matriz: responsable (R), encargado (A), soporte (S), consultado (C) e informado (I). El tipo de soporte es opcional. Si la incluye, se denomina matriz RASCI y, si la excluye, se denomina matriz RACI.

Al comenzar con la plantilla adjunta, su equipo de CCoE puede crear una matriz RACI o RASCI para su organización. La plantilla contiene los equipos, las funciones y las tareas que son habituales en los modelos operativos de la nube. La base de esta matriz son las tareas relacionadas con la integración de las operaciones y las capacidades de CCoE. Sin embargo, puede personalizar esta plantilla para que se adapte a las necesidades de la estructura y el caso de uso de su organización.

La implementación de una matriz RACI no tiene límites. Este enfoque funciona para grandes organizaciones, empresas emergentes y todo lo demás. En el caso de las organizaciones pequeñas, el mismo recurso puede desempeñar varias funciones.

Epics

Crear la matriz

Tarea	Descripción	Habilidades requeridas
Identifique a las partes interesadas principales.	Identifique a los principales administradores de servicios y equipos que estén vinculados a los objetivos estratégicos de su modelo operativo de nube.	Administrador de proyectos
Personalice la plantilla de la matriz.	Descargue la plantilla en la sección de Adjuntos y, a continuación, actualice la matriz RACI o RASCI de la siguiente manera: • En la hoja de trabajo de Equipos de nube, actualice los nombres de los flujos de CCoE, los nombres de los equipos y las descripciones de los equipos según sea necesario para su organización. • En la hoja de trabajo de Roles de nube, actualice los roles, los nombres de los equipos y las descripciones de los roles según sea necesario para su organización. • En la hoja de trabajo de RASCI, actualice lo siguiente según sea	Administrador de proyectos

Tarea	Descripción	Habilidades requeridas
	necesario para su organización: • En la fila 1 y la columna A, actualice los flujos de CCoE. • En la fila 2, actualice los nombres de los equipos. • En la fila 3, actualice los nombres de los roles. • En las columnas D y E, actualice los campos y actividades generales que desee incluir en el diagrama RASCI.	
Planifique las reuniones.	1. Comunique los objetivos de la RASCI a todas las partes interesadas. 2. Planifique una o más reuniones para que pueda asistir un representante autorizado de cada equipo.	Administrador de proyectos

Tarea	Descripción	Habilidades requeridas
Complete la matriz.	En la reunión con todas las partes interesadas, haga lo siguiente: 1. Confirme que esté presente un representante de cada equipo. La participación del equipo es obligatoria para poder asignar con precisión los tipos de responsabilidad para cada tarea. 2. Revise qué es una matriz RASCI y sus objetivos con los participantes. 3. Revise el modelo de responsabilidad compartida con los participantes para que comprendan el alcance de las responsabilidades de su organización en materia de seguridad en la nube. 4. En la hoja de trabajo de RASCI, complete las columnas F a AN para cada tarea o actividad para asignar los siguientes tipos de responsabilidad: • Responsable (R) – Este rol es responsable de realizar el trabajo para completar la tarea. • Encargado (A) – Este rol es el encargado de garantizar que la tarea se	Administrador de proyectos

Tarea	Descripción	Habilidades requeridas
	complete. Esta función también es responsab le de garantizar que se cumplan los requisitos previos y de delegar la tarea a los responsables. • Soporte (S) – Este rol ayuda a los responsab les a completar la tarea. Este tipo de responsab ilidad es opcional y puede optar por excluirlo para crear una matriz RACI más tradicional. • Consultado (C) – Se debe consultar a este rol para obtener opiniones o experiencia sobre la tarea. Dependiendo de la tarea, es posible que este tipo de responsabilidad no sea obligatorio. • Informado (I) – Se debe mantener informado a este rol sobre el progreso de la tarea y se le debe notificar cuando se complete la tarea. • En blanco – Este rol no está involucrado en la actividad o tarea.	

Tarea	Descripción	Habilidades requeridas
Comparta la matriz RASCI.	Cuando la matriz RACI o RASCI esté completa, haga que los líderes la aprueben. Guárdela en un repositorio compartido o en una ubicación central donde todas las partes interesadas puedan acceder a ella. Le recomendamos que utilice procesos de control de documentos estándar para registrar y aprobar las revisiones de la matriz.	Administrador de proyectos

Recursos relacionados

- Modelo de responsabilidad compartida de AWS

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Crear un IDE de AWS Cloud9 que utilice volúmenes de Amazon EBS con cifrado predeterminado

Creado por Janardhan Malyala (AWS) y Dhrubajyoti Mukherjee (AWS)

Entorno: producción	Tecnologías: operaciones	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: AWS Cloud9; AWS KMS		

Resumen

Puede utilizar el cifrado predeterminado para reforzar el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS) y de las copias de instantáneas en la nube de Amazon Web Services (AWS).

Puede crear un entorno de desarrollo integrado (IDE) de AWS Cloud9 que utilice volúmenes de EBS con cifrado predeterminado. Sin embargo, el rol vinculado al servicio de AWS Identity and Access Management (IAM) de AWS Cloud9 requiere acceso a la clave del AWS Key Management Service (AWS KMS) para estos volúmenes de EBS. Si no se proporciona acceso, el IDE de AWS Cloud9 podría no lanzarse y la depuración podría ser difícil.

Este patrón proporciona los pasos para agregar el rol vinculado al servicio de AWS Cloud9 a la clave de AWS KMS que utilizan los volúmenes de EBS. La configuración descrita en este patrón ayuda a crear y lanzar correctamente un IDE que utilice volúmenes de EBS con cifrado predeterminado.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Cifrado predeterminado activado para los volúmenes de EBS. Para obtener más información sobre el cifrado predeterminado, consulte Cifrado de Amazon EBS en la documentación de Amazon Elastic Compute Cloud (Amazon EC2).
- Una clave KMS existente administrada por el cliente para cifrar los volúmenes de EBS.

Nota: no se necesita crear un rol vinculado al servicio para AWS Cloud9. Al crear un entorno de desarrollo de AWS Cloud9, es AWS Cloud9 el que crea el rol vinculado al servicio.

Arquitectura

Pila de tecnología

- AWS Cloud9
- IAM
- AWS KMS

Herramientas

- AWS Cloud9 es un entorno de desarrollo integrado (IDE) que ayuda a codificar, crear, ejecutar, probar y depurar software. También ayuda a lanzar software a la nube de AWS.
- Amazon Elastic Block Store (Amazon EBS) proporciona volúmenes de almacenamiento por bloques para su uso con instancias de Amazon Elastic Compute Cloud (Amazon EC2).
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Key Management Service (AWS KMS) facilita poder crear y controlar claves criptográficas para proteger los datos.

Epics

Buscar el valor de la clave de cifrado predeterminado

Tarea	Descripción	Habilidades requeridas
Registre el valor de la clave de cifrado predeterminado para los volúmenes de EBS.	Inicie sesión en la consola de administración de AWS y abra la consola de Amazon EC2. Elija el panel de control de EC2 y, a continuación,	Arquitecto e ingeniero de nube DevOps

Tarea	Descripción	Habilidades requeridas
	elija Protección y seguridad de datos en los atributos de la cuenta. En la sección de cifrado de EBS, copie y registre el valor de la clave de cifrado predeterminada.	

Proporcionar acceso a la clave de AWS KMS

Tarea	Descripción	Habilidades requeridas
Proporcione a AWS Cloud9 acceso a la clave de KMS para los volúmenes de EBS.	1. Abra la consola de AWS KMS y, a continuación, seleccione Customer managed keys (Claves administradas por el cliente). Seleccione la clave de AWS KMS utilizada para el cifrado de Amazon EBS y, a continuación, View key (Ver clave). 2. En la pestaña Key policy (Política de claves), confirme que puede ver el texto de la política de claves. Si no puede ver el formulario de texto, seleccione Change to policy view (Cambiar a la vista de políticas). 3. Elija Editar. Agregue el código que aparece en la sección de información adicional a la política y, a	Arquitecto de nube, DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	continuación, seleccione Save changes (Guardar cambios). Los cambios en la política permiten que la función vinculada al servicio de AWS Cloud9, `AWSServiceRoleForAWSCloud9` , acceda a la clave. Para obtener más información sobre la actualización de una política de claves, consulte How to change a key policy (Cómo cambiar una política de claves) en la documentación de AWS KMS. Importante: El rol vinculado al servicio para AWS Cloud9 se crea automáticamente al lanzar el primer IDE. Para obtener más información, consulte Creating a service-linked role (Crear un rol vinculado a un servicio) en la documentación de AWS Cloud9.	

Crear y lanzar el IDE

Tarea	Descripción	Habilidades requeridas
Cree e inicie el IDE de AWS Cloud9.	Abra la consola de AWS Cloud9 y seleccione Create environment (Crear entorno). Configure el IDE según sus requisitos siguiendo los pasos de Creating an EC2 environment (Crear un entorno EC2) de la documentación de AWS Cloud9.	Arquitecto de nube, DevOps ingeniero

Recursos relacionados

- Encrypt EBS volumes used by AWS Cloud9 (Cifrar los volúmenes de EBS utilizados por AWS Cloud9)
- Create a service-linked role for AWS Cloud9 (Crear un rol vinculado a un servicio para AWS Cloud9)
- Create an EC2 environment in AWS Cloud9 (Crear un entorno de EC2 en AWS Cloud9)

Información adicional

Actualizaciones de las políticas de clave de AWS KMS

Sustituya `<aws_accountid>` por el ID de la cuenta de AWS.

```
{
            "Sid": "Allow use of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::<aws_accountid>:role/aws-service-role/
cloud9.amazonaws.com/AWSServiceRoleForAWSCloud9"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
```

```
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow attachment of persistent resources",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::<aws_accountid>:role/aws-service-role/
cloud9.amazonaws.com/AWSServiceRoleForAWSCloud9"
            },
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                }
            }
        }
```

Uso de una clave multicuenta

Si quiere utilizar una clave de KMS multicuenta, debe utilizar una concesión en combinación con la política de claves de KMS. Esto permite el acceso multicuenta a la clave. En la misma cuenta que utilizó para crear el entorno Cloud9, ejecute el siguiente comando en la terminal.

```
aws kms create-grant \
 --region <Region where Cloud9 environment is created> \
 --key-id <The cross-account KMS key ARN> \
 --grantee-principal arn:aws:iam::<The account where Cloud9 environment is
 created>:role/aws-service-role/cloud9.amazonaws.com/AWSServiceRoleForAWSCloud9 \
 --operations "Encrypt" "Decrypt" "ReEncryptFrom" "ReEncryptTo" "GenerateDataKey"
 "GenerateDataKeyWithoutPlaintext" "DescribeKey" "CreateGrant"
```

Tras ejecutar este comando, puede crear entornos de Cloud9 mediante el cifrado de EBS con una clave de otra cuenta.

Crea automáticamente CloudWatch paneles de Amazon basados en etiquetas

Creado por Janak Vadaria (AWS), RAJNEESH TYAGI (AWS) y Vinodkumar Mandalapu (AWS)

Repositorio de código: Goldensignals	Entorno: producción	Tecnologías: operaciones; nativas de la nube; administración y gobierno
Servicios de AWS: AWS CDK; Amazon CloudWatch; AWS CodeBuild; AWS CodePipeline		

Resumen

Crear diferentes CloudWatch paneles de Amazon de forma manual puede llevar mucho tiempo, especialmente cuando hay que crear y actualizar varios recursos para escalar automáticamente el entorno. Una solución que cree y actualice sus CloudWatch paneles automáticamente puede ahorrarle tiempo. Este patrón le ayuda a implementar un proceso totalmente automatizado que AWS Cloud Development Kit (AWS CDK) crea y actualiza CloudWatch paneles para sus AWS recursos en función de los eventos de cambio de etiquetas, para mostrar las métricas de Golden Signals.

En la ingeniería de confiabilidad de sitios (SRE), Golden Signals se refiere a un conjunto integral de métricas que ofrecen una visión amplia de un servicio desde la perspectiva del usuario o del consumidor. Estas métricas se componen de la latencia, el tráfico, los errores y la saturación. Para obtener más información, consulte ¿Qué es la ingeniería de confiabilidad del sitio (SRE)? en el AWS sitio web.

La solución que proporciona este patrón se basa en eventos. Una vez implementada, monitorea continuamente los eventos de cambio de etiqueta y actualiza automáticamente los CloudWatch paneles y las alarmas.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS

- AWS Command Line Interface (AWS CLI), instalado y configurado
- Requisitos previos para la versión 2 AWS CDK
- Un entorno de arranque en AWS
- Python versión 3
- AWS SDK para Python (Boto3), instalado
- Node.js, versión 18 o posterior
- El administrador de paquetes de nodos (npm), instalado y configurado para AWS CDK
- Familiaridad moderada (nivel 200) con el y AWS CDK AWS CodePipeline

Limitaciones

Actualmente, esta solución crea paneles automatizados únicamente para los siguientes servicios de AWS:

- Amazon Relational Database Service (Amazon RDS)
- AWS Auto Scaling
- Amazon Simple Notification Service (Amazon SNS)
- Amazon DynamoDB
- AWS Lambda

Arquitectura

Pila de tecnología de destino

- CloudWatch paneles
- CloudWatch alarmas

Arquitectura de destino

1. Un evento de cambio de AWS etiqueta para las etiquetas de la aplicación configuradas o los cambios de código inicia una canalización AWS CodePipeline para crear e implementar paneles actualizados. CloudWatch

2. AWS CodeBuild ejecuta un script de Python para buscar los recursos que tienen etiquetas configuradas y almacena los ID de los recursos en un archivo local de un CodeBuild entorno.
3. CodeBuild ejecuta cdk synth para generar AWS CloudFormation plantillas que despliegan CloudWatch paneles y alarmas.
4. CodePipeline despliega las AWS CloudFormation plantillas en la región y especificadas. Cuenta de AWS
5. Cuando la AWS CloudFormation pila se haya desplegado correctamente, podrá ver los CloudWatch paneles y las alarmas.

Automatizar y escalar

Esta solución se ha automatizado mediante el uso de AWS CDK. Puedes encontrar el código en el CloudWatch repositorio de GitHub Golden Signals Dashboards en Amazon. Para un escalado adicional y para crear paneles personalizados, puede configurar varias claves y valores de etiquetas.

Herramientas

Servicios de Amazon

- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes, incluidas AWS Lambda funciones, puntos de enlace de invocación HTTP que utilizan destinos de API o buses de eventos, entre otros. Cuentas de AWS
- AWS CodePipelinele ayuda a modelar y configurar rápidamente las diferentes etapas de una versión de software y a automatizar los pasos necesarios para publicar los cambios de software de forma continua.
- AWS CodeBuildes un servicio de compilación totalmente gestionado que le ayuda a compilar el código fuente, ejecutar pruebas unitarias y producir artefactos listos para su despliegue.
- AWS CodeCommites un servicio de control de versiones que te ayuda a almacenar y gestionar de forma privada los repositorios de Git sin necesidad de gestionar tu propio sistema de control de código fuente.
- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que le ayuda a interactuar con los servicios de AWS mediante comandos en su shell de línea de comandos.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Prácticas recomendadas

Como práctica recomendada de seguridad, puedes usar el cifrado y la autenticación para los repositorios de origen que se conectan a tus canalizaciones. Para obtener más información sobre las prácticas recomendadas, consulta las CodePipeline mejores prácticas y los casos de uso en la CodePipeline documentación.

Epics

Configure e implemente la aplicación de muestra

Tarea	Descripción	Habilidades requeridas
Configure e implemente la aplicación de muestra.	1. Clone el repositorio de código de GitHub muestra mediante el comando: `git clone https://github.com/aws-samples/golden-signals-dashboards-sample-app` 2. Navegue hasta el repositorio clonado de su ordenador y abra el `src/project-settings.ts` archivo con el editor que prefiera. 3. Cambie el valor `projectSettings` constante de acuerdo con las etiquetas de sus AWS recursos y las asignaciones de aplicaciones.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	4. Establezca las `AWS_ACCOUNT` variables`AWS_REGION`, y de `GS_DASHBOARD_INSTANCE` entorno: • `AWS_ACCOUNT` Establézcalo en el ID de cuenta de tu AWS cuenta. • `AWS_REGION` Configúrelo en la región en la que desea implementar la aplicación de muestra. • `GS_DASHBOARD_INSTANCE` `devtest`Configúrelo en`prod`, o, según su entorno de desarrollo. (Lo recomendamos `test` para el procedimiento de prueba descrito en este patrón). 5. Configúrelo AWS CLI con sus AWS credenciales. Para obtener más información, consulte Establecer y ver los valores de configuración mediante los comandos de la AWS CLI documentación. 6. Ejecute el siguiente comando para implementar la aplicación de ejemplo del panel de control Golden Signals:	

Tarea	Descripción	Habilidades requeridas
	`sh deploy.sh`	

Tarea	Descripción	Habilidades requeridas
Cree paneles y alarmas automáticamente.	Tras implementar la aplicación de ejemplo, puede crear cualquiera de los recursos compatibles con esta solución con los valores de etiqueta esperados, lo que creará automáticamente los cuadros de mando y las alarmas especificados. Para probar esta solución, cree una AWS Lambda función: 1. Inicie sesión AWS Management Console en el Región de AWS lugar donde implementó la aplicación de muestra. 2. Abra la consola en https://console.aws.amazon.com/lambda/. 3. Seleccione Crear una función y, a continuación, introduzca el nombre de la función. 4. En el panel de configuración avanzada, seleccione Habilitar etiquetas y, a continuación, elija Agregar nueva etiqueta. Introduzca la clave y el valor siguientes:	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	• Clave: `AutoDashboard` • Valor: `True` 5. Elija Crear función. La función Lambda inicia inmediatamente una canalización de código, que crea automáticamente los cuadros de mando y las alarmas para esa función Lambda concreta. 6. Para ver los paneles y las alarmas automatizados, abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/. Puede ver los paneles y las alarmas personalizados de la función que especificó en la `projectSettings` constante (APP1-Lambda de forma predeterminada). 7. Seleccione el panel de control de la función Lambda para ver los paneles automatizados adicionales que se crearon como parte de esta solución. 8. Repita estos pasos para otros servicios, como Amazon RDS, Amazon SNS y DynamoDB AWS	

Tarea	Descripción	Habilidades requeridas
	Auto Scaling, para generar los paneles asociados. Para ver un ejemplo de Amazon RDS, consulte la sección de información adicional.	

Elimine la aplicación de muestra

Tarea	Descripción	Habilidades requeridas
Extraiga el `golden-signals-dashboard` constructo.	1. Para eliminar todas las AWS CloudFormation pilas creadas por la aplicación de ejemplo, debe volver a configurar las variables `AWS_ACCOUNT` de `GS_DASHBOARD_INSTANCE` entorno y. `AWS_REGION` El `destroy.sh` comando requiere estas configuraciones. • `AWS_ACCOUNT` es el identificador de su AWS cuenta. • `AWS_REGION` es la región en la que implementó su aplicación de muestra. • `GS_DASHBOARD_INSTANCE` es `devtest`, o`prod`, se basa en su configuración anterior.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	2. Configúrelo AWS CLI con sus AWS credenciales. 3. Ejecute el siguiente comando para eliminar la aplicación de muestra y todas las AWS CloudForm ation pilas asociadas: `sh destroy.sh`	

Resolución de problemas

Problema	Solución
No se encontró el comando de Python (en referencia a `findresources.sh` la línea 8).	Comprueba la versión de tu instalación de Python. Si ha instalado la versión 3 de Python, `python` `python3` sustitúyala por la línea 8 del `resources.sh` archivo y vuelva a ejecutar el `sh deploy.sh` comando para implementar la solución.

Recursos relacionados

- Bootstrapping (documentación)AWS CDK
- Uso de perfiles con nombre asignado (documentación)AWS CLI
- AWS CDK Taller

Información adicional

La siguiente ilustración muestra un panel de ejemplo para Amazon RDS que se crea como parte de esta solución.

Encuentre los recursos de AWS en función de su fecha de creación mediante las consultas avanzadas de AWS Config.

Creado por Inna Saman (AWS)

Entorno: producción	Tecnologías: operaciones; Seguridad, identidad y conformidad	Servicios de AWS: AWS Config; Amazon EBS; Amazon EC2; Amazon S3; AWS Lambda

Resumen

Este patrón muestra cómo encontrar recursos de AWS en función de su fecha de creación mediante la característica de consultas avanzadas de AWS Config.

Las consultas avanzadas de AWS Config utilizan un subconjunto de SQL para consultar el estado de configuración de los recursos de AWS para la gestión del inventario, la inteligencia operativa, la seguridad y la conformidad. Puede utilizar estas consultas para buscar recursos de AWS en una sola cuenta de AWS y región de AWS o en varias cuentas y regiones. Al ejecutar una consulta que utilice la resourceCreationTimepropiedad, puede devolver una lista de sus recursos de AWS en función de su fecha de creación específica. Puede ejecutar consultas avanzadas de AWS Config utilizando cualquiera de las siguientes opciones:

- El editor de consultas de AWS Config de la consola de AWS Config
- La interfaz de la línea de comandos de AWS (AWS CLI)

La consulta de ejemplo de la sección Additional information (Información adicional) de este patrón devuelve una lista de los recursos de AWS creados en un período específico de 60 días. El resultado de la consulta incluye información sobre lo siguiente para cada recurso identificado:

- ID de cuenta
- Región
- Nombre del recurso
- ID de recurso

- Tipo de recurso
- Etiquetas
- Hora de creación

La consulta de ejemplo también muestra cómo se puede ajustar la lista de inventario a tipos de recursos específicos con la opción «WHERE... Instrucción IN". Puede utilizar una consulta similar para buscar otros tipos de recursos de AWS que también funcionen con etiquetas.

Nota: Para consultar recursos en varias cuentas y regiones de AWS o en una organización de AWS Organizations, debe usar un agregador de AWS Config. Para obtener más información, consulte Agregación de datos de varias cuentas y regiones en la Guía del desarrollador de AWS Config. Los recursos globales se registran únicamente en su región de origen. Por ejemplo, AWS Identity and Access Management (IAM) es un recurso global y está registrado en us-east-1 (región de Virginia del Norte).

Requisitos previos y limitaciones

Requisitos previos

- Una o más cuentas de AWS activas con AWS Config activado para registrar todos los tipos de recursos compatibles (configuración predeterminada)
- (Para consultas de varias cuentas y varias regiones) Un agregador de AWS Config activado

Limitaciones

- Los resultados de las consultas avanzadas de AWS Config están paginados. Al elegir exportar, se exportan hasta 500 resultados desde la consola de administración de AWS. También puede usar las API para recuperar hasta 100 resultados paginados a la vez.
- Las consultas avanzadas de AWS Config utilizan un subconjunto de SQL que tiene sus propias limitaciones de sintaxis. Para obtener más información, consulte Limitaciones a la hora de Consultar el estado de configuración actual de los recursos de AWS en la Guía para desarrolladores de AWS Config.

Herramientas

Herramientas

- AWS Config brinda una visión detallada de la configuración de los recursos de AWS y de cómo están configurados. Lo ayuda a identificar cómo se relacionan los recursos entre sí y cómo han cambiado sus configuraciones a lo largo del tiempo.
- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de la línea de comandos.

Epics

Ejecute una consulta avanzada de AWS Config

Tarea	Descripción	Habilidades requeridas
Compruebe que los recursos consultados son compatibles con AWS Config.	Para obtener una lista completa de los recursos de AWS compatibles con AWS Config, consulte los Tipos de recursos compatibles en la Guía para desarrolladores de AWS Config.	Administrador de la nube
Verifique que el registrador de configuración está creado y en funcionamiento.	Siga las instrucciones de Administrar el registrador de configuración de la Guía para desarrolladores de AWS Config. Nota: AWS Config crea automáticamente y luego inicia el registrador de configuración predeterminado.	Administrador de la nube
Ejecute la consulta.	Siga las instrucciones de Consultas con el editor de consultas SQL (consola) o Consultas con el editor de consultas SQL (AWS CLI) de	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	la Guía para desarrolladores de AWS Config. Nota: Si recibe errores al ejecutar los comandos de la CLI de AWS, asegúrese de utilizar la versión más reciente de la CLI de AWS. Para consultas de cuenta y región de AWS únicas En la página del Query editor (Editor de consultas), en la sección Query scope (Alcance de la consulta), asegúrese de elegir Solo esta cuenta y región. Para consultas de varias cuentas y varias regiones En la página del Query editor (Editor de consultas), en la sección Query scope (Alcance de la consulta), asegúrese de crear y seleccionar un agregador de AWS Config. Para obtener más informaci ón, consulte Agregar datos de varias cuentas y regiones en la Guía del desarrollador de AWS Config. Si las consultas en varias cuentas o regiones no funcionan, siga las instrucci	

Tarea	Descripción	Habilidades requeridas
	ones de Solución de problemas relacionados con la agregación de datos de varias cuentas y regiones de la Guía para desarrolladores de AWS Config. Nota: Para modificar el ámbito de la consulta en función del tipo de recurso, utilice el constructo WHERE resourceType IN (…). Para ver un ejemplo de consulta, consulte el Ejemplo de consulta avanzada de AWS Config en la sección Additional information (Información adicional).	

Información adicional

Ejemplo de consulta avanzada de AWS Config

La consulta de ejemplo de la sección Additional information (Información adicional) de este patrón devuelve una lista de los recursos de AWS creados en un período específico de 60 días. Para ver más ejemplos de consultas avanzadas de AWS Config, consulte Ejemplos de consultas en la Guía para desarrolladores de AWS Config.

```
SELECT
  accountId,
  awsRegion,
  resourceName,
  resourceId,
  resourceType,
  resourceCreationTime,
  tags
WHERE
  resourceType IN (
```

```
    'AWS::CloudFormation::Stack',
    'AWS::EC2::VPC',
    'AWS::EC2::Volume',
    'AWS::EC2::Instance',
    'AWS::RDS::DBInstance',
    'AWS::ElasticLoadBalancingV2::LoadBalancer',
    'AWS::ServiceCatalog::CloudFormationProvisionedProduct',
    'AWS::EC2::NetworkInterface',
    'AWS::EC2::Subnet',
    'AWS::EC2::SecurityGroup',
    'AWS::AutoScaling::AutoScalingGroup',
    'AWS::Lambda::Function',
    'AWS::DynamoDB::Table',
    'AWS::S3::Bucket'
  )
  AND resourceCreationTime BETWEEN '2022-05-23T00:00:00.000Z' AND
 '2022-07-23T17:59:51.000Z'
ORDER BY
  accountId ASC,
  resourceType ASC
```

Protección y privacidad de datos

AWS Config se activa en cada región de AWS por separado. Para cumplir con los requisitos reglamentarios, es necesario tener en cuenta consideraciones especiales como la creación de agregadores regionales independientes. Para obtener más información, consulte Protección de datos en AWS Config en la Guía para desarrolladores de AWS Config.

Permisos de IAM

Se requiere la política administrada de AWS_ ConfigRole AWS como conjunto mínimo de permisos para ejecutar consultas avanzadas de AWS Config. Para obtener más información, consulte Política de rol de IAM para obtener detalles de configuración en la sección Permisos para el rol de IAM asignado a AWS Config de la Guía para desarrolladores de AWS Config.

Vea los detalles de la instantánea de EBS de su cuenta u organización de AWS

Entorno: producción	Tecnologías: operaciones, almacenamiento y copia de seguridad	Servicios de AWS: Amazon EBS

Resumen

Este patrón describe cómo puede generar automáticamente un informe bajo demanda de todas las instantáneas de Amazon Elastic Block Store (Amazon EBS) de su cuenta de Amazon Web Services (AWS) o unidad organizativa (OU) en AWS Organizations.

Amazon EBS es un easy-to-use servicio de almacenamiento en bloques escalable y de alto rendimiento diseñado para Amazon Elastic Compute Cloud (Amazon EC2). Un volumen de EBS proporciona un almacenamiento duradero y persistente que se puede adjuntar a sus instancias EC2. Puede utilizar los volúmenes de EBS como almacenamiento principal para sus datos y realizar una point-in-time copia de seguridad de los volúmenes de EBS mediante la creación de una instantánea. Puede utilizar la Consola de administración de AWS o la Interfaz de la línea de comandos de AWS (AWS CLI) para ver los detalles de instantáneas de EBS específicas. Este patrón proporciona una forma programática de recuperar información sobre todas las instantáneas de EBS de su cuenta o unidad organizativa de AWS.

Puede usar el script que proporciona este patrón para generar un archivo de valores separados por comas (CSV) que contenga la siguiente información sobre cada instantánea: Identificador de cuenta, Identificador de instantánea, Identificador de volumen y tamaño, fecha en que se tomó la instantánea, Identificador de instancia y descripción. Si las instantáneas de EBS están etiquetadas, el informe también incluye los atributos del propietario y del equipo.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Instalación y configuración de la versión 2 de AWS CLI

- Rol de AWS Identity and Access Management (IAM) con los permisos adecuados (permisos de acceso para una cuenta específica o para todas las cuentas de una OU si planea ejecutar el script desde AWS Organizations)

Arquitectura

El siguiente diagrama muestra el flujo de trabajo del script que genera un informe bajo demanda de las instantáneas de EBS distribuidas en varias cuentas de AWS de una OU.

Herramientas

Servicios de AWS

- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.
- Amazon Elastic Block Store (Amazon EBS) brinda volúmenes de almacenamiento por bloques para su uso con instancias de EC2.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Organizations es un servicio de administración de cuentas que le permite agrupar varias cuentas de AWS en una organización que usted crea y administra de manera centralizada.

Código

El código de la aplicación de ejemplo utilizada en este patrón está disponible en el repositorio GitHub aws-ebs-snapshots-awsorganizations. Siga las instrucciones de la siguiente sección para utilizar los archivos de muestra.

Epics

Descargue el script

Tarea	Descripción	Habilidades requeridas
Descargar el script Python.	GetSnapshotDetails AllDescargue GitHub el script AccountsOU.py del repositor io.	AWS general

Obtenga los detalles de las instantáneas de EBS para una cuenta de AWS

Tarea	Descripción	Habilidades requeridas
Ejecute el script de Python.	Ejecute el comando: `python3 getsnapsh otinfo.py --file <output-file>.csv --region <region-name>` donde `<output-file>` se refiere al archivo de salida CSV en el que desea que se coloque la información sobre las instantáneas de EBS y `<region-name>` es la región de AWS en la que se almacenan las instantáneas. Por ejemplo: `python3 getsnapsh otinfo.py --file snapshots.csv --region us-east-1`	AWS general

Obtenga los detalles de las instantáneas de EBS de una organización

Tarea	Descripción	Habilidades requeridas
Ejecute el script de Python.	Ejecute el comando: `python3 getsnapsh otinfo.py --file <output-file>.csv --role <IAM-role> --region <region-name>` donde `<output-file>` se refiere al archivo de salida CSV en el que desea que se coloque la información sobre las instantáneas de EBS, `<IAM-role>` es una función que proporciona permisos para acceder a AWS Organizations y `<region-name>` es la región de AWS en la que se almacenan las instantáneas. Por ejemplo: `python3 getsnapsh otinfo.py --file snapshots.csv --role <IAM role> --region us-west-2`	AWS general

Recursos relacionados

- Documentación de Amazon EBS
- Acciones de Amazon EBS
- Referencia de EBS API

- Mejorar el rendimiento de Amazon EBS
- Recursos de Amazon EBS
- Precios de las instantáneas de EBS

Información adicional

Tipos de instantáneas de EBS

Amazon EBS ofrece tres tipos de instantáneas, según la propiedad y el acceso:

- De su propiedad: de manera predeterminada, solo usted puede crear volúmenes de instantáneas que sean de su propiedad.
- Instantáneas públicas: puede compartir las instantáneas públicamente con todas las demás cuentas de AWS. Para crear una instantánea pública, modifique los permisos de la instantánea para compartirla con las cuentas de AWS que especifique. Los usuarios que autorice podrán usar las instantáneas que comparta para crear sus propios volúmenes de EBS, mientras que la instantánea original se mantendrá sin cambios. Puede también poner las instantáneas no cifradas a disposición del público para todos los usuarios de AWS. Sin embargo, no puede poner sus instantáneas cifradas a disposición del público por razones de seguridad. Las instantáneas públicas representan un riesgo de seguridad importante debido a la posibilidad de exponer datos personales y confidenciales. Recomendamos encarecidamente no compartir las instantáneas de EBS con todas las cuentas de AWS. Para obtener más información acerca de cómo compartir instantáneas, consulte la documentación de AWS.
- Instantáneas privadas: puede compartir instantáneas de forma privada con las cuentas de AWS individuales que especifique. Para compartir la instantánea de forma privada con cuentas de AWS específicas, siga las instrucciones de la documentación de AWS y elija Privado en la configuración de permisos. Los usuarios que autorice podrán usar las instantáneas que comparta para crear sus propios volúmenes de EBS, mientras que la instantánea original se mantendrá sin cambios.

Resúmenes y procedimientos

La siguiente tabla proporciona enlaces a más información sobre las instantáneas de EBS, incluida la forma de reducir los costos de volumen de EBS mediante el resultado y eliminación de las instantáneas no utilizadas, y de archivar las instantáneas a las que se accede con poca frecuencia y que no requieren una recuperación rápida o frecuente.

Para obtener más información	Consulte
Las instantáneas, sus características y limitaciones	Crear instantáneas de Amazon EBS
Cómo crear una instantánea	Consola: Crear una instantánea AWS CLI: comando create-snapshot Por ejemplo: `aws ec2 create-snapshot --volume-id vol-1234567890abcdef0 --description " volume snapshot"`
Eliminar instantáneas (información general)	Eliminar una instantánea de Amazon EBS
Cómo eliminar una instantánea	Consola: Eliminar una instantánea AWS CLI: comando delete-snapshot Por ejemplo: `aws ec2 delete-snapshot --snapshot-id snap-1234567890abcdef0`
Archivado de instantáneas (información general)	Archivar instantáneas de Amazon EBS Archivo de instantáneas de Amazon EBS (publicación de blog)
Cómo archivar una instantánea	Consola: Archivar una instantánea AWS CLI: modify-snapshot-tier comando
¿Cómo recuperar una instantánea archivada?	Consola: restaurar una instantánea archivada AWS CLI: restore-snapshot-tier comando
Precios de las instantáneas	Precios de Amazon EBS

PREGUNTAS FRECUENTES

¿Cuál es el periodo de archivo mínimo?

El periodo de archivo mínimo es de 90 días.

¿Cuánto tardaría en restaurarse una instantánea archivada?

Puede tardar hasta 72 horas en restaurar una instantánea archivada del nivel de archivo al nivel estándar, según el tamaño de la instantánea.

¿Las instantáneas archivadas son siempre instantáneas completas?

Las instantáneas archivadas siempre son instantáneas completas.

¿Qué instantáneas puede archivar un usuario?

Solo puede archivar instantáneas que posea en su cuenta.

¿Se puede archivar una instantánea del volumen de dispositivo raíz de una Imagen de máquina de Amazon (AMI) registrada?

No. No puede archivar una instantánea del volumen de dispositivo raíz de una AMI registrada.

¿Cuáles son las consideraciones de seguridad al compartir una instantánea?

Cuando comparte una instantánea, concede a otras personas acceso a todos los datos de la instantánea. Comparta instantáneas solo con aquellas personas en las que confíe sus datos.

¿Cómo se comparte una instantánea con otra región de AWS?

Las instantáneas están restringidas a la región en la que se han creado. Para compartir una instantánea con otra región, copie la instantánea en dicha región y, luego, comparta la copia.

¿Puede compartir instantáneas cifradas?

No puede compartir instantáneas que estén cifradas con la clave administrada de AWS predeterminada. Solo puede compartir instantáneas que estén cifradas con una clave administrada por el cliente. Cuando comparta una instantánea cifrada, también deberá compartir la clave administrada por el cliente usada para cifrar la instantánea.

¿Qué pasa con las instantáneas sin cifrar?

Puede compartir instantáneas sin cifrar de forma pública.

Más patrones

- Permitir a las instancias de EC2 el acceso de escritura a los buckets de S3 en las cuentas de AMS
- Automatice la evaluación de recursos de AWS
- Automatizar los escaneos de seguridad para cargas de trabajo entre cuentas mediante Amazon Inspector y AWS Security Hub
- ???
- Cree un flujo de trabajo de MLOps mediante Amazon SageMaker y Azure DevOps
- Centralice la supervisión mediante Amazon CloudWatch Observability Access Manager
- Configure el registro y la supervisión de eventos de seguridad en su entorno de AWS IoT
- Conectarse a una instancia de Amazon EC2 mediante el uso de Session Manager
- Cree alarmas para métricas personalizadas mediante la detección de CloudWatch anomalías de Amazon
- ???
- Mejore el rendimiento operativo al habilitar Amazon DevOps Guru en varias regiones, cuentas y unidades organizativas de AWS con la AWS CDK
- Incorporar y migrar instancias de Windows de EC2 a una cuenta de AWS Managed Services
- Instale el agente SSM y el CloudWatch agente en los nodos de trabajo de Amazon EKS mediante preBootstrapCommands
- Integrar el controlador universal Stonebranch con AWS Mainframe Modernization
- Lance un CodeBuild proyecto en todas las cuentas de AWS mediante Step Functions y una función de proxy Lambda
- Supervisar y corregir la eliminación programada de las claves de AWS KMS
- Supervisar el uso de una imagen de máquina de Amazon compartida en varias cuentas de AWS
- Ejecute las tareas de AWS Systems Manager Automation de forma sincrónica desde AWS Step Functions
- Ejecute cargas de trabajo programadas y basadas en eventos a escala con AWS Fargate.
- Configure la detección de CloudFormation desviaciones de AWS en una organización multirregional y multicuenta
- Configurar la recuperación de desastres para SAP en IBM Db2 en AWS
- Etiquete automáticamente las conexiones de puerta de enlace de tránsito con AWS Organizations
- Vea los registros y las métricas de AWS Network Firewall mediante Splunk

SaaS

Temas

Administrar los inquilinos de varios productos SaaS en un único plano de control

Creado por Ramanna Avancha (AWS), Jenifer Pascal (AWS), Kishan Kavala (AWS) y Anusha Mandava (AWS)

Entorno: PoC o piloto	Tecnologías: SaaS	Servicios de AWS: Amazon API Gateway; Amazon Cognito; AWS Lambda; AWS Step Functions; Amazon DynamoDB

Resumen

Este patrón muestra cómo gestionar los ciclos de vida de los inquilinos en varios productos de software como servicio (SaaS) en un único plano de control en la nube de AWS. La arquitectura de referencia proporcionada puede ayudar a las organizaciones a reducir la implementación de características redundantes y compartidas en sus productos SaaS individuales y a proporcionar eficiencias de gobierno a escala.

Las grandes empresas pueden tener varios productos SaaS en varias unidades de negocio. A menudo, estos productos deben aprovisionarse para que los utilicen inquilinos externos con diferentes niveles de suscripción. Sin una solución de inquilino común, los administradores de TI deben dedicar tiempo a administrar características indiferenciadas en varias API de SaaS, en lugar de centrarse en el desarrollo de las características principales del producto.

La solución de inquilino común que se proporciona en este patrón puede ayudar a centralizar la administración de muchas de las características de los productos SaaS compartidos de una organización, incluidas las siguientes:

- Seguridad
- Aprovisionamiento de inquilinos
- Almacenamiento de datos del inquilino
- Comunicaciones con los inquilinos

- Gestión de productos
- Registro y supervisión de métricas

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Conocimiento de Amazon Cognito o de un proveedor de identidades (IdP) externo
- Conocimiento de Amazon API Gateway
- Conocimiento de AWS Lambda
- Conocimiento de Amazon DynamoDB
- Conocimientos de AWS Identity and Access Management (IAM)
- Conocimiento de AWS Step Functions
- Conocimientos de AWS CloudTrail y Amazon CloudWatch
- Conocimiento de las bibliotecas y el código de Python
- Conocimiento de las API de SaaS, incluyendo los diferentes tipos de usuarios (organizaciones, inquilinos, administradores y usuarios de aplicaciones), los modelos de suscripción y los modelos de aislamiento de inquilinos
- Conocimiento de los requisitos de SaaS multiproducto y de las suscripciones multiusuario de su organización

Limitaciones

- Las integraciones entre la solución de inquilino común y los productos SaaS individuales no se incluyen en este patrón.
- Este patrón implementa el servicio Amazon Cognito únicamente en una sola región de AWS.

Arquitectura

Pila de tecnología de destino

- Amazon API Gateway
- Amazon Cognito

- AWS CloudTrail
- Amazon CloudWatch
- Amazon DynamoDB
- IAM
- AWS Lambda
- Amazon Simple Storage Service (Amazon S3)
- Amazon Simple Notification Service (Amazon SNS)
- AWS Step Functions

Arquitectura de destino

El siguiente diagrama muestra un ejemplo de flujo de trabajo para administrar los ciclos de vida de los inquilinos en varios productos SaaS en un único plano de control en la nube de AWS.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un usuario de AWS inicia el aprovisionamiento de inquilinos, el aprovisionamiento de productos o las acciones relacionadas con la administración mediante una llamada a un punto de conexión de API Gateway.
2. El usuario se autentica mediante un token de acceso que se recupera de un grupo de usuarios de Amazon Cognito o de otro IdP.
3. Las tareas individuales de aprovisionamiento o administración se ejecutan mediante funciones de Lambda que se integran con los puntos de conexión de API de API Gateway.
4. Las API de administración de la solución de arrendamiento común (para inquilinos, productos y usuarios) recopilan todos los parámetros de entrada, encabezados y tokens necesarios. A continuación, las API de administración invocan las funciones de Lambda asociadas.
5. El servicio de IAM valida los permisos de IAM tanto para las API de administración como para las funciones de Lambda.
6. Las funciones de Lambda almacenan y recuperan datos de los catálogos (para inquilinos, productos y usuarios) en DynamoDB y Amazon S3.
7. Una vez validados los permisos, se invoca un flujo de trabajo de AWS Step Functions para realizar una tarea específica. El ejemplo del diagrama muestra un flujo de trabajo de aprovisionamiento de inquilinos.

8. Las tareas individuales del flujo de trabajo de AWS Step Functions se ejecutan en un flujo de trabajo predeterminado (máquina de estado).
9. Todos los datos esenciales necesarios para ejecutar la función de Lambda asociada a cada tarea del flujo de trabajo se recuperan de DynamoDB o Amazon S3. Es posible que sea necesario aprovisionar otros recursos de AWS mediante una CloudFormation plantilla de AWS.
10. Si es necesario, el flujo de trabajo envía una solicitud para aprovisionar recursos de AWS adicionales para un producto SaaS específico a la cuenta de AWS de ese producto.
11. Cuando la solicitud se realiza correctamente o no, el flujo de trabajo publica la actualización de estado como un mensaje en un tema de Amazon SNS.
12. Amazon SNS está suscrito al tema Amazon SNS del flujo de trabajo Step Functions.
13. A continuación, Amazon SNS envía la actualización del estado del flujo de trabajo al usuario de AWS.
14. Los registros de las acciones de cada servicio de AWS, incluida una pista de auditoría de las llamadas a la API, se envían a CloudWatch. Se pueden configurar reglas y alarmas específicas CloudWatch para cada caso de uso.
15. Los registros se archivan en buckets de Amazon S3 para fines de auditoría.

Automatizar y escalar

Este patrón utiliza una CloudFormation plantilla para ayudar a automatizar la implementación de la solución Common Tenant. La plantilla también puede ayudarle a vender rápidamente los recursos asociados al alza o a la baja.

Para obtener más información, consulte Trabajar con CloudFormation plantillas de AWS en la Guía del CloudFormation usuario de AWS.

Herramientas

Herramientas

- Amazon API Gateway le ayuda a crear, publicar, mantener, supervisar y proteger REST, HTTP y WebSocket API a cualquier escala.
- Amazon Cognito ofrece autenticación, autorización y administración de usuarios para aplicaciones móviles y web.
- AWS le CloudTrail ayuda a auditar la gobernanza, el cumplimiento y el riesgo operativo de su cuenta de AWS.

- Amazon le CloudWatch ayuda a monitorizar las métricas de sus recursos de AWS y las aplicaciones que ejecuta en AWS en tiempo real.
- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Amazon Simple Notification Service (Amazon SNS) le ayuda a coordinar y gestionar el intercambio de mensajes entre publicadores y clientes, incluyendo los servidores web y las direcciones de correo electrónico.
- AWS Step Functions es un servicio de orquestación sin servidor que le ayuda a combinar funciones de Lambda de AWS y otros servicios de AWS para crear aplicaciones esenciales desde el punto de vista empresarial.

Prácticas recomendadas

La solución de este patrón utiliza un único plano de control para gestionar la incorporación de varios inquilinos y proporcionar acceso a varios productos de SaaS. El plano de control ayuda a los usuarios administrativos a gestionar otros cuatro planos con características específicas:

- Plano de seguridad
- Plano de flujo de trabajo
- Plano de comunicación
- Plano de registro y monitoreo

Epics

Configuración del plano de seguridad

Tarea	Descripción	Habilidades requeridas
Establezca los requisitos para su plataforma SaaS multiusuario.	Establezca requisitos detallados para lo siguiente: • Inquilinos • Usuarios • Roles • Productos SaaS de • Suscripciones • Intercambios de perfiles	Arquitecto de la nube, administrador de sistemas de AWS
Configure el servicio de Amazon Cognito.	Siga las instrucciones de Introducción a Amazon Cognito de la Guía para desarrolladores de Amazon Cognito.	Arquitecto de la nube
Configure las políticas de IAM necesarias.	Cree las políticas de IAM necesarias para su caso de uso. A continuación, asigne las políticas a los roles de IAM en Amazon Cognito. Para obtener más información, consulte Administrar el acceso mediante políticas y Control de acceso basado en roles en la Guía para desarrolladores de Amazon Cognito.	Administrador de la nube, arquitecto de la nube, seguridad de AWS IAM
Configure los permisos de API necesarios.	Configure los permisos de acceso a API Gateway	Administrador de la nube, arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	mediante roles y políticas de IAM y autorizadores Lambda. Para obtener instrucciones, consulte las secciones siguientes de la Guía de desarrolladores de Amazon API Gateway: • Control del acceso a una API con permisos de IAM • Uso de autorizadores Lambda de API Gateway	

Configuración del plano de datos

Tarea	Descripción	Habilidades requeridas
Cree los catálogos de datos necesarios.	1. Cree tablas de DynamoDB para almacenar los datos de los catálogos de usuarios. Asegúrese de incluir los atributos y funciones de los usuarios. Además, asegúrese de modelar los datos en las tablas del catálogo para mantener los atributos obligatorios y opcionales de cada usuario y función. 2. Cree tablas de DynamoDB para almacenar los datos de los catálogos de productos. Asegúrese de modelar los casos de	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	uso específicos para sus productos SaaS. 3. Cree tablas de DynamoDB para almacenar los datos de los catálogos de inquilinos. Asegúrese de configurar los modelos de suscripción para los inquilinos, los productos y las licencias para las suscripciones multiSaaS y las etiquetas. Para obtener más informaci ón, consulte Configuración de DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.	

Configuración del plano de control

Tarea	Descripción	Habilidades requeridas
Cree funciones de Lambda y API de API Gateway para ejecutar las tareas necesarias del plano de control.	Cree funciones de Lambda y API de API Gateway independientes para añadir, eliminar y gestionar lo siguiente: • Usuarios • Inquilinos • Productos	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	Para obtener más información, consulte Uso de AWS Lambda con Amazon API Gateway en la Guía para desarrolladores de AWS Lambda.	

Configuración del plano de flujo de trabajo

Tarea	Descripción	Habilidades requeridas
Identifique las tareas que deben ejecutar los flujos de trabajo de AWS Step Functions.	Identifique y documente los requisitos detallados del flujo de trabajo de AWS Step Functions para lo siguiente: • Usuarios • Inquilinos • Productos Importante: Asegúrese de que las partes interesadas clave aprueben los requisitos.	Propietario de la aplicación
Cree los flujos de trabajo de AWS Step Functions necesarios.	1. Cree los flujos de trabajo necesarios para los usuarios, inquilinos y productos en AWS Step Functions. Para obtener más información, consulte la Guía para desarrolladores de AWS Step Functions. 2. Identifique los mecanismos de reintentos y gestión	Desarrollador de aplicaciones, responsable de compilación

Tarea	Descripción	Habilidades requeridas
	de errores. Para obtener más información, consulte Gestión de errores, reintentos y añadir alertas a las máquinas de estado de Step Function en el blog de AWS. 3. Implemente los pasos del flujo de trabajo mediante funciones de Lambda. Para obtener instrucciones, consulte Creación de una máquina de estado de Step Functions que utilice Lambda en la Guía para desarrolladores de AWS Step Functions. 4. Integre cualquier servicio externo con AWS Step Functions según sea necesario. 5. Mantenga el estado de cada flujo de trabajo en una tabla de DynamoDB y comunique el estado de cada flujo de trabajo mediante Amazon SNS.	

Configuración del plano de comunicación

Tarea	Descripción	Habilidades requeridas
Crear temas de Amazon SNS.	Cree temas de Amazon SNS para recibir notificaciones sobre lo siguiente: • Estados del flujo de trabajo • Errores • Reintentos Para obtener más informaci ón, consulte Creación de un tema de SNS en la Guía para desarrolladores de Amazon SNS.	Propietario de la aplicación, arquitecto de la nube
Suscribir puntos de conexión a cada tema de Amazon SNS.	Para recibir los mensajes publicados en un tema de Amazon SNS, tiene que suscribirse a un punto de conexión en cada tema. Para obtener más información, consulte el tema Suscripción a un tema de Amazon SNS en la Guía para desarrolladores de Amazon SNS.	Desarrollador de aplicaciones, arquitecto de la nube

Configuración del plano de registro y supervisión

Tarea	Descripción	Habilidades requeridas
Active el registro para cada componente de la solución común para inquilinos.	Active el registro a nivel de componente para cada recurso de la solución de inquilino común que haya creado. Para obtener instrucciones, consulte lo siguiente: • ¿Cómo activo CloudWatch los registros para solucionar problemas con mi API REST o WebSocket API de API Gateway? (Centro de conocimientos de AWS) • Registro mediante CloudWatch registros (guía para desarrolladores de AWS Step Functions) • Registro de funciones de Lambda de AWS en Python (Guía para desarrolladores de AWS Lambda) • Registro y supervisión en Amazon Cognito (Guía para desarrolladores de Amazon Cognito) • Supervisión con Amazon CloudWatch (Guía para desarrolladores de Amazon DynamoDB)	Administrador de sistemas de AWS, desarrollador de aplicaciones, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	Nota: Puede consolidar los registros de cada recurso en una cuenta de registro centralizada mediante las políticas de IAM. Para obtener más información, consulte Registro centralizado y barreras de protección para varias cuentas.	

Aprovisionar e implementar la solución de inquilino común

Tarea	Descripción	Habilidades requeridas
Cree plantillas CloudFormation .	Automatice la implementación y el mantenimiento de la solución Common Tenant completa y todos sus componentes mediante el uso de CloudFormation plantillas. Para obtener más información, consulte la Guía del CloudFormation usuario de AWS.	Desarrollador, DevOps ingeniero y CloudFormation desarrollador de aplicaciones

Recursos relacionados

- Control del acceso a una API de REST con grupos de usuarios de Amazon Cognito como autorizador (Guía para desarrolladores de Amazon API Gateway)
- Uso de autorizadores Lambda de API Gateway (Guía para desarrolladores de Amazon API Gateway)
- Grupos de usuarios de Amazon Cognito (Guía para desarrolladores de Amazon Cognito)

- CloudWatch Consola multicuentas entre regiones (Guía del CloudWatch usuario de Amazon)

Más patrones

- Automatice la identificación y planificación de la estrategia de migración mediante AppScore
- Automatice la creación de recursos AppStream 2.0 con AWS CloudFormation
- Cree una arquitectura sin servidor multiusuario en Amazon Service OpenSearch
- Implemente el aislamiento de usuarios de SaaS para Amazon S3 mediante una máquina expendedora de tokens de AWS Lambda
- Integrar el controlador universal Stonebranch con AWS Mainframe Modernization
- Incorporación de inquilinos en la arquitectura SaaS para el modelo de silo mediante C# y AWS CDK

Seguridad, identidad, conformidad

Temas

- Acceder a los servicios de AWS desde una aplicación ASP.NET Core mediante los grupos de identidades de Amazon Cognito
- Autenticar Microsoft SQL Server en Amazon EC2 mediante AWS Directory Service
- Automatice la respuesta a incidentes y el análisis forense
- Automatizar la corrección de los resultados del estándar de AWS Security Hub
- Automatizar los escaneos de seguridad para cargas de trabajo entre cuentas mediante Amazon Inspector y AWS Security Hub
- Vuelva a habilitar AWS automáticamente CloudTrail mediante una regla de corrección personalizada en AWS Config
- Corrija automáticamente las instancias y los clústeres de bases de datos de Amazon RDS no cifrados
- Cambie automáticamente las claves de acceso de los usuarios de IAM a escala con AWS Organizations y AWS Secrets Manager
- Valide e implemente automáticamente las políticas y funciones de IAM en una cuenta de AWS mediante CodePipeline IAM Access Analyzer y macros de AWS CloudFormation
- Integración bidireccional de AWS Security Hub con el software Jira
- Cree un proceso para imágenes de contenedores reforzadas con Generador de imágenes de EC2 y Terraform
- Centralice la administración de claves de acceso de IAM en AWS Organizations mediante Terraform
- Registro centralizado y barrera de protección para varias cuentas
- Comprueba la versión de registro de acceso, HTTPS y TLS en una CloudFront distribución de Amazon
- Compruebe si hay entradas de red de un solo host en las reglas de ingreso de grupos de seguridad para IPv4 e IPv6
- Elija un flujo de autenticación de Amazon Cognito para aplicaciones empresariales
- Cree reglas personalizadas de AWS Config mediante las políticas de AWS CloudFormation Guard
- Crear un informe consolidado de los resultados de seguridad de Prowler en varias cuentas de AWS

- Eliminar volúmenes de Amazon Elastic Block Store (Amazon EBS) no utilizados con AWS Config y AWS Systems Manager
- Implemente y gestione los controles de la Torre de Control de AWS mediante AWS CDK y AWS CloudFormation
- Implementación y administración de los controles de AWS Control Tower mediante Terraform
- Implemente una canalización que detecte simultáneamente los problemas de seguridad en varios entregables de código
- Implemente controles de acceso basados en atributos de detección para subredes públicas mediante AWS Config
- Implemente controles de acceso preventivos basados en atributos para las subredes públicas
- Implementar la solución Security Automations para AWS WAF mediante Terraform
- Genere dinámicamente una política de IAM con IAM Access Analyzer mediante Step Functions
- Habilite Amazon de GuardDuty forma condicional mediante plantillas de AWS CloudFormation
- Habilitar el cifrado transparente de datos en Amazon RDS para SQL Server
- Asegúrese de que las CloudFormation pilas de AWS se lancen desde buckets S3 autorizados
- Asegúrese de que los equilibradores de carga de AWS usen protocolos de escucha seguros (HTTPS, SSL/TLS)
- Asegúrese de que el cifrado de los datos en reposo de Amazon EMR esté habilitado en el momento del lanzamiento
- Asegúrese de que el perfil de IAM esté asociado a una instancia de EC2
- Asegúrese de que el clúster de Amazon Redshift esté cifrado en el momento de su creación
- Exporte un informe de las identidades del centro de identidad de IAM de AWS y sus asignaciones mediante PowerShell
- Supervisar y corregir la eliminación programada de las claves de AWS KMS
- Identifique los buckets públicos de S3 en AWS Organizations mediante Security Hub
- Gestione los conjuntos de permisos del AWS IAM Identity Center como código mediante AWS CodePipeline
- Administrar credenciales mediante AWS Secrets Manager
- Supervisar los clústeres de Amazon EMR para comprobar el cifrado en tránsito en el momento del lanzamiento
- Supervise ElastiCache los clústeres de Amazon para comprobar el cifrado en reposo
- Supervisar los pares de claves de instancias EC2 mediante AWS Config

- Supervise ElastiCache los clústeres para grupos de seguridad
- Supervisar la actividad del usuario raíz de IAM
- Enviar una notificación cuando se cree un usuario de IAM
- Impida el acceso a Internet a nivel de cuenta mediante una política de control de servicios
- Escanea los repositorios de Git en busca de información confidencial y problemas de seguridad mediante git-secrets
- Enviar alertas desde AWS Network Firewall a un canal de Slack
- Simplifique la administración de certificados privados mediante AWS Private CA y AWS RAM
- Cómo desactivar los controles estándar de seguridad en todas las cuentas de los miembros de Security Hub en un entorno de varias cuentas
- Actualice las credenciales de la CLI de AWS desde el centro de identidad de IAM de AWS mediante PowerShell
- Utilice AWS Config para supervisar las configuraciones de seguridad de Amazon Redshift
- Utilice Network Firewall para capturar los nombres de dominio DNS de la indicación del nombre del servidor (SNI) para el tráfico saliente
- Usa Terraform para habilitar Amazon automáticamente GuardDuty para una organización
- Compruebe que los nuevos clústeres de Amazon Redshift tengan puntos de conexión SSL necesarios
- Compruebe que los nuevos clústeres de Amazon Redshift se lanzan en una VPC
- Más patrones

Acceder a los servicios de AWS desde una aplicación ASP.NET Core mediante los grupos de identidades de Amazon Cognito

Creado por Bibhuti Sahu (AWS) y Marcelo Barbosa (AWS)

Entorno: PoC o piloto	Tecnologías: seguridad, identidad, conformidad; aplicaciones web y móviles	Servicios de AWS: Amazon Cognito

Resumen

Este patrón explica cómo puede configurar los grupos de usuarios y grupos de identidades de Amazon Cognito y, a continuación, habilitar una aplicación ASP.NET Core para que acceda a los recursos de AWS tras una autenticación correcta.

Amazon Cognito ofrece autenticación, autorización y administración de usuarios para sus aplicaciones móviles y web. Los dos componentes principales de Amazon Cognito son los grupos de usuarios y los grupos de identidades.

Un grupo de usuarios es un directorio de usuarios en Amazon Cognito. Con un grupo de usuarios, los usuarios pueden iniciar sesión en su aplicación web o móvil mediante Amazon Cognito. Los usuarios también pueden iniciar sesión a través de proveedores de identidad sociales como Google, Facebook, Amazon o Apple y a través de proveedores de identidad SAML.

Con los grupos de identidades de Amazon Cognito (identidades federadas), se pueden crear identidades únicas para los usuarios y federarlas con proveedores de identidad. Con un grupo de identidades, puede obtener credenciales de AWS temporales con privilegios limitados para obtener acceso a otros servicios de AWS. Antes de empezar a usar su nuevo grupo de identidades de Amazon Cognito, debe asignar uno o más roles de AWS Identity and Access Management (IAM) para determinar el nivel de acceso que desea que tengan los usuarios de la aplicación a los recursos de AWS. Los grupos de identidades definen dos tipos de identidades: autenticadas y sin autenticar. A cada tipo de identidad se le puede asignar su propio rol en IAM. Las identidades autenticadas pertenecen a usuarios que se han autenticado mediante un proveedor de inicio de sesión público (grupos de usuarios de Amazon Cognito, Facebook, Google, SAML o cualquier proveedor de OpenID Connect) o un proveedor de desarrolladores (su propio proceso de autenticación backend), mientras que las identidades no autenticadas suelen pertenecer a usuarios invitados. Cuando Amazon

Cognito reciba una solicitud de usuario, el servicio determina si la solicitud está autenticada o no autenticada, determina qué rol está asociado a qué tipo de autenticación y, a continuación, usa la política adjunta a ese rol para responder a la solicitud.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS con Amazon Cognito y permisos de IAM
- Acceso a los recursos de AWS que desea utilizar
- ASP.NET Core 2.0.0 o posterior

Arquitectura

Pila de tecnología

- Amazon Cognito
- ASP.NET Core

Arquitectura de destino

Herramientas

Herramientas, SDK y servicios de AWS

- Visual Studio o Visual Studio Code
- Amazon. AspNetCore.Identity.Cognito (1.0.4) — paquete NuGet
- AWSSDK.S3 (3.3.110.32) — paquete NuGet
- Amazon Cognito

Código

El archivo .zip adjunto incluye archivos de muestra que ilustran lo siguiente:

- Cómo recuperar un token de acceso para el usuario que ha iniciado sesión
- Cómo intercambiar un token de acceso por credenciales de AWS

- Cómo acceder al servicio de Amazon Simple Storage Service (Amazon S3) con credenciales de AWS

Rol de IAM para identidades autenticadas

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "mobileanalytics:PutEvents",
        "cognito-sync:*",
        "cognito-identity:*",
        "s3:ListAllMyBuckets*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Epics

Crear un grupo de usuarios de Amazon Cognito

Tarea	Descripción	Habilidades requeridas
Cree un grupo de usuarios.	1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon Cognito en https://console.aws.amazon.com/cognito/home. 2. Elija Manage User Pools (Administrar grupos de usuarios).	Desarrollador

Tarea	Descripción	Habilidades requeridas
	3. En la esquina superior derecha de la página, elija Create a User Pool (Crear un grupo de usuarios). 4. Proporcione un nombre para su grupo de usuarios, seleccione Revisar valores predeterminados y, a continuación, seleccione Crear grupo. 5. Apunte el ID de grupo.	

Tarea	Descripción	Habilidades requeridas
Agregar un cliente de aplicación.	Puede crear una aplicación para utilizar las páginas web integradas para que sus usuarios se inscriban e inicien sesión. 1. En la barra de navegación de la parte izquierda de la página del grupo de usuarios, seleccione Clientes de aplicaciones en Configuración general y, a continuación, seleccione Añadir un cliente de aplicaciones. 2. Asigne un nombre a su aplicación y, a continuación elija Crear cliente de aplicación. 3. Anote el ID de cliente de la aplicación y el secreto del cliente (seleccione Mostrar detalles para ver el secreto del cliente).	Desarrollador

Creación de un grupo de identidades en Amazon Cognito

Tarea	Descripción	Habilidades requeridas
Crear un grupo de identidades de .	1. En la consola de Amazon Cognito, elija Administrar grupos de identidades y, a continuación, Crear nuevo grupo de identidades.	Desarrollador

Tarea	Descripción	Habilidades requeridas
	2. Especifique un nombre para el grupo de identidades. 3. Si desea habilitar las identidades no autentica das, seleccione esa opción en la sección Identidades no autenticadas. 4. En la sección Proveedores de autenticación, configure el grupo de identidades de Cognito configurando el ID del grupo de usuarios y el ID del cliente de la aplicación y, a continuación, seleccione Crear grupo.	
Asigne roles de IAM para el grupo de identidades.	Puede editar los roles de IAM para los usuarios autenticados y no autenticados o mantener los valores predeterm inados y, a continuación, seleccione Permitir. Para este patrón, editaremos el rol de IAM autenticado y proporcionaremos acceso para `s3:ListAllMyBucket s` . Para ver un código de muestra, consulte el rol de IAM proporcionado anteriorm ente en la sección Herramien tas.	Desarrollador

Tarea	Descripción	Habilidades requeridas
Copie el ID del grupo de identidades.	Si selecciona Permitir en el paso anterior, se muestra la página Introducción a Amazon Cognito. En esta página, puede copiar el ID del grupo de identidades de la sección Obtener credenciales de AWS o seleccionar Editar grupo de identidades en la esquina superior derecha y copiar el ID del grupo de identidades de la pantalla que aparece.	Desarrollador

Configuración de su aplicación de muestra

Tarea	Descripción	Habilidades requeridas
Clone la aplicación web ASP.NET core de muestra.	1. Clona la aplicación web .NET core de ejemplo desde https://github.com /aws/ -provider.git. aws-aspnet-cognito-identity 2. Navegue hasta la carpeta `samples` y abra la solución. En este proyecto, usted configurará el archivo `appsettings.json` y agregará una página nueva que mostrará todos los buckets de S3 después de iniciar sesión correctam ente.	Desarrollador

Tarea	Descripción	Habilidades requeridas
Agregar dependencias.	Agregue una NuGet dependencia para `Amazon.AspNetCore.Identity.Cognito` a su aplicación ASP.NET Core.	Desarrollador
Agregue las claves y los valores de configuración a appsettings.json.	Incluya el código del archivo `appsettings.json` adjunto en su archivo `appsettings.json` y, a continuación, sustituya los marcadores de posición por los valores de los pasos anteriores.	Desarrollador
Cree un nuevo usuario e inicie sesión.	Cree un nuevo usuario en el grupo de usuarios de Amazon Cognito y verifique que el usuario existe en Usuarios y grupos en el grupo de usuarios.	Desarrollador
Cree una nueva página de Razor llamada MyS3buckets.	Agregue una nueva página de Razor de ASP.NET Core a su aplicación de muestra y reemplace el contenido del ejemplo adjunto por `MyS3Bucket.cshtml` y `MyS3Bucket.cshtml.cs`. Agregue la nueva página de MyS3bucket en la barra de navegación de la página `_Layout.cshtml`.	Desarrollador

Solución de problemas

Problema	Solución
Tras abrir la aplicación de muestra desde el GitHub repositorio, aparece un error al intentar agregar el NuGet paquete al proyecto de muestras.	En la carpeta `src`, asegúrese de eliminarl o de la referencia al proyecto `Amazon.As pNetCore.Identity.Cognito` del archivo `Samples.sln` . A continuación, puede añadir el NuGet paquete al proyecto Samples sin ningún problema.

Recursos relacionados

- Amazon Cognito
- Grupos de usuarios de Amazon Cognito
- Grupos de identidades de Amazon Cognito
- Ejemplos de políticas de acceso
- GitHub - Proveedor de identidad AWS ASP.NET Cognito

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Autenticar Microsoft SQL Server en Amazon EC2 mediante AWS Directory Service

Creado por Jagadish Kantubugata (AWS) y Oludahun Bade Ajidahun (AWS)

Entorno: PoC o piloto	Origen: Active Directory	Destino: AWS Directory Service
Tipo R: N/D	Carga de trabajo: Microsoft	Tecnologías: Seguridad, identidad, conformidad; bases de datos
Servicios de AWS: AWS Directory Service		

Resumen

Este patrón describe cómo crear un directorio de AWS Directory Service y usarlo para autenticar Microsoft SQL Server en una instancia de Amazon Elastic Compute Cloud (Amazon EC2).

AWS Directory Service ofrece varios modos de utilizar Amazon Cloud Directory y Microsoft Active Directory (AD) con otros servicios de AWS. En los directorios se almacena información sobre usuarios, grupos y dispositivos, y los administradores pueden usarlos para administrar el acceso a la información y los recursos. AWS Directory Service ofrece varias opciones de directorios para utilizar aplicaciones existentes compatibles con Microsoft AD o el protocolo ligero de acceso a directorios (LDAP) en la nube. También ofrece las mismas opciones para los desarrolladores que necesiten un directorio para administrar usuarios, grupos, dispositivos y accesos.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una nube privada virtual (VPC) con un mínimo de dos subredes privadas y dos subredes públicas
- Un rol de AWS Identity and Access Management (IAM) para unir el servidor al dominio

Arquitectura

Pila de tecnología de origen

- El origen puede ser un Active Directory en las instalaciones

Pila de tecnología de destino

- AWS Directory Service para Microsoft Active Directory (AWS Managed Microsoft AD)

Arquitectura de destino

Herramientas

- SQL Server Management Studio (SSMS) es una herramienta para administrar SQL Server, que incluye el acceso, la configuración y la administración de los componentes de SQL Server.

Epics

Configure un directorio

Tarea	Descripción	Habilidades requeridas
Seleccione AWS Managed Microsoft AD como tipo de directorio.	En la consola de AWS Directory Service, seleccione Directorios, Configurar directorio, AWS Managed Microsoft AD, Siguiente.	DevOps
Seleccione la edición.	De las ediciones disponibles para AWS Managed Microsoft AD, elija Standard Edition.	DevOps
Especifique el nombre de DNS del directorio.	Utilice un nombre de dominio completo. Este nombre solo se resolverá dentro de su	DevOps

Tarea	Descripción	Habilidades requeridas
	VPC. No es necesario que pueda resolverse públicamente.	
Establecer la contraseña del administrador.	La contraseña para el usuario administrativo predeterminado denominado Admin.	DevOps
Elegir la VPC y las subredes.	Elija la VPC que contendrá el directorio y las subredes de los controladores de dominio. Si no tiene una VPC con al menos dos subredes, deberá crear una.	DevOps
Revise e inicie el directorio.	Revise la información de edición y precio del directorio y, a continuación, seleccione Crear directorio.	DevOps

Lance una instancia de EC2 para SQL Server en el dominio

Tarea	Descripción	Habilidades requeridas
Seleccione una AMI para SQL Server.	Los pasos en esta epic unen de forma sencilla una instancia de EC2 de Windows al directorio de AWS Managed Microsoft AD. En la consola de Amazon EC2, seleccione Lanzar instancia y, a continuación, seleccione la imagen de	DevOps, administrador de bases de datos

Tarea	Descripción	Habilidades requeridas
	máquina de Amazon (AMI) adecuada para SQL Server.	
Configure los detalles de la instancia.	Configure la instancia de Windows para adecuarla a sus necesidades de SQL Server.	DevOps, DBA
Seleccione el nombre del par de claves.	Seleccione un par de claves y, a continuación, lance la instancia.	DevOps, DBA
Añada una red.	Seleccione la VPC en la que se creó su directorio.	DevOps, DBA
Seleccione un Rol de IAM.	En Configuración avanzada, seleccione un perfil de IAM que tenga las políticas administradas por AWS `AmazonSSMManagedInstanceCore` y `AmazonSSMDirectoryServiceAccess` adjuntas.	DevOps, DBA
Agregue una subred.	Seleccione una de las subredes públicas de su VPC. La subred que seleccione debe tener todo el tráfico externo dirigido a una puerta de enlace de Internet. De lo contrario, no podrá conectarse a la instancia de forma remota.	DevOps, DBA
Seleccione su dominio.	Seleccione el dominio que creó en la lista de directorio de dominios.	DevOps, DBA

Tarea	Descripción	Habilidades requeridas
Lanzamiento de la instancia.	Seleccione Lanzar instancia.	Administrador de base de datos

Autenticar SQL Server mediante Directory Service

Tarea	Descripción	Habilidades requeridas
Inicie sesión como administrador de Windows.	Inicie sesión en la instancia de EC2 de Windows con las credenciales de administrador de Windows.	Administrador de base de datos
Inicie sesión en SQL Server.	Inicie SQL Server Management Studio (SSMS) e inicie sesión en SQL Server mediante el método de autenticación de Windows.	Administrador de base de datos
Cree un nombre de usuario para el usuario del directorio.	En SSMS, seleccione Seguridad y, a continuación, elija Nuevo inicio de sesión.	Administrador de base de datos
Busque un nombre de inicio de sesión.	Pulse el botón de búsqueda situado junto al cuadro de texto de inicio de sesión.	Administrador de base de datos
Seleccione una ubicación.	En el cuadro de diálogo Seleccionar usuario o grupo, elija Ubicaciones.	Administrador de base de datos
Introduzca las credenciales de red.	Introduzca las credenciales de red completas que usó al crear el servicio de directorio; por ejemplo: `test.com\admin` .	Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Seleccione el directorio.	Escriba el nombre del directorio de AWS y, después, seleccione OK (Aceptar).	Administrador de base de datos
Seleccione un nombre de objeto.	Seleccione el usuario para el que desea crear el inicio de sesión. Seleccione la ubicación, elija el directorio completo, busque el usuario y añada el nombre de usuario.	Administrador de base de datos
Inicie sesión en la instancia de SQL Server.	Inicie sesión en la instancia de EC2 de Windows para SQL Server con sus credenciales de dominio.	Administrador de base de datos
Inicie sesión en SQL Server como usuario de dominio.	Inicie SSMS y conéctese al motor de base de datos mediante el método de autenticación de Windows.	Administrador de base de datos

Recursos relacionados

- Documentación de AWS Directory Service (sitio web de AWS)
- Cree un directorio con AWS Managed Microsoft AD (documentación de AWS Directory Service)
- Únase de forma fluida a una instancia de EC2 de Windows (documentación de AWS Directory Service)
- Microsoft SQL Server en AWS (Web de AWS)
- Documentación de SSMS (sitio web de Microsoft)
- Cree un inicio de sesión en SQL Server (documentación de SQL Server)

Automatice la respuesta a incidentes y el análisis forense

Creado por Lucas Kauffman (AWS) y Tomek Jakubowski (AWS)

Repositorio de código: aws-automated-incident-response-and-forensics	Entorno: producción	Tecnologías: seguridad, identidad, conformidad
Servicios de AWS: Amazon EC2; AWS Lambda; Amazon S3; AWS Security Hub; AWS Identity and Access Management		

Resumen

Este patrón implementa un conjunto de procesos que utilizan funciones de AWS Lambda para proporcionar lo siguiente:

- Una forma de iniciar el proceso de respuesta a un incidente con un conocimiento mínimo
- Procesos automatizados y repetibles que están alineados con la Guía de respuesta a incidentes de seguridad de AWS
- Separación de cuentas para ejecutar los pasos de automatización, almacenar artefactos y crear entornos forenses

El marco forense y de respuesta automática a incidentes sigue un proceso forense digital estándar que consta de las siguientes fases:

1. Contención
2. Adquisición
3. Examen
4. Análisis

Puede realizar investigaciones sobre datos estáticos (por ejemplo, memoria adquirida o imágenes de disco) y sobre datos dinámicos activos pero en sistemas separados.

Para obtener más información, consulte la sección Detalles adicionales.

Requisitos previos y limitaciones

Requisitos previos

- Dos cuentas de AWS:
  - Cuenta de seguridad, que puede ser una cuenta existente, pero preferiblemente nueva
  - Cuenta forense, preferiblemente nueva
- Configuración de AWS Organizations
- En las cuentas de los miembros de organizaciones:
  - La función Amazon Elastic Compute Cloud (Amazon EC2) debe tener acceso a Amazon Simple Storage Service (Amazon S3) y AWS Systems Manager de AWS Systems Manager debe poder acceder a ella. Recomendamos utilizar la función gestionada de AWS `AmazonSSMManagedInstanceCore`. Tenga en cuenta que esta función se asociará automáticamente a la instancia de EC2 cuando se inicie la respuesta al incidente. Cuando finalice la respuesta, AWS Identity and Access Management (IAM) eliminará todos los derechos de la instancia.
  - Puntos de conexión de la nube privada virtual (VPC) en la cuenta de miembro de AWS y en las VPC de análisis y respuesta a incidentes. Estos puntos de conexión son: S3 Gateway, EC2 Messages, SSM y SSM Messages.
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada en las instancias EC2. Si las instancias EC2 no tienen la CLI de AWS instalada, se necesitará acceso a Internet para que la instantánea del disco y la adquisición de memoria funcionen. En este caso, los scripts se conectarán a Internet para descargar los archivos de instalación de la CLI de AWS y los instalarán en las instancias.

Limitaciones

- Este marco no pretende generar artefactos que puedan considerarse pruebas electrónicas y que puedan presentarse ante un tribunal.
- Actualmente, este patrón solo admite instancias basadas en Linux que se ejecutan en una arquitectura x86.

Arquitectura

Pila de tecnología de destino

- AWS CloudFormation
- AWS CloudTrail
- AWS Config
- IAM
- Lambda
- Amazon S3
- AWS Key Management Server (AWS KMS)
- AWS Security Hub
- Amazon Simple Notification Service (Amazon SNS)
- AWS Step Functions

Arquitectura de destino

Además de la cuenta de miembro, el entorno de destino consta de dos cuentas principales: una cuenta de seguridad y una cuenta de análisis forense. Se utilizan dos cuentas por las siguientes razones:

- Para separarlas de cualquier otra cuenta de cliente a fin de reducir el radio de explosión en caso de un análisis forense fallido
- Para ayudar a garantizar el aislamiento y la protección de la integridad de los artefactos que se están analizando
- Para mantener la confidencialidad de la investigación
- Para evitar situaciones en las que los actores de la amenaza pudieran haber utilizado todos los recursos inmediatamente disponibles para su cuenta de AWS comprometida, alcanzando las Service Quotas e impidiéndole crear una instancia de Amazon EC2 para realizar investigaciones.

Además, disponer de cuentas de seguridad y de análisis forenses independientes permite crear funciones distintas: un sistema de respuesta para obtener pruebas y otra de investigador para analizarlas. Cada rol tendría acceso a su cuenta independiente.

El siguiente diagrama muestra solo la interacción entre las cuentas. Los detalles de cada cuenta se muestran en los diagramas siguientes y se adjunta un diagrama completo.

En el siguiente diagrama se muestra la cuenta de miembro.

1. Se envía un evento al tema Amazon SNS de Slack.

En el siguiente diagrama se muestra la cuenta de seguridad.

2. El tema SNS de la cuenta de seguridad inicia los eventos forenses.

En el siguiente diagrama se muestra la cuenta de análisis forense.

La cuenta de seguridad es donde se crean los dos flujos de trabajo principales de AWS Step Functions para la adquisición de memoria e imágenes de disco. Una vez ejecutados los flujos de trabajo, acceden a la cuenta miembro que tiene las instancias de EC2 involucradas en un incidente e inician un conjunto de funciones de Lambda que recopilarán un volcado de memoria o un volcado de disco. Luego, esos artefactos se almacenan en la cuenta de análisis forense.

La cuenta de análisis forense guardará los artefactos recopilados por el flujo de trabajo de Step Functions en el bucket de S3 de artefactos de análisis. La cuenta de análisis forense también tendrá una canalización de EC2 Image Builder que crea una imagen de máquina de Amazon (AMI) de una instancia de análisis forense. Actualmente, la imagen se basa en SANS SIFT Workstation.

El proceso de creación utiliza la VPC de mantenimiento, que tiene conectividad a Internet. La imagen se puede utilizar posteriormente para activar la instancia de EC2 para analizar los artefactos recopilados en la VPC de análisis.

La VPC de análisis no tiene conectividad a Internet. De forma predeterminada, el patrón crea tres subredes de análisis privadas. Puede crear hasta 200 subredes, que es la cuota para el número de subredes de una VPC, pero es necesario añadir esas subredes a los puntos de conexión de VPC para que el administrador de sesiones de AWS Systems Manager automatice la ejecución de comandos en ellas.

Desde el punto de vista de las prácticas recomendadas, recomendamos utilizar AWS CloudTrail y AWS Config para hacer lo siguiente:

- Realice un seguimiento de los cambios realizados en su cuenta de análisis forense
- Supervise el acceso y la integridad de los artefactos que se almacenan y analizan

Flujo de trabajo

El siguiente diagrama muestra los pasos clave de un flujo de trabajo que incluye el proceso y el árbol de decisiones desde el momento en que una instancia se ve comprometida hasta que se analiza y contiene.

1. ¿Se ha establecido la etiqueta `SecurityIncidentStatus` con el valor Analizar? Si es así, haga lo siguiente:
   a. Adjunte los perfiles de IAM correctos para AWS Systems Manager y Amazon S3.
   b. Envíe un mensaje de Amazon SNS a la cola de Amazon SNS de Slack.
   c. Envíe un mensaje de Amazon SNS a la cola `SecurityIncident`.
   d. Invoque el equipo de estado de adquisición de memoria y disco.
2. ¿Se han adquirido la memoria y el disco? Si la respuesta es no, se ha producido un error.
3. Etiquete la instancia EC2 con la etiqueta `Contain`.
4. Adjunte el rol de IAM y el grupo de seguridad para aislar completamente la instancia.

Automatizar y escalar

La intención de este patrón es proporcionar una solución escalable para realizar análisis forenses y de respuesta a incidentes en varias cuentas de una sola organización de AWS Organizations.

Herramientas

Servicios de AWS

- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.

- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto para interactuar con los servicios de AWS mediante comandos en el intérprete de comandos de línea de comandos.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Key Management Service (AWS KMS) le ayuda a crear y controlar claves criptográficas para proteger sus datos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Security Hub proporciona una visión completa de su estado de seguridad en AWS. También le permite comprobar si su entorno de AWS cumple con los estándares y las prácticas recomendadas del sector de seguridad.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- AWS Step Functions es un servicio de orquestación sin servidor que le permite combinar funciones de Lambda AWS y otros servicios de AWS para crear aplicaciones esenciales desde el punto de vista empresarial.
- AWS Systems Manager le permite administrar las aplicaciones y la infraestructura que se ejecutan en la nube de AWS. Simplifica la administración de aplicaciones y recursos, reduce el tiempo requerido para detectar y resolver problemas operativos y ayuda a utilizar y administrar los recursos de AWS a escala de manera segura.

Código

Para obtener el código y las directrices específicas de implementación y uso, consulte el repositorio del Marco Forense y de Respuesta GitHub Automatizada a Incidentes.

Epics

Implemente las plantillas CloudFormation

Tarea	Descripción	Habilidades requeridas
Implemente CloudFormation plantillas.	Las CloudFormation plantillas están marcadas del 1 al 7 y la primera palabra del nombre del script indica en qué cuenta se debe implementar la plantilla. Tenga en cuenta que el orden de lanzamiento de las CloudFormation plantillas es importante. • `1-forensic-AnalysisVPCnS3Buckets.yaml` : se implementó en la cuenta de análisis forense. Crea los buckets S3 y la VPC de análisis, y se activa. CloudTrail • `2-forensic-MaintenanceVPCnEC2ImageBuilderPipeline.yaml` : implementa la VPC de mantenimiento y la canalización del generador de imágenes basada en SANS SIFT. • `3-security_IR-Disk_Mem_automation.yaml` : implementa las funciones en la cuenta de seguridad que permiten	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	la adquisición de discos y memoria. • `4-security_LiME_Volatility_Factory.yaml` : inicia una función de compilación para empezar a crear los módulos de memoria en función de los ID de AMI proporcionados. Tenga en cuenta que los ID de AMI son diferentes según las regiones de AWS. Siempre que necesite nuevos módulos de memoria, puede volver a ejecutar este script con los nuevos ID de AMI. Considere la posibilidad de integrarlo con las canalizaciones de creación de AMI de Golden Image (si se utilizan en su entorno). • `5-member-IR-automation.yaml` : crea la función de automatización de respuesta a incidentes de los miembros, que inicia el proceso de respuesta a incidentes. Permite compartir los volúmenes de Amazon Elastic Block Store (Amazon EBS) entre cuentas, publicar automáticamente en los canales de	

Tarea	Descripción	Habilidades requeridas
	Slack durante el proceso de respuesta a incidentes, iniciar el proceso forense y aislar las instancias una vez finalizado el proceso. • `6-forensic-artifact-s3-policies.yaml` : una vez implementados todos los scripts, este script corrige los permisos necesarios para todas las interacciones entre cuentas. • `7-security-IR-vpc.yaml` : configura una VPC utilizada para el procesamiento del volumen de respuesta a incidentes. Para iniciar el marco de respuesta a incidentes para una instancia de EC2 específica, cree una etiqueta con la clave `SecurityIncidentStatus` y el valor `Analyze`. Esto iniciará la función de Lambda de miembro que iniciará automáticamente el aislamiento y la memoria, así como la adquisición de discos.	

Tarea	Descripción	Habilidades requeridas
Opere el marco.	La función de Lambda también volverá a etiquetar el activo al final (o en caso de fallo) con `Contain`. Esto inicia la contención, que aísla completamente la instancia sin un grupo de seguridad entrante ni saliente y con un rol de IAM que impide todo acceso. Siga los pasos del repositorio. GitHub	Administrador de AWS

Implemente acciones personalizadas de Security Hub

Tarea	Descripción	Habilidades requeridas
Implemente las acciones personalizadas de Security Hub mediante una CloudFormation plantilla.	Para crear una acción personalizada de forma que pueda usar la lista desplegable de Security Hub, implemente la `Modules/SecurityHub Custom Actions/SecurityHubCustomActions.yaml` CloudFormation plantilla. A continuación, modifique la función `IRAutomation` en cada una de las cuentas de los miembros para permitir que la función de Lambda que ejecuta la acción asuma la función `IRAutomation` .	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	Para obtener más información, consulte el GitHub repositorio.	

Recursos relacionados

- Guía de respuesta a incidentes de seguridad de AWS

Información adicional

Al utilizar este entorno, un equipo del centro de operaciones de seguridad (SOC) puede mejorar su proceso de respuesta a los incidentes de seguridad de la siguiente manera:

- Tener la capacidad de realizar análisis forenses en un entorno dividido para evitar comprometer accidentalmente los recursos de producción
- Disponer de un proceso estandarizado, repetible y automatizado para la contención y el análisis.
- Ofrecer a cualquier propietario o administrador de una cuenta la posibilidad de iniciar el proceso de respuesta a los incidentes con un conocimiento mínimo de cómo usar las etiquetas
- Disponer de un entorno limpio y estandarizado para realizar análisis de incidentes y análisis forenses sin el ruido de un entorno más grande
- Tener la capacidad de crear múltiples entornos de análisis en paralelo
- Centrar los recursos del SOC en la respuesta a los incidentes en lugar de en el mantenimiento y la documentación de un entorno forense en la nube
- Pasar de un proceso manual a uno automatizado para lograr la escalabilidad
- Uso CloudFormation de plantillas para mantener la coherencia y evitar tareas repetibles

Además, evita el uso de una infraestructura persistente y paga por los recursos cuando los necesita.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Automatizar la corrección de los resultados del estándar de AWS Security Hub

Documento creado por Chandini Penmetsa (AWS) y Aromal Raj Jayarajan (AWS)

Entorno: Producción	Tecnologías: seguridad, identidad, cumplimiento	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: AWS CloudFormation; Amazon CloudWatch; AWS Lambda; AWS Security Hub; Amazon SNS		

Resumen

Con AWS Security Hub, puede habilitar comprobaciones de las prácticas recomendadas estándar, como las siguientes:

- Prácticas recomendadas de seguridad básica de AWS
- CIS AWS Foundations Benchmark
- La norma de seguridad de datos del sector de pagos con tarjeta (PCI DSS)

Cada uno de estos estándares tiene controles predefinidos. Security Hub comprueba el control en una cuenta de AWS determinada e informa de los resultados.

AWS Security Hub envía todos los resultados a Amazon de forma EventBridge predeterminada. Este patrón proporciona un control de seguridad que implementa una EventBridge regla para identificar los hallazgos estándar de las mejores prácticas de seguridad fundamentales de AWS. La regla identifica los siguientes resultados para escalado automático, nubes privadas virtuales (VPC), Amazon Elastic Block Store (Amazon EBS) y Amazon Relational Database Service (Amazon RDS), según el estándar de prácticas recomendadas de AWS Foundational Security:

- [AutoScaling.1] Los grupos de Auto Scaling asociados a un balanceador de cargas deben usar comprobaciones de estado del balanceador de cargas

- [EC2.2] El grupo de seguridad predeterminado de VPC no debe permitir el tráfico entrante ni saliente
- [EC2.6] El registro de flujo de VPC debe estar habilitado en todas las VPC
- [EC2.7] El cifrado predeterminado de EBS debe estar habilitado
- [RDS.1] Las instantáneas de RDS deben ser privadas
- [RDS.6] Se debe configurar la supervisión mejorada para las instancias y los clústeres de base de datos de RDS
- [RDS.7] Los clústeres de RDS deben tener habilitada la protección frente a eliminación

La EventBridge regla remite estos hallazgos a una función de AWS Lambda, que corrige el hallazgo. A continuación, la función de Lambda envía una notificación con información de corrección a un tema de Amazon Simple Notification Service (Amazon SNS).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Una dirección de correo electrónico en la que se desee recibir la notificación de la corrección
- Security Hub y AWS Config habilitados en la región de AWS en la que se pretende implementar el control
- Un bucket de Amazon Simple Storage Service (Amazon S3) en la misma región que el control para cargar el código de AWS Lambda

Limitaciones

- Este control de seguridad corrige automáticamente los nuevos resultados notificados después de la implementación del control de seguridad. Para corregir los resultados existentes, selecciónelos manualmente en la consola de Security Hub. A continuación, en Acciones, seleccione la acción personalizada AFSBPremedy que AWS creó como parte de la implementación. CloudFormation
- Este control de seguridad es regional, por lo que debe implementarse en las regiones de AWS que se desee supervisar.
- Para la solución EC2.6, para habilitar los registros de flujo de VPC, se creará un grupo de registros de CloudWatch Amazon Logs con el formatoVpcFlowLogs//vpc_id. Si existe un grupo de registros con el mismo nombre, se utilizará el grupo de registros existente.

- Para la corrección EC2.7, para habilitar el cifrado predeterminado de Amazon EBS, se usa la clave de AWS Key Management Service (AWS KMS). Este cambio impide el uso de determinadas instancias que no admiten el cifrado.

Arquitectura

Pila de tecnología de destino

- Función de Lambda
- Tema de Amazon SNS
- EventBridge regla
- Roles de AWS Identity and Access Management (IAM) para la función de Lambda, registros de flujo de la VPC y supervisión mejorada de Amazon Relational Database Service (Amazon RDS)

Arquitectura de destino

Automatizar y escalar

Si utiliza AWS Organizations, puede utilizar AWS CloudFormation StackSets para implementar esta plantilla en varias cuentas que desee que supervise.

Herramientas

Herramientas

- AWS CloudFormation: AWS CloudFormation es un servicio que le ayuda a modelar y configurar los recursos de AWS mediante el uso de la infraestructura como código.
- EventBridge— Amazon EventBridge ofrece un flujo de datos en tiempo real desde sus propias aplicaciones, aplicaciones de software como servicio (SaaS) y servicios de AWS, y dirige esos datos a objetivos como las funciones Lambda.
- Lambda: AWS Lambda admite ejecutar código sin aprovisionar ni administrar servidores.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos altamente escalable que se puede utilizar para una amplia gama de soluciones de almacenamiento, incluidos sitios web, aplicaciones móviles, copias de seguridad y lagos de datos.

- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) coordina y gestiona la entrega o el envío de mensajes entre publicadores y clientes, incluyendo los servidores web y las direcciones de correo electrónico. Los suscriptores reciben todos los mensajes publicados de los temas a los que están suscritos y todos los suscriptores de un tema reciben los mismos mensajes.

Prácticas recomendadas

- Nueve prácticas recomendadas de AWS Security Hub
- Estándar de prácticas recomendadas de AWS Foundational Security

Epics

Implementar el control de seguridad

Tarea	Descripción	Habilidades requeridas
Elimine el bucket de S3.	En la consola de Amazon S3, seleccione o cree un bucket de S3 con un nombre único que no contenga barras diagonales en el inicio. Los nombres de bucket de S3 son únicos globalmente y todas las cuentas de AWS comparten el espacio de nombres. Su bucket de S3 debe estar en la misma región de que los resultados de Security Hub que se están evaluando.	Arquitecto de la nube
Cargue el código Lambda en el bucket de S3.	Cargue el archivo .zip de código Lambda que se proporciona en la sección «Adjuntos» en el bucket de S3 definido.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation plantilla de AWS.	Implemente la CloudForm ation plantilla de AWS que se proporciona como adjunto a este patrón. En la epic siguiente, proporcione los valores de los parámetros.	Arquitecto de la nube

Complete los parámetros de la CloudFormation plantilla de AWS

Tarea	Descripción	Habilidades requeridas
Proporcione el nombre del bucket de S3.	Escriba el nombre del bucket de S3 que ha creado en la primera epic.	Arquitecto de la nube
Proporcione el prefijo de Amazon S3.	Proporcione la ubicación del archivo .zip del código Lambda en su bucket de S3, sin barras diagonales iniciales (por ejemplo, <directory>/<file-name>.zip).	Arquitecto de la nube
Proporcione el ARN de tema de SNS.	Proporcione el nombre de recurso de Amazon (ARN) del tema de SNS si desea utilizar un tema de SNS existente para las notificaciones de corrección. Para usar un tema de SNS nuevo, mantenga el valor como «None» (el valor predeterminado).	Arquitecto de la nube
Proporcione una dirección de correo electrónico.	Indique una dirección de correo electrónico en la que desee recibir las notificac	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	iones de corrección (solo es necesaria cuando desea que AWS CloudFormation cree el tema de SNS).	
Defina el nivel de registro.	Defina el nivel y la frecuenci a de registro de la función de Lambda. «Info» designa mensajes informativos detallados sobre el progreso de la aplicación. «Error» designa eventos de error que todavía permiten que la aplicación siga ejecutándose. «Warning» designa situacion es potencialmente peligrosas.	Arquitecto de la nube
Proporcione el ARN del rol de IAM de los registros de flujo de la VPC.	Proporcione el ARN del rol de IAM que se utilizará para los registros de flujo de la VPC. (Si se introduce «Ninguno» como entrada, AWS CloudFormation crea un rol de IAM y lo usa).	Arquitecto de la nube
Proporcione el ARN del rol de IAM de supervisión mejorada de RDS.	Proporcione el ARN del rol de IAM que se utilizará para la supervisión mejorada de RDS. (Si se introduce «Ninguno», AWS CloudFormation crea un rol de IAM y lo usa).	Arquitecto de la nube

Confirmar la suscripción

Tarea	Descripción	Habilidades requeridas
Confirme la suscripción a Amazon SNS.	Cuando la plantilla se implementa correctamente, si se ha creado un nuevo tema de SNS, se envía un mensaje de suscripción a la dirección de correo electróni co proporcionada. Para recibir notificaciones de correcció n se debe confirmar este mensaje de correo electrónico de suscripción.	Arquitecto de la nube

Recursos relacionados

- Creación de una pila en la CloudFormation consola de AWS
- AWS Lambda
- AWS Security Hub

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Automatizar los escaneos de seguridad para cargas de trabajo entre cuentas mediante Amazon Inspector y AWS Security Hub

Creado por Ramya Pulipaka (AWS) y Mikesh Khanal (AWS)

Entorno: producción	Tecnologías: seguridad, identidad, conformidad; operaciones	Servicios de AWS: Amazon Inspector; Amazon SNS; AWS Lambda; AWS Security Hub; Amazon CloudWatch

Resumen

Este patrón describe cómo buscar automáticamente vulnerabilidades en cargas de trabajo entre cuentas en la nube de Amazon Web Services (AWS).

El patrón ayuda a crear una programación para escaneos basados en hosts de instancias de Amazon Elastic Compute Cloud (Amazon EC2) que se agrupan por etiquetas o para escaneos de Amazon Inspector basados en red. Una CloudFormation pila de AWS implementa todos los recursos y servicios de AWS necesarios en sus cuentas de AWS.

Los resultados de Amazon Inspector se exportan a AWS Security Hub y proporcionan información sobre las vulnerabilidades en sus cuentas, regiones de AWS, nubes privadas virtuales (VPC) e instancias de EC2. Puede recibir estos resultados por correo electrónico o puede crear un tema del Amazon Simple Notification Service (Amazon SNS) que utilice un punto de conexión HTTP para enviar los resultados a herramientas de emisión de tickets, software de información de seguridad y gestión de eventos (SIEM) u otras soluciones de seguridad de terceros.

Requisitos previos y limitaciones

Requisitos previos

- Una dirección de correo electrónico existente para recibir notificaciones por correo electrónico de Amazon SNS.
- Un punto de conexión HTTP existente utilizado por las herramientas de emisión de tickets, el software SIEM u otras soluciones de seguridad de terceros.

- Cuentas de AWS activas que alojan cargas de trabajo entre cuentas, incluyendo una cuenta de auditoría central.
- Security Hub, habilitado y configurado. Puede usar este patrón sin Security Hub, pero le recomendamos usar Security Hub por la información que genera. Para obtener más información, consulte Configuración de Security Hub en la documentación de AWS Security Hub.
- Debe haber instalado un agente de Amazon Inspector en cada instancia de EC2 que desee escanear. Puede instalar el Agente de Amazon Inspector en múltiples instancias de EC2 utilizando el comando AWS Systems Manager Run.

Habilidades

- Experiencia en el uso de conjuntos de pilas `self-managed` y `service-managed` permisos para ellos en AWS CloudFormation. Si desea utilizar permisos `self-managed` para implementar instancias de pila en cuentas específicas en regiones específicas, debe crear los roles de AWS Identity and Access Management (IAM) requeridos. Si desea utilizar permisos `service-managed` para implementar instancias de pila en cuentas administradas por AWS Organizations en regiones específicas, no necesita crear los roles de IAM requeridos. Para obtener más información, consulte Crear un conjunto de pilas en la CloudFormation documentación de AWS.

Limitaciones

- Si no se aplica ninguna etiqueta a las instancias de EC2 de una cuenta, Amazon Inspector escanea todas las instancias de EC2 de esa cuenta.
- Los conjuntos de CloudFormation pilas de AWS y el onboard-audit-account archivo.yaml (adjunto) deben implementarse en la misma región.
- De forma predeterminada, Amazon Inspector Classic no admite resultados agregados. Security Hub es la solución recomendada para ver las evaluaciones de varias cuentas o regiones de AWS.
- El enfoque de este patrón se puede escalar a la cuota de publicación de 30 000 transacciones por segundo (TPS) para un tema de SNS en la región Este de EE. UU. (Norte de Virginia) (us-east-1), aunque los límites varían según la región. Para escalar con mayor eficacia y evitar la pérdida de datos, se recomienda utilizar Amazon Simple Queue Service (Amazon SQS) antes del tema SNS.

Arquitectura

El siguiente diagrama ilustra el flujo de trabajo para escanear automáticamente instancias de EC2.

El flujo de trabajo consta de los pasos siguientes:

1. Una EventBridge regla de Amazon utiliza una expresión cron para autoiniciarse según un cronograma específico e inicia Amazon Inspector.

2. Amazon Inspector escanea las instancias de EC2 etiquetadas de la cuenta.

3. Amazon Inspector envía los resultados a Security Hub, que genera información sobre el flujo de trabajo, la priorización y la corrección.

4. Amazon Inspector también envía el estado de la evaluación a un tema de SNS de la cuenta de auditoría. Se invoca una función de Lambda de AWS si se publica un evento `findings reported` en el tema de SNS.

5. La función de Lambda obtiene, formatea y envía los resultados a otro tema de SNS de la cuenta de auditoría.

6. Los resultados se envían a las direcciones de correo electrónico que están suscritas al tema de SNS. Los detalles y recomendaciones completos se envían en formato JSON al punto de conexión HTTP suscrito.

Pila de tecnología

- AWS Control Tower
- EventBridge
- IAM
- Amazon Inspector
- Lambda
- Security Hub
- Amazon SNS

Herramientas

- AWS CloudFormation: AWS lo CloudFormation ayuda a modelar y configurar sus recursos de AWS para que pueda dedicar menos tiempo a administrarlos y más tiempo a centrarse en sus aplicaciones.
- AWS CloudFormation StackSets: AWS CloudFormation StackSets amplía la funcionalidad de las pilas al permitirle crear, actualizar o eliminar pilas en varias cuentas y regiones con una sola operación.
- AWS Control Tower: AWS Control Tower crea una capa de abstracción u orquestación que combina e integra las capacidades de varios otros servicios de AWS, incluyendo AWS Organizations.
- Amazon EventBridge: EventBridge es un servicio de bus de eventos sin servidor que facilita la conexión de sus aplicaciones con datos de diversas fuentes.
- AWS Lambda: Lambda es un servicio informático que facilita poder ejecutar código sin aprovisionar ni administrar servidores.
- AWS Security Hub: le proporciona una visión completa de su estado de seguridad en AWS y le ayuda a comprobar su entorno con los estándares y las prácticas recomendadas del sector de la seguridad.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) es un servicio administrado que proporciona la entrega de mensajes de los publicadores a los suscriptores.

Epics

Implemente la CloudFormation plantilla de AWS

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation plantilla de AWS en la cuenta de auditoría.	Descargue y guarde el archivo `onboard-audit-acco unt.yaml` (adjunto) en una ruta local de su ordenador. Inicie sesión en la consola de administración de AWS de su cuenta de auditoría, abra	Desarrollador, ingeniero de seguridad

Tarea	Descripción	Habilidades requeridas
	la CloudFormation consola de AWS y, a continuación, seleccione Create stack. Seleccione Preparar plantilla en la sección Requisitos previos y, a continuación, seleccione La plantilla está lista. Elija el Origen de la plantilla en la sección de Especificar plantilla y luego elija La plantilla está lista. Cargue el archivo `onboard-audit-account.yaml` y, a continuación, configure las opciones restantes según sus necesidades. Importante: Asegúrese de configurar los siguientes parámetros de entrada: • `DestinationEmailAddress` – Introduzca una dirección de correo electrónico para recibir los resultados. • `HTTPEndpoint` – Proporcione un punto de conexión HTTP para sus herramientas de emisión de tickets o SIEM. También puede implementar la CloudFormation plantilla	

Tarea	Descripción	Habilidades requeridas
	de AWS mediante la interfaz de línea de comandos de AWS (AWS CLI). Para obtener más información al respecto, consulte Creación de una pila en la CloudFormation documentación de AWS.	
Confirme la suscripción a Amazon SNS.	Abra la bandeja de entrada de correo electrónico y elija Confirmar la suscripción en el correo electrónico que reciba de Amazon SNS. Esto abre una ventana del navegador web y muestra la confirmación de la suscripción.	Desarrollador, ingeniero de seguridad

Cree conjuntos de CloudFormation pilas de AWS para automatizar la programación de escaneos de Amazon Inspector

Tarea	Descripción	Habilidades requeridas
Cree conjuntos de pilas en la cuenta de auditoría.	Descargue el archivo `vulnerability-management-program.yaml` (adjunto) a una ruta local de su ordenador. En la CloudFormation consola de AWS, selecciona Ver conjuntos de pilas y, a continuación, selecciona Crear. StackSet Seleccione La plantilla está lista, seleccione Cargar un archivo de	Desarrollador, ingeniero de seguridad

Tarea	Descripción	Habilidades requeridas
	plantilla y, a continuación, cargue el archivo `vulnerability-management-program.yaml` . Si quiere usar `self-managed` permisos, siga las instrucciones de Crear un conjunto de pilas con permisos autogestionados en la CloudFormation documentación de AWS. Esto crea conjuntos de pilas en cuentas individuales. Si quiere usar `service-managed` permisos, siga las instrucciones de Crear un conjunto de pilas con permisos administrados por servicios en la documentación de AWS CloudFormation . Esto crea conjuntos de pilas en toda su organización o unidades organizativas especificadas (OUS). Importante: Asegúrese de que los siguientes parámetros de entrada estén configurados para sus conjuntos de pilas: • `AssessmentSchedule` — El calendario de EventBridge uso de las expresiones cron.	

Tarea	Descripción	Habilidades requeridas
	• `Duration` – La duración de la ejecución de la evaluación de Amazon Inspector en segundos. • `CentralSNSTopicArn` – El nombre de recurso de Amazon (ARN) para el tema de SNS central. • `Tagkey` – La clave de etiqueta que está asociada con el grupo de recursos. • `Tagvalue` – El valor de etiqueta que está asociado con el grupo de recursos. Si quiere escanear las instancias de EC2 de la cuenta de auditoría, debe ejecutar el `vulnerability-management-program.yaml` archivo como una CloudFormation pila de AWS en la cuenta de auditoría.	
Valide la solución.	Compruebe que recibe los resultados por correo electrónico o punto de conexión HTTP según la programación que especificó para Amazon Inspector.	Desarrollador, ingeniero de seguridad

Recursos relacionados

- Escalar sus pruebas de vulnerabilidad de seguridad con Amazon Inspector
- Corregir automáticamente los resultados de seguridad de Amazon Inspector
- Cómo simplificar la configuración de la evaluación de seguridad mediante Amazon EC2, AWS Systems Manager y Amazon Inspector

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Vuelva a habilitar AWS automáticamente CloudTrail mediante una regla de corrección personalizada en AWS Config

Creado por Manigandan Shri (AWS)

Entorno: producción	Tecnologías: infraestructura; seguridad, identidad, conformidad	Servicios de AWS: Amazon S3; AWS Config; AWS KMS; AWS Identity and Access Management; AWS Systems Manager; AWS CloudTrail

Resumen

La visibilidad de la actividad de su cuenta de Amazon Web Services (AWS) es una práctica recomendada operativa y de seguridad importante. AWS le CloudTrail ayuda con la gobernanza, el cumplimiento y la auditoría operativa y de riesgos de su cuenta.

Para garantizar que CloudTrail siga habilitada en su cuenta, AWS Config proporciona la regla `cloudtrail-enabled` administrada. Si CloudTrail está desactivada, la `cloudtrail-enabled` regla la vuelve a activar automáticamente mediante una corrección automática.

Sin embargo, debe asegurarse de seguir las prácticas recomendadas de seguridad CloudTrail si utiliza la corrección automática. Estas prácticas recomendadas incluyen la activación CloudTrail en todas las regiones de AWS, el registro de las cargas de trabajo de lectura y escritura, la habilitación de información y el cifrado de los archivos de registro con cifrado del lado del servidor mediante claves administradas del AWS Key Management Service (AWS KMS) (SSE-KMS).

Este patrón le ayuda a seguir estas prácticas recomendadas de seguridad, ya que proporciona una acción correctiva personalizada para volver a activarla automáticamente en su cuenta. CloudTrail

Importante: Te recomendamos que utilices políticas de control de servicios (SCP) para evitar cualquier manipulación. CloudTrail Para obtener más información al respecto, consulte la CloudTrail sección Impedir la manipulación de AWS de Cómo utilizar AWS Organizations para simplificar la seguridad a gran escala en el blog de seguridad de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Permisos para crear un manual de procedimientos de Automatización de AWS Systems Manager
- Un registro de seguimiento existente para su cuenta

Limitaciones

Este patrón no admite las siguientes acciones:

- Configurar una clave de prefijo de Amazon Simple Storage Service (Amazon S3) para la ubicación de almacenamiento
- Publicar en un tema de Amazon Simple Notification Service (Amazon SNS)
- Configuración de Amazon CloudWatch Logs para monitorizar tus CloudTrail registros

Arquitectura

Pila de tecnología

- AWS Config
- CloudTrail
- Systems Manager
- Automatización de Systems Manager

Herramientas

- AWS Config brinda una visión detallada de la configuración de los recursos de AWS de su cuenta.
- AWS le CloudTrail ayuda a habilitar la gobernanza, el cumplimiento y la auditoría operativa y de riesgos de su cuenta.
- AWS Key Management Service (AWS KMS) es un servicio de cifrado y administración de claves.
- AWS Systems Manager le ayuda a ver y controlar la infraestructura en AWS.

- Automatización de AWS Systems Manager simplifica las tareas comunes de mantenimiento e implementación de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) y otros recursos de AWS.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Código

El archivo cloudtrail-remediation-action.yml (adjunto) le ayuda a crear un manual de automatización de Systems Manager para configurarlo y volver a activarlo utilizando las mejores prácticas de seguridad. CloudTrail

Epics

Configure CloudTrail

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3.	Inicie sesión en la consola de administración de AWS, abra la consola de Amazon S3 y, a continuación, cree un bucket de S3 para almacenar los CloudTrail registros. Para obtener más información, consulte Creación de un bucket en la documentación de Amazon S3.	Administrador de sistemas
Añada una política de bucket que permita CloudTrail entregar los archivos de registro al bucket de S3.	CloudTrail debe tener los permisos necesarios para entregar los archivos de registro a su bucket de S3. En la consola de Amazon S3, elija el bucket de S3 que ha creado anteriormente y, a continuación, elija Permisos.	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	Cree una política de bucket de S3 mediante la política de bucket de Amazon S3 que CloudTrail aparece en la CloudTrail documentación. Para conocer los pasos sobre cómo añadir una política a un bucket de S3, consulte Cómo añadir una política de bucket mediante la consola de Amazon S3 en la documenta ción de Amazon S3. Importante: Si especificó un prefijo al crear su ruta CloudTrail, asegúrese de incluirlo en la política de buckets de S3. El prefijo es un añadido opcional a la clave del objeto de S3 que crea una organización en forma de carpeta en su bucket de S3. Para obtener más informaci ón al respecto, consulte Crear una ruta en la CloudTrail documentación.	

Tarea	Descripción	Habilidades requeridas
Creación de una clave de KMS.	Cree una clave de AWS KMS CloudTrail para cifrar los objetos antes de añadirlos al bucket de S3. Para obtener ayuda con esta historia, consulte Cifrar archivos de CloudTrail registro con claves administradas de AWS KMS (SSE-KMS) en la documenta ción. CloudTrail	Administrador de sistemas
Agregue una política de claves a la clave de KMS.	Adjunte una política de claves de KMS para permitir el uso de CloudTrail la clave de KMS. Para obtener ayuda con esta historia, consulte Cifrar archivos de CloudTrail registro con claves administradas por AWS KMS (SSE-KMS) en la documentación. CloudTrail Importante: no requiere permisos. CloudTrail `Decrypt`	Administrador de sistemas
Manual de AssumeRole instrucciones de Create for Systems Manager	Cree un `AssumeRole` para que Systems Manager Automation ejecute el manual de procedimientos. Para obtener instrucciones y más información sobre esto, consulte Configura r la automatización en la documentación de Systems Manager.	Administrador de sistemas

Cree y pruebe el manual de procedimientos de Systems Manager Automation

Tarea	Descripción	Habilidades requeridas
Cree el manual de procedimientos de Systems Manager Automation.	Utilice el archivo `cloudtrail-remediation-action.yml` (adjunto) para crear el manual de procedimiento de Systems Manager Automation. Para obtener más información sobre esto, consulte Creación de documentos de Systems Manager en la documentación de Systems Manager.	Administrador de sistemas
Pruebe el manual de procedimientos.	En la consola de Systems Manager, pruebe el manual de procedimientos de Systems Manager Automation que creó anteriormente. Para obtener más información sobre esto, consulte Realizar una automatización simple en la documentación de Systems Manager.	Administrador de sistemas

Configure la corrección automática para la regla en AWS Config.

Tarea	Descripción	Habilidades requeridas
Agregue la regla CloudTrail activada.	En la consola de AWS Config, elija Rules (Reglas) y, a continuación, seleccione Add rule (Añadir regla). En la página Add rule (Añadir regla), seleccione Add custom rule	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	(Añadir regla personalizada). En la página Configure rule (Configurar regla), escriba un nombre y una descripción, y agregue la regla `cloudtrail-enabled` . Para obtener más información, consulte Administrar las reglas de todas las cuentas de la organización en la documentación de AWS Config.	

Tarea	Descripción	Habilidades requeridas
Agregue la acción correctora automática.	En la lista desplegable Actions (Acciones), seleccione Manage remediation (Administrar la corrección). Elija Auto remediation (Corrección automática) y, a continuación, elija el manual de procedimientos de Systems Manager que creó anteriormente. Los siguientes son los parámetros de entrada necesarios para CloudTrail: • `CloudTrailName` • `CloudTrailS3BucketName` • `CloudTrailKmsKeyId` • `AssumeRole` (opcional) Los siguientes parámetros de entrada están configurados en true de forma predeterminada: • `IsMultiRegionTrail` • `IsOrganizationTrail` • `IncludeGlobalServiceEvents` • `EnableLogFileValidation`	Administrador de sistemas

Tarea	Descripción	Habilidades requeridas
	Conserve los valores predeterminados para el parámetro de límites de velocidad y el parámetro de ID de recurso. Seleccione Save (Guardar). Para obtener más informaci ón, consulte Corregir recursos de AWS no conformes con las reglas de AWS Config en la documentación de AWS Config.	
Pruebe la regla de corrección automática.	Para probar la regla de corrección automática, abra la CloudTrail consola, elija Rutas y, a continuación, elija la ruta. Seleccione Stop logging (Detener el registro) para desactivar el registro de los registros de seguimien to. Cuando se le pida que confirme, seleccione Detener el registro. CloudTrail detiene el registro de la actividad de esa ruta. Siga las instrucciones de Evaluación de sus recursos en la documentación de AWS Config para asegurarse de que CloudTrail se volvió a habilitar automáticamente.	Administrador de sistemas

Recursos relacionados

Configure CloudTrail

- Creación de un bucket de S3
- Política de bucket de Amazon S3 para CloudTrail
- Cómo añadir una política de bucket mediante la consola de Amazon S3
- Creación de un registro de seguimiento
- Configuración de automatización
- Cifrado de archivos de CloudTrail registro con claves administradas por AWS KMS (SSE-KMS)

Cree de un manual de procedimientos de Systems Manager Automation

- Etiquetado de documentos de Systems Manager
- Ejecución de una automatización sencilla

Configure la regla de corrección automática en AWS Config

- Administración de las reglas de AWS Config
- Corregir recursos de AWS no conformes con reglas de AWS Config

Recursos adicionales

- AWS CloudTrail : prácticas recomendadas de seguridad
- Introducción a AWS Systems Manager
- Introducción a AWS Config
- Cómo empezar a usar AWS CloudTrail

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Corrija automáticamente las instancias y los clústeres de bases de datos de Amazon RDS no cifrados

Creado por Ajay Rawat (AWS) y Josh Joy (AWS)

Entorno: PoC o piloto	Tecnologías: Seguridad, identidad, cumplimiento; Bases de datos	Servicios de AWS: AWS Config; AWS KMS; AWS Identity and Access Management; AWS Systems Manager; Amazon RDS

Resumen

Este patrón describe cómo corregir automáticamente las instancias y los clústeres de bases de datos no cifrados del Amazon Relational Database Service (Amazon RDS) en Amazon Web Services (AWS) mediante AWS Config, los manuales de procedimientos de AWS Systems Manager y las claves del AWS Key Management Service (AWS KMS).

Las instancias de base de datos RDS encriptadas proporcionan una capa adicional de protección de datos al proteger sus datos del acceso no autorizado al almacenamiento subyacente. Puede utilizar el cifrado de Amazon RDS para aumentar la protección de datos de las aplicaciones implementadas en la nube de AWS y para cumplir con los requisitos de conformidad para el cifrado en reposo. Puede habilitar el cifrado para una instancia de base de datos de RDS cuando la cree, pero no después de haberla creado. Sin embargo, puede añadir cifrado a una instancia de base de datos RDS sin cifrar creando una instantánea de su instancia de base de datos y, a continuación, creando una copia cifrada de esa instantánea. A continuación, puede restaurar una instancia de base de datos a partir de la instantánea encriptada para obtener una copia encriptada de su instancia de base de datos original.

Este patrón utiliza las reglas de AWS Config para evaluar las instancias y los clústeres de bases de datos de RDS. Aplica las correcciones mediante el uso de manuales de AWS Systems Manager, que definen las acciones que se deben realizar en los recursos de Amazon RDS no conformes, y claves de AWS KMS para cifrar las instantáneas de la base de datos. A continuación, aplica las políticas de control de servicios (SCP) para evitar la creación de nuevos clústeres e instancias de bases de datos sin cifrado.

El código de este patrón se proporciona en GitHub.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Los archivos del repositorio de código GitHub fuente de este patrón se descargan en su ordenador
- Una instancia de base de datos de RDS o un clúster sin cifrar
- Una clave de AWS KMS existente para cifrar instancias y clústeres de bases de datos de RDS
- Acceso para actualizar la política de recursos de claves de KMS
- AWS Config está habilitado en su cuenta de AWS (consulte Introducción a AWS Config en la documentación de AWS)

Limitaciones

- Puede activar la encriptación para una instancia de base de datos RDS sólo cuando la cree, no después de haberla creado.
- No se puede tener una réplica de lectura cifrada de una instancia de base de datos sin cifrar ni una réplica de lectura sin cifrar de una instancia de base de datos cifrada.
- No se puede restaurar una copia de seguridad ni una instantánea sin cifrar en una instancia de base de datos cifrada.
- El cifrado de Amazon RDS está disponible para la mayoría de las clases de instancias de bases de datos. Para ver una lista de excepciones, consulte Cifrado de los recursos de Amazon RDS en la documentación de Amazon RDS.
- Para copiar una instantánea cifrada de una región de AWS en otra, debe especificar la clave KMS de la región de AWS de destino. Esto se debe a que las claves de KMS son específicas de la región de AWS en la que se crean.
- La instantánea de origen permanece cifrada durante todo el proceso de copia. Amazon RDS utiliza el cifrado de sobre para proteger los datos durante el proceso de copia. Para más información, consulte Cifrado de sobre en la documentación de AWS KMS.
- No se puede descifrar una instancia de bases de datos cifrada. Sin embargo, puede exportar datos de una instancia de bases de datos cifrada e importar datos a una instancia de bases de datos sin cifrar.

- Debe eliminar una clave KMS solo cuando esté seguro de que ya no necesita usarla. Si no está seguro, considere la posibilidad de desactivar la clave KMS en lugar de eliminarla. Puede volver a habilitar una clave KMS deshabilitada si necesita volver a usarla más adelante, pero no puede recuperar una clave KMS eliminada.
- Si no elige conservar las copias de seguridad automatizadas, se eliminarán las copias de seguridad automatizadas que se encuentren en la misma región de AWS que la instancia de base de datos. No se pueden recuperar después de eliminar la instancia de base de datos.
- Las copias de seguridad automatizadas se retienen durante el período de retención establecido en la instancia de base de datos en el momento de eliminarla. Este período de retención establecido se produce independientemente de si decide crear o no una instantánea de base de datos final.
- Si la corrección automática está habilitada, esta solución cifra todas las bases de datos que tienen la misma clave de KMS.

Arquitectura

El siguiente diagrama ilustra la arquitectura de la CloudFormation implementación de AWS. Tenga en cuenta que también puede implementar este patrón mediante el AWS Cloud Development Kit (AWS CDK).

Herramientas

Herramientas

- AWS le CloudFormation ayuda a configurar automáticamente sus recursos de AWS. Le permite utilizar un archivo de plantilla para crear y eliminar una colección de recursos juntos como una sola unidad (una pila).
- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software para definir su infraestructura de nube en código y aprovisionarla mediante lenguajes de programación conocidos.

Servicios y características de AWS

- AWS Config realiza un seguimiento de la configuración de sus recursos de AWS y de sus relaciones con los demás recursos. También puede evaluar la conformidad de esos recursos de AWS. Este servicio utiliza reglas que se pueden configurar para evaluar los recursos de AWS en función de las configuraciones deseadas. Puede usar un conjunto de reglas administradas por

AWS Config para situaciones de conformidad comunes o puede crear sus propias reglas para situaciones personalizadas. Si se descubre que un recurso de AWS no cumple con las normas, puede especificar una acción correctiva mediante un manual de procedimientos de AWS Systems Manager y, si lo desea, enviar una alerta a través de un tema del Amazon Simple Notification Service (Amazon SNS). En otras palabras, puede asociar las acciones correctivas a las reglas de AWS Config y optar por ejecutarlas automáticamente para abordar los recursos no conformes sin intervención manual. Si un recurso sigue sin cumplir las normas tras la corrección automática, puede configurar la regla para que vuelva a intentar la corrección automática.

- Amazon Relational Database Service (Amazon RDS) facilita la configuración, la operación y el escalado de una base de datos relacional en la nube. El componente básico de Amazon RDS es la instancia de base de datos, que es un entorno de base de datos aislado en la nube de AWS. Amazon RDS ofrece una selección de tipos de instancia optimizados para adaptarse a diferentes casos de uso de bases de datos relacionales. Los tipos de instancias tienen varios tipos de combinaciones de CPU, memoria, almacenamiento y capacidad de red. También, brindan la flexibilidad para elegir la combinación adecuada de recursos para las bases de datos. Cada tipo de instancia incluye varios tamaños de instancia, lo que permite escalar sus bases de datos según los requisitos de la carga de trabajo de destino.
- AWS Key Management Service (AWS KMS) es un servicio administrado que permite crear y controlar fácilmente las claves de AWS KMS que se utilizan para cifrar datos. Una clave KMS es una representación lógica de una clave raíz. La clave de KMS incluye metadatos, como el ID de clave, la fecha de creación, la descripción y el estado de la clave.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- Las políticas de control de servicios (SCP) ofrece un control central sobre los máximos permisos disponibles para todas las cuentas de su organización. Las políticas de control de servicios le ayudan a garantizar que sus cuentas se mantengan dentro de las directrices de control de acceso de su organización. Las SCP no afectan a los usuarios ni a los roles de la cuenta de administración. Afectan solo a las cuentas miembro de su organización. Es absolutamente recomendable que no asocie políticas SCP al nodo raíz de la organización sin probar exhaustivamente el impacto que tendrá la política en las cuentas. En lugar de ello, cree una unidad organizativa (OU) en la que pueda mover sus cuentas de una en una, o al menos en incrementos pequeños, a fin de garantizar que no bloquee inadvertidamente a los usuarios de servicios clave.

Código

El código fuente y las plantillas de este patrón están disponibles en un GitHub repositorio. El patrón ofrece dos opciones de implementación: puede implementar una CloudFormation plantilla de AWS para crear la función de corrección que cifra las instancias y los clústeres de bases de datos de RDS, o puede usar la CDK de AWS. El repositorio tiene carpetas independientes para estas dos opciones.

En la sección Epics se proporcionan step-by-step instrucciones para implementar la plantilla. CloudFormation Si desea utilizar la AWS CDK, siga las instrucciones del archivo README.md del repositorio. GitHub

Prácticas recomendadas

- Habilite el cifrado de datos en reposo y en tránsito.
- Habilite AWS Config en todas las cuentas y regiones de AWS.
- Registre los cambios de configuración de todos los tipos de recursos.
- Rote con regularidad sus credenciales de IAM.
- Aproveche el etiquetado para AWS Config, lo que facilita la administración, búsqueda y filtrado de recursos.

Epics

Cree la función de corrección de IAM y el manual de procedimientos de AWS Systems Manager

Tarea	Descripción	Habilidades requeridas
Descargue la plantilla. CloudFormation	Descarga el `unencrypted-to-encrypted-rds.template.json` archivo del GitHub repositorio.	DevOps ingeniero
Crea la CloudFormation pila.	1. Inicie sesión en la consola de administración de AWS y abra la CloudFormation consola en https://console.aws.amazon.com/cloudformation/. 2. Inicie la plantilla `unencrypted-to-enc`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`rypted-rds.templat e.json` para crear una nueva pila. Para obtener más informaci ón sobre la implementación de plantillas, consulte la CloudFormation documenta ción de AWS.	
Revise CloudFormation los parámetros y valores.	1. Revise los detalles de la pila y actualice los valores en función de los requisitos de su entorno. 2. Elija Crear pila para implementar la plantilla.	DevOps ingeniero
Revise los recursos.	El estado cambia a CREATE_COMPLETE tras crear la pila. Revise los recursos creados (función de IAM, manual de administr ación de AWS Systems Manager) en la CloudForm ation consola.	DevOps ingeniero

Actualizar la política de claves de AWS KMS

Tarea	Descripción	Habilidades requeridas
Actualice su política de claves de KMS.	1. Asegúrese de que el alias de la clave `alias/RDS EncryptionAtRestKM SAlias` exista.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	2. La instrucción de la política de claves debe incluir el rol de corrección de IAM. (Comprueba los recursos creados por la CloudForm ation plantilla que utilizaste en la epopeya anterior). 3. En la siguiente política de claves, actualice las partes que aparecen en negrita para que coincidan con su cuenta y con el rol de IAM que se creó. `{ "Sid": "Allow access through RDS for all principals in the account that are authorized to use RDS", "Effect": "Allow", "Principal": { "AWS": "arn:aws: iam:: <your-AWS-account-ID>”:role/ <your-IAM-remediation-role>" }, "Action": ["kms:Encrypt", "kms:Decrypt", "kms:ReEn crypt*", "kms:Gene rateDataKey*", "kms:Crea teGrant",`	

Tarea	Descripción	Habilidades requeridas
	<pre>"kms:List Grants", "kms:Desc ribeKey"], "Resource": "*", "Condition": { "StringEquals": { "kms:ViaS ervice": "rds.us-e ast-1.amazonaws.com", "kms:Call erAccount": "<your-AW S-account-ID>" } } }</pre>	

Encuentre y corrija los recursos que no cumplen con las normas

Tarea	Descripción	Habilidades requeridas
Vea los recursos que no cumplen con las normas.	1. Para ver una lista de recursos no conformes, abra la consola de AWS Config en https://console.aws.amazon.com/config/. 2. En el panel de navegación, elija Reglas y, a continuación, elija la regla `rds-storage-encrypted` . Los recursos no conformes que se muestran en la consola de AWS Config serán	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	instancias, no clústeres. La automatización de la corrección cifra las instancias y los clústeres y crea una instancia recién cifrada o un clúster recién creado. Sin embargo, asegúrese de no corregir simultáneamente varias instancias que pertenezcan al mismo clúster. Antes de corregir cualquier instancia o volumen de base de datos de RDS, asegúrese de que la instancia de base de datos de RDS no esté en uso. Confirme que no se estén realizando operaciones de escritura mientras se crea la instantánea, para asegurarse de que la instantánea contiene los datos originales. Considere la posibilidad de establecer un período de mantenimiento durante el cual se ejecute la corrección.	

Tarea	Descripción	Habilidades requeridas
Resuelva los recursos no conformes.	1. Cuando esté listo y el período de mantenimiento esté activo, elija el recurso que desee corregir y, a continuación, elija Remediar. La columna Estado de la acción debería mostrar ahora la Ejecución de la acción en cola. 2. Vea el progreso y el estado de la corrección en Systems Manager. Abra la consola de AWS Systems Manager en https://console.aws.amazon.com/systems-manager/. En el panel de navegación, elija Automatización y, a continuación, seleccione el ID de ejecución de la automatización correspondiente para ver más detalles.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Verificar que la instancia de base de datos de RDS esté disponible.	Cuando se complete la automatización, estará disponible la instancia de base de datos RDS recién cifrada. La instancia de base de datos de RDS cifrada tendrá el prefijo `encrypted` seguido del nombre original. Por ejemplo, si el nombre de la instancia de base de datos de RDS no cifrada fuera `database-1` , la instancia de base de datos de RDS recién cifrada sería `encrypted-database-1` .	DevOps ingeniero
Termine la instancia no cifrada.	Una vez completada la corrección y validado el recurso recién cifrado, puede terminar la instancia no cifrada. Asegúrese de confirmar que el recurso recién cifrado coincide con el recurso no cifrado antes de cancelar cualquier recurso.	DevOps ingeniero

Aplicar los SCP

Tarea	Descripción	Habilidades requeridas
Aplique los SCP.	Aplique los SCP para evitar que en el futuro se creen instancias de bases de datos y clústeres sin cifrado. Use el	Ingeniero de seguridad

Tarea	Descripción	Habilidades requeridas
	`rds_encrypted.json` archivo que se proporciona en el GitHub repositorio para este fin y siga las instrucciones de la documentación de AWS.	

Recursos relacionados

Referencias

- Configuración de AWS Config
- Reglas personalizadas de AWS Config
- Conceptos de AWS KMS
- Documentos de AWS Systems Manager
- Políticas de control de servicios

Herramientas

- AWS CloudFormation
- AWS Cloud Development Kit (AWS CDK)

Guías y patrones

- Vuelva a habilitar AWS automáticamente CloudTrail mediante una regla de corrección personalizada en AWS Config

Información adicional

PREGUNTAS FRECUENTES

P: ¿Cómo funciona AWS Config?

A. Cuando activa AWS Config, primero descubre los recursos de AWS compatibles que existen en su cuenta y genera un elemento de configuración para cada recurso. AWS Config genera

también elementos de configuración cuando cambia la configuración de un recurso y mantiene los registros históricos de los elementos de configuración de los recursos desde el momento en que inicie el registrador de configuración. De forma predeterminada, AWS Config crea los elementos de configuración para cada recurso admitido en la región de AWS. Si no desea que AWS Config cree elementos de configuración para todos los recursos admitidos, puede especificar los tipos de recursos de los que desee realizar el seguimiento.

P: ¿Cómo se relacionan las reglas de AWS Config y AWS Config con AWS Security Hub?

R. AWS Security Hub es un servicio de seguridad y conformidad que proporciona una gestión de la postura de seguridad y conformidad como un servicio. Utiliza las reglas de AWS Config y AWS Config como mecanismo principal para evaluar la configuración de los recursos de AWS. Las reglas de AWS Config también se pueden usar para evaluar directamente la configuración de los recursos. Las reglas de configuración también son utilizadas por otros servicios de AWS, como AWS Control Tower y AWS Firewall Manager.

Cambie automáticamente las claves de acceso de los usuarios de IAM a escala con AWS Organizations y AWS Secrets Manager

Creado por Tracy Hickey (AWS), Gaurav Verma (AWS), Laura Seletos (AWS), Michael Davie (AWS) y Arvind Patel (AWS)

Entorno: PoC o piloto	Tecnologías: seguridad, identidad, cumplimiento	Servicios de AWS: AWS CloudFormation; Amazon CloudWatch Events; AWS Identity and Access Management; AWS Lambda; AWS Organizations; Amazon S3; Amazon SES; AWS Secrets Manager

Resumen

Importante: como práctica recomendada, AWS recomienda utilizar las funciones de AWS Identity and Access Management (IAM) en lugar de usuarios de IAM con credenciales a largo plazo, como claves de acceso. El enfoque documentado en este patrón está destinado únicamente a las implementaciones heredadas que requieren credenciales de API de AWS de larga duración. Para estas implementaciones, le recomendamos que considere opciones para usar credenciales a corto plazo, como el uso de perfiles de instancia de Amazon Elastic Compute Cloud (Amazon EC2) o Funciones de IAM en cualquier lugar. El enfoque de este artículo es solo para los casos en los que no pueda cambiar a usar credenciales de corta duración de forma inmediata y necesite que las credenciales de larga duración se roten según un cronograma. Con este enfoque, usted es responsable de actualizar periódicamente el código o la configuración de su aplicación antigua para utilizar las credenciales de API rotadas.

Las claves de acceso son credenciales a largo plazo para un usuario de IAM. La rotación periódica de sus credenciales de IAM ayuda a evitar que un conjunto comprometido de claves de acceso de IAM acceda a los componentes de su cuenta de AWS. La rotación de las credenciales de IAM también es una parte importante de las prácticas recomendadas de seguridad en IAM.

Este patrón le ayuda a rotar automáticamente las claves de acceso de IAM mediante CloudFormation plantillas de AWS, que se proporcionan en el repositorio de rotación de claves de GitHub IAM.

El patrón admite la implementación en una o varias cuentas. Si utiliza AWS Organizations, esta solución identifica todos los ID de cuentas de AWS de su organización y escala dinámicamente a medida que se eliminan cuentas o se crean cuentas nuevas. La función centralizada de AWS Lambda utiliza un rol de IAM asumido para ejecutar localmente las funciones de rotación en varias cuentas que seleccione.

- Las nuevas claves de acceso de IAM se generan cuando las claves de acceso existentes tienen 90 días de antigüedad.
- Las nuevas claves de acceso se almacenan en secreto en AWS Secrets Manager. Una política basada en recursos permite que solo la entidad principal de IAM especificada acceda al secreto y lo recupere. Si decide almacenar las claves en la cuenta de administración, las claves de todas las cuentas se almacenan en la cuenta de administración.
- La dirección de correo electrónico asignada al propietario de la cuenta de AWS en la que se crearon las nuevas claves de acceso recibe una notificación.
- Las claves de acceso anteriores se desactivan a los 100 días y, a continuación, se eliminan a los 110 días.
- Se envía una notificación centralizada por correo electrónico al propietario de la cuenta de AWS.

Las funciones de Lambda y Amazon realizan estas acciones CloudWatch automáticamente. A continuación, puede recuperar el nuevo par de claves de acceso y sustituirlas en el código o las aplicaciones. Los períodos de rotación, eliminación y desactivación se pueden personalizar.

Requisitos previos y limitaciones

- Al menos una cuenta de AWS activa.
- AWS Organizations, configuración y puesta en marcha (consulte el tutorial).
- Permisos para consultar AWS Organizations desde su cuenta de administración. Para obtener más información, consulte AWS Organizations y roles vinculados a servicios en la documentación de AWS Organizations.
- Un director de IAM que tiene permisos para lanzar la CloudFormation plantilla de AWS y los recursos asociados. Para obtener más información, consulte Otorgar permisos autogestionados en la CloudFormation documentación de AWS.
- Un bucket de Amazon Simple Storage Service (Amazon S3) para implementar los recursos.

- Amazon Simple Email Service (Amazon SES) salió del entorno aislado. Para obtener más información, consulte Salida del entorno aislado de Amazon SES en la documentación de Amazon SES.
- Si decide ejecutar Lambda en una nube privada virtual (VPC), debe crear los siguientes recursos antes de ejecutar la plantilla principal: CloudFormation
  - Una VPC.
  - Una subred
  - Puntos de conexión para Amazon SES, AWS Systems Manager, AWS Security Token Service (AWS STS), Amazon S3 y AWS Secrets Manager. (Puede ejecutar la plantilla de punto final que se proporciona en el repositorio de rotación de claves de GitHub IAM para crear estos puntos de enlace).
- El usuario y la contraseña del Protocolo simple de transferencia de correo (SMTP) almacenados en los parámetros de AWS Systems Manager (parámetros SSM). Los parámetros deben coincidir con los parámetros de la CloudFormation plantilla principal.

Arquitectura

Pila de tecnología

- Amazon CloudWatch
- Amazon EventBridge
- IAM
- AWS Lambda
- AWS Organizations
- Amazon S3

Arquitectura

Los siguientes diagramas muestran los componentes y flujos de trabajo de este patrón. La solución admite dos escenarios para almacenar las credenciales: en una cuenta de miembro y en la cuenta de administración.

Opción 1: almacenar las credenciales en una cuenta de miembro

Opción 2: almacenar las credenciales en la cuenta de administración

Los diagramas muestran el siguiente flujo de trabajo:

1. Un EventBridge evento inicia una función `account_inventory` Lambda cada 24 horas.
2. Esta función de Lambda consulta a AWS Organizations una lista de todos los ID, nombres de cuenta y correos electrónicos de cuentas de AWS.
3. La función de Lambda `account_inventory` inicia una función de Lambda `access_key_auto_rotation` para cada ID de cuenta de AWS y le pasa los metadatos para su procesamiento adicional.
4. La función de Lambda `access_key_auto_rotation` utiliza un rol de IAM asumido para acceder al ID de la cuenta de AWS. El script de Lambda ejecuta una auditoría de todos los usuarios y sus claves de acceso de IAM en la cuenta.
5. Si la antigüedad de la clave de acceso de IAM no ha superado el umbral de las prácticas recomendadas, la función de Lambda no realiza ninguna otra acción.
6. Si la antigüedad de la clave de acceso de IAM ha superado el umbral de las prácticas recomendadas, la función de Lambda `access_key_auto_rotation` determina qué acción de rotación se debe realizar.
7. Cuando es necesario realizar alguna acción, la función de Lambda `access_key_auto_rotation` crea y actualiza un secreto en AWS Secrets Manager si se genera una clave nueva. También se crea una política basada en recursos que sólo permite a la entidad principal de seguridad IAM especificada acceder al secreto y recuperarlo. En el caso de la opción 1, las credenciales se almacenan en Secrets Manager en la cuenta correspondiente. En el caso de la opción 2 (si la marca `StoreSecretsInCentralAccount` está establecida en True), las credenciales se almacenan en Secrets Manager, en la cuenta de administración.
8. Se inicia una función de Lambda `notifier` para notificar la actividad de rotación al propietario de la cuenta. Esta función recibe el ID de la cuenta de AWS, el nombre de la cuenta, el correo electrónico de la cuenta y las acciones de rotación que se realizaron.
9. La función de Lambda `notifier` consulta el bucket de S3 de implementación en busca de una plantilla de correo electrónico y la actualiza dinámicamente con los metadatos de actividad pertinentes. Luego, el correo electrónico se envía a la dirección de correo electrónico del propietario de la cuenta.

Notas:

- Esta solución es compatible con la resiliencia en varias zonas de disponibilidad. Sin embargo, no admite la resiliencia en varias regiones de AWS. Para obtener soporte en varias regiones, puede implementar la solución en la segunda región y mantener desactivada la EventBridge regla de rotación de claves. A continuación, puede activar la regla cuando desee ejecutar la solución en la segunda región.
- Puede ejecutar esta solución en modo auditoría. En el modo de auditoría, las claves de acceso de IAM no se modifican, pero se envía un correo electrónico para notificar a los usuarios. Para ejecutar la solución en modo auditoría, defina la marca `DryRunFlag` en True cuando ejecute la plantilla de rotación de claves o en la variable de entorno de la función de Lambda `access_key_auto_rotation`.

Automatizar y escalar

Las CloudFormation plantillas que automatizan esta solución se proporcionan en el repositorio de rotación de claves de GitHub IAM y se enumeran en la sección Código. En AWS Organizations, puede utilizarla CloudFormation StackSetspara implementar la `ASA-iam-key-auto-rotation-iam-assumed-roles.yaml` CloudFormation plantilla en varias cuentas en lugar de implementar la solución de forma individual en cada cuenta de miembro.

Herramientas

Servicios de AWS

- Amazon le CloudWatch ayuda a monitorizar las métricas de sus recursos de AWS y las aplicaciones que ejecuta en AWS en tiempo real.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Organizations es un servicio de administración de cuentas que permite agrupar varias cuentas AWS en una organización que usted crea y administra de manera centralizada.
- AWS Secrets Manager ayuda a reemplazar las credenciales codificadas en el código, incluidas las contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación.

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Amazon Simple Email Service (Amazon SES) facilita poder enviar y recibir correos electrónicos a través de los dominios y direcciones de correo electrónico propios.
- Amazon Simple Notification Service (Amazon SNS) permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- Amazon Virtual Private Cloud (Amazon VPC) permite lanzar recursos de AWS en una red virtual que se haya definido. Esa red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.
- Los puntos de enlace de Amazon VPC proporcionan una interfaz para conectarse a los servicios impulsados por AWS PrivateLink, incluidos muchos servicios de AWS. Para cada subred que especifique de su VPC, se crea una interfaz de red de punto de conexión en la subred y se le asigna una dirección IP privada del intervalo de direcciones de la subred.

Código

CloudFormation Las plantillas de AWS, los scripts de Python y la documentación de runbook necesarios están disponibles en el repositorio de rotación de claves de GitHub IAM. Las plantillas se implementan de la siguiente manera.

Plantilla	Implementar en	Notas
`ASA-iam-key-auto-rotation-and-notifier-solution.yaml`	Cuenta de implementación	Esta es la plantilla principal de la solución.
`ASA-iam-key-auto-rotation-iam-assumed-roles.yaml`	Cuentas de uno o varios miembros en las que desee rotar las credenciales	Puede utilizar conjuntos de CloudFormation pilas para implementar esta plantilla en varias cuentas.
`ASA-iam-key-auto-rotation-list-accounts-role.yaml`	Cuenta central/gestión	Utilice esta plantilla para mantener un inventario de las cuentas en AWS Organizations.

`ASA-iam-key-auto-rotation-vpc-endpoints.yaml`	Cuenta de implementación	Utilice esta plantilla para automatizar la creación de puntos de conexión solo si desea ejecutar las funciones de Lambda en una VPC (establezca el parámetro `RunLambdaInVPC` en True en la plantilla principal).

Epics

Configurar la solución

Tarea	Descripción	Habilidades requeridas
Elija su bucket de S3 de implementación.	Inicie sesión en la consola de administración de AWS de su cuenta, abra la consola de Amazon S3 y, a continuación, elija el bucket de S3 para su implementación. Si desea implementar la solución para varias cuentas en AWS Organizations, inicie sesión en la cuenta de administración de su organización.	Arquitecto de la nube
Clonar el repositorio.	Clona el repositorio de rotación de claves de GitHub IAM en tu escritorio local.	Arquitecto de la nube
Carguar archivos en el bucket de S3.	Suba los archivos clonados a su bucket S3. Use la siguiente estructura de carpetas predeterminada para copiar y pegar todos los archivos y	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	directorios clonados: `asa/asa-iam-rotation` Nota: Puede personalizar esta estructura de carpetas en las CloudFormation plantillas.	
Modifique la plantilla de correo electrónico.	Modifique la plantilla de correo electrónico `iam-auto-key-rotation-enforcement.html` (que se encuentra en la carpeta `template`) según sus necesidades. Sustituya `[Department Name Here]` al final de la plantilla por el nombre de su departamento.	Arquitecto de la nube

Implementar la solución.

Tarea	Descripción	Habilidades requeridas
Inicie la CloudFormation plantilla para la rotación de claves.	1. Inicie la plantilla `ASA-iam-key-auto-rotation-and-notifier-solution.yaml` en la cuenta de implementación. Para obtener más información, consulte Selección de una plantilla de pila en la CloudFormation documentación.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	2. Especifique los valores de los parámetros, entre los que se incluyen: • CloudFormation Nombre del depósito de S3 (`S3BucketName`): el nombre del depósito de S3 de despliegue que contiene el código Lambda. • CloudFormation Prefijo del bucket de S3 (`S3BucketPrefix`): prefijo del bucket de S3. • Nombre de rol de IAM asumido (`IAMRoleName`): el nombre del rol que asumirá la función de Lambda `key-rotation` para rotar las claves. • Nombre de la función de ejecución de IAM (`ExecutionRoleName`): nombre de la función de ejecución de IAM que utiliza la función de Lambda `key-rotation`. • Nombre de la función de ejecución de IAM (`InventoryExecutionRoleName`): nombre de	

Tarea	Descripción	Habilidades requeridas
	la función de ejecución de IAM que utiliza la función de Lambda `account_inventory` . • Marca de ejecución en seco (modo auditoría) (`DryRunFlag`): establézcalo en True para activar el modo de auditoría (predeter minado). Configúrelo en False para activar el modo de aplicación. • Cuenta para enumerar las cuentas de la organización (`OrgListAccount`): el ID de cuenta de la cuenta central o de administr ación que se utilizará para enumerar las cuentas de la organizac ión. • Nombre del rol de la lista de cuentas (`OrgListRo le`): el nombre del rol que se utilizará para enumerar las cuentas de la organización. • Marca de almacenam iento de secretos para la cuenta central (`StoreSecr etsInCent`	

Tarea	Descripción	Habilidades requeridas
	`ralAccount`): se establece en True para almacenar los secretos en la cuenta central. Configúrelo en False para almacenar los secretos en la cuenta correspon diente. • Regiones para replicar las credencia les (`Credentia lReplicat ionRegions`): las regiones de AWS en las que desea replicar las credenciales (Secrets Manager), separadas por comas; por ejemplo, `us-east-2,us-west-1,us-west-2` . Omita la región en la que está creando la pila. • Ejecutar Lambda en VPC (`RunLambdaInVpc`): se establece en True para ejecutar funciones de Lambda en una VPC específica. Debe haber creado puntos de conexión de VPC y conectar una puerta de enlace NAT a la subred que contiene la función de Lambda. Para más	

Tarea	Descripción	Habilidades requeridas
	información, consulte el artículo de re:Post sobre esta opción. • ID de la VPC para las funciones de Lambda (`VpcId`), CIDR de VPC para la regla de grupo de seguridad (`VpcCidr`) e ID de subred para las funciones de Lambda (`SubnetId`): proporcio ne información sobre la VPC, el CIDR y la subred si establece `RunLambda InVpc` en True. • Dirección de correo electrónico del administr ador (`AdminEmai lAddress`): una dirección de correo electrónico válida a la que enviar notificaciones. • ID de AWS Organizat ions (`AWSOrgID`): el identificador único de su organización. Este identificador comienza con `o-` y va seguido de entre 10 y 32 letras en minúscula o dígitos. • Nombre del archivo de plantilla de correo electrónico [Modo auditoría] (`EmailTemp`	

Tarea	Descripción	Habilidades requeridas
	`lateAudit`) y [Modo aplicar] (`EmailTemp lateEnforce`): nombre del archivo de la plantilla HTML de correo electrónico que el módulo `notifier` enviará para los modos de auditoría y cumplimiento. • Nombre del parámetro SSM del usuario SMTP (`SMTPUserParamName`) y nombre del parámetro SSM de la contraseña SMTP (`SMTPPassw ordParamName`): información de usuario y contraseña del Protocolo simple de transferencia de correo (SMTP).	

Tarea	Descripción	Habilidades requeridas
Inicie la CloudFormation plantilla para los roles asumidos.	1. En la CloudFormation consola de AWS, ejecute la `ASA-iam-key-auto-rotation-iam-assumed-roles.yaml` plantilla para cada cuenta en la que desee rotar las claves. Si tiene más de una cuenta, puede implementar la CloudFormation plantilla principal en su cuenta de administración como una pila e implementar la `ASA-iam-key-auto-rotation-iam-assumed-roles.yaml` plantilla con los conjuntos de CloudFormation pilas en todas las cuentas requeridas. Para obtener más información, consulte Trabajar con AWS CloudFormation StackSets en la CloudFormation documentación. 2. Especifique los valores de los siguientes parámetros: • Nombre de rol de IAM asumido (`IAMRoleName`): el nombre del rol IAM que será asumido por la función `access_key_auto_rotation` de Lambda.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	Puede mantener el valor predeterminado. • Nombre del rol de ejecución de IAM (`ExecutionRoleName`): el rol de IAM que asumirá el rol de subcuenta para ejecutar la función de Lambda. • ID de cuenta principal de AWS (`PrimaryAccountID`): el ID de cuenta de AWS en el que se implementará la plantilla principal. • Grupo de exención de IAM (`IAMExemptionGroup`): el nombre del grupo de IAM que se utiliza para facilitar la exclusión de las cuentas de IAM de la rotación automática de claves.	

Tarea	Descripción	Habilidades requeridas
Inicie la CloudFormation plantilla para el inventario de cuentas.	1. Inicie la plantilla `ASA-iam-key-auto-rotation-list-accounts-role.yaml` en la cuenta central o de administración 2. Especifique los valores de los siguientes parámetros: • Nombre de rol de IAM asumido (`IAMRoleName`): el nombre del rol IAM que asumirá la función `access_key_auto_rotation` de Lambda. • Nombre del rol de ejecución de IAM para la cuenta de Lambda (`AccountExecutionRoleName`): el nombre del rol de IAM que asumirá la función `notifier` de Lambda. • Nombre del rol de ejecución de IAM para la rotación Lambda (`RotationExecutionRoleName`): nombre del rol de IAM que asumirá la función de Lambda `access_key_auto_rotation`. • ID de cuenta principal de AWS (`PrimaryAc`	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	`countID`): el ID de cuenta de AWS en el que se implementará la plantilla principal.	
Inicie la CloudFormation plantilla para los puntos finales de la VPC.	Esta tarea es opcional. 1. Inicie la plantilla `ASA-iam-key-auto-rotation-vpc-endpoints.yaml` en la cuenta de implement ación. 2. Especifique los valores de los siguientes parámetros: • ID de VPC (`pVpcId`), ID de subred (`pSubnetId`) e intervalo de CIDR para la VPC (`pVPCCidr`): proporcionan información sobre la VPC, el CIDR y la subred. • Establezca el parámetro para cada punto de conexión de VPC en True. Si ya tiene puntos de conexión, puede elegir False.	Arquitecto de la nube

Recursos relacionados

- Prácticas recomendadas de seguridad en IAM (documentación de IAM)
- AWS Organizations y roles vinculados al servicio (documentación sobre AWS Organizations)
- Selección de una plantilla de pila (documentación) CloudFormation

- Trabajar con AWS CloudFormation StackSets (CloudFormation documentación)

Valide e implemente automáticamente las políticas y funciones de IAM en una cuenta de AWS mediante CodePipeline IAM Access Analyzer y macros de AWS CloudFormation

Creado por Helton Henrique Ribeiro (AWS) y Guilherme Simoes (AWS)

Repositorio de código: canalización de funciones de IAM	Entorno: PoC o piloto	Tecnologías: seguridad, identidad, conformidad; DevOps
Servicios de AWS: AWS CloudFormation CodeBuild; AWS CodeCommit; AWS CodePipeline; AWS Lambda; AWS SAM		

Resumen

Este patrón describe los pasos y proporciona código para crear un proceso de implementación que permita a sus equipos de desarrollo crear políticas y roles de AWS Identity and Access Management (IAM) en sus cuentas de Amazon Web Services (AWS). Este enfoque ayuda a su organización a reducir los gastos generales de sus equipos operativos y a acelerar el proceso de implementación. También ayuda a sus desarrolladores a crear roles y políticas de IAM que sean compatibles con sus controles de gobierno y seguridad actuales.

El enfoque de este patrón utiliza AWS Identity and Access Management Access Analyzer para validar las políticas de IAM que desea adjuntar a las funciones de IAM y utiliza AWS CloudFormation para implementar las funciones de IAM. Sin embargo, en lugar de editar directamente el archivo de CloudFormation plantilla de AWS, su equipo de desarrollo crea políticas y funciones de IAM con formato JSON. Una CloudFormation macro de AWS transforma estos archivos de políticas con formato JSON en tipos de recursos de AWS CloudFormation IAM antes de comenzar la implementación.

La canalización de implementación (`RolesPipeline`) tiene las etapas de origen, validación e implementación. Durante la fase de origen, su equipo de desarrollo envía los archivos JSON que

contienen la definición de las funciones y políticas de IAM a un repositorio de AWS CodeCommit . CodeBuild A continuación, AWS ejecuta un script para validar esos archivos y los copia en un bucket de Amazon Simple Storage Service (Amazon S3). Como sus equipos de desarrollo no tienen acceso directo al archivo de CloudFormation plantilla de AWS almacenado en un depósito de S3 independiente, deben seguir el proceso de creación y validación de archivos JSON.

Por último, durante la fase de implementación, AWS CodeDeploy utiliza una CloudFormation pila de AWS para actualizar o eliminar las políticas y funciones de IAM de una cuenta.

Importante: El flujo de trabajo de este patrón es una prueba de concepto (POC) y le recomendamos que solo lo utilice en un entorno de prueba. Si desea utilizar el enfoque de este patrón en un entorno de producción, consulte las Prácticas recomendadas de seguridad en IAM en la documentación de IAM y realice los cambios necesarios en sus roles de IAM y en los servicios de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Un bucket de S3 nuevo o existente para la canalización `RolesPipeline`. Asegúrese de que las credenciales de acceso que está utilizando tengan permisos para cargar objetos en este bucket.
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada. Para obtener más información, consulte Instalar, actualizar y desinstalar la CLI de AWS en la documentación de la CLI de AWS.
- CLI de AWS Serverless Application Model (AWS SAM), instalada y configurada. Para obtener más información al respecto, consulte Instalación de la CLI de AWS SAM en la documentación de AWS SAM.
- Python 3, instalado en su máquina local. Para obtener más información, consulte la documentación de Python.
- Un cliente Git, Instalado y configurado.
- El GitHub `IAM roles pipeline` repositorio, clonado en su máquina local.
- Políticas y roles de IAM con formato JSON existentes. Para obtener más información al respecto, consulta el ReadMearchivo en el `IAM roles pipeline` repositorio de Github.
- Su equipo de desarrolladores no debe tener permisos para editar los CodeDeploy recursos de AWS CodePipeline y de esta solución. CodeBuild

Limitaciones

- El flujo de trabajo de este patrón es una prueba de concepto (POC) y le recomendamos que solo lo utilice en un entorno de prueba. Si desea utilizar el enfoque de este patrón en un entorno de producción, consulte las Prácticas recomendadas de seguridad en IAM en la documentación de IAM y realice los cambios necesarios en sus roles de IAM y en los servicios de AWS.

Arquitectura

En el siguiente diagrama, se muestra cómo validar e implementar automáticamente las funciones y políticas de IAM en una cuenta mediante el uso de CodePipeline macros de AWS y IAM Access Analyzer. CloudFormation

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un desarrollador escribe archivos JSON que contienen las definiciones de las políticas y los roles de IAM. El desarrollador envía el código a un CodeCommit repositorio y, a CodePipeline continuación, inicia la canalización. `RolesPipeline`
2. CodeBuild valida los archivos JSON mediante IAM Access Analyzer. Si se detecta algún problema de seguridad o relacionado con errores, se detiene el proceso de implementación.
3. Si no se detecta ningún problema de seguridad o relacionado con errores, los archivos JSON se envían al bucket de S3 `RolesBucket`.
4. A continuación, una CloudFormation macro de AWS implementada como una función de AWS Lambda lee los archivos JSON del `RolesBucket` bucket y los transforma en tipos de recursos de AWS CloudFormation IAM.
5. Una CloudFormation pila de AWS predefinida instala, actualiza o elimina las políticas y funciones de IAM de la cuenta.

Automatizar y escalar

CloudFormation Las plantillas de AWS que implementan automáticamente este patrón se proporcionan en el repositorio de canalización de roles de GitHub IAM.

Herramientas

- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- IAM Access Analyzer le ayuda a identificar los recursos de su organización y sus cuentas, como buckets de S3 o roles de IAM, que se comparten con una entidad externa. Esto le ayuda a identificar el acceso no deseado a sus recursos y datos.
- AWS Serverless Application Model (AWS SAM) es un marco de código abierto que permite crear aplicaciones sin servidor en la nube de AWS.

Código

El código fuente y las plantillas de este patrón están disponibles en el repositorio de la canalización de roles de GitHub IAM.

Epics

Clone el repositorio

Tarea	Descripción	Habilidades requeridas
Clone el repositorio de muestra.	Clona el repositorio de canalización de roles de GitHub IAM en tu máquina local.	Desarrollador de aplicaciones, AWS general

Implemente la canalización RolesPipeline

Tarea	Descripción	Habilidades requeridas
Implemente la canalización.	1. Vaya al directorio que contiene el repositorio clonado.	Desarrollador de aplicaciones, AWS general

Tarea	Descripción	Habilidades requeridas
	2. Ejecute el comando `make deploy bucket=<bucket_name>` . Importante: debe sustituir `<bucket_name>` por el nombre de su bucket de S3 existente. 3. Ejecute el comando `aws codepipeline get-pipeline –name RolesPipeline` para comprobar si la implementación se ha realizado correctamente.	
Clone el repositorio de la canalización.	1. La CloudFormation pila de `RolesPipeline` AWS crea el `roles-pipeline-repo` CodeCommit repositorio. 2. Inicie sesión en la consola de administración de AWS, abra la CodeCommit consola de AWS y, a continuación, copie la URL del CodeCommit repositorio para clonarlo en su máquina local. Para obtener más información al respecto, consulte Conectarse a un CodeCommit repositorio de AWS en la CodeCommit documentación de AWS.	Desarrollador de aplicaciones, AWS general

Pruebe la RolesPipeline canalización

Tarea	Descripción	Habilidades requeridas
Pruebe la RolesPipeline canalización con políticas y funciones de IAM válidas.	1. Cree archivos JSON para sus políticas y roles de IAM. Puede utilizar los ejemplos del `role-example` directorio del GitHub `IAM roles pipeline` repositorio. 2. Defina sus políticas y roles de IAM con las configuraciones requeridas. Importante: Asegúrese de seguir el formato descrito en el `ReadMe` archivo del GitHub `IAM roles pipeline` repositorio. 3. Inserte las modificaciones en el `roles-pipeline-repo` CodeCommit repositorio. 4. Verifique la implement ación de la canalización `RolesPipeline` . 5. Asegúrese de que las políticas y los roles de IAM estén implementados correctamente en la cuenta. 6. Valide si existe un límite de permisos asociado a las políticas o los roles de IAM. Para obtener más informaci ón, consulte Límites de permisos para las entidades	Desarrollador de aplicaciones, AWS general

Tarea	Descripción	Habilidades requeridas
	de IAM en la documentación de IAM.	
Pruebe la RolesPipeline canalización con políticas y funciones de IAM no válidas.	1. Modifique el `roles-pipeline-repo` CodeCommit repositorio e incluya funciones o políticas de IAM no válidas. Por ejemplo, puede utilizar una acción que no exista o una versión de la política de IAM no válida. 2. Verifique la implementación de la canalización. IAM Access Analyzer detiene la canalización durante la fase de validación si detecta políticas o roles de IAM no válidos.	Desarrollador de aplicaciones, AWS general

Eliminación de sus recursos

Tarea	Descripción	Habilidades requeridas
Prepárese para la limpieza.	Vacíe los buckets de S3 y, a continuación, ejecute el comando `destroy`.	Desarrollador de aplicaciones, AWS general
Elimine la RolesStack pila.	1. La `RolesPipeline` canalización crea una CloudFormation pila de `RolesStack` AWS que implementa las políticas y funciones de IAM. Debe eliminar esta pila antes de	Desarrollador de aplicaciones, AWS general

Tarea	Descripción	Habilidades requeridas
	eliminar la canalización `RolesPipeline` . 2. Inicie sesión en la consola de administración de AWS, abra la CloudForm ation consola de AWS y, a continuación, elija la `RolesStack` pila y elija Eliminar.	
Elimine la RolesPipeline pila.	Para eliminar la CloudForm ation pila de `RolesPipe line` AWS, sigue las instrucciones del ReadMearchivo del `IAM roles pipeline` repositorio de Github.	Desarrollador de aplicaciones, AWS general

Recursos relacionados

- IAM Access Analyzer: validación de políticas (Blog de noticias de AWS)
- Uso de CloudFormation macros de AWS para realizar un procesamiento personalizado en plantillas (CloudFormation documentación de AWS)
- Creación de funciones Lambda con Python (documentación de AWS Lambda)

Integración bidireccional de AWS Security Hub con el software Jira

Creado por Joaquín Manuel Rinaudo (AWS)

Repositorio de código: Integración de Security Hub a JIRA	Entorno: PoC o piloto	Tecnologías: seguridad, identidad, conformidad
Carga de trabajo: todas las demás cargas de trabajo	Servicios de AWS: AWS Lambda; AWS Security Hub; Amazon CloudWatch	

Resumen

Esta solución crea una integración bidireccional entre AWS Security Hub y Jira. Esta solución le permite crear y actualizar de forma automática y manual los tickets de JIRA a partir de los resultados de Security Hub. Los equipos de seguridad pueden usar esta integración para notificar a los equipos de desarrollo cualquier resultado grave en materia de seguridad que requiera la adopción de medidas.

La solución le permite:

- Seleccionar qué controles de Security Hub crean o actualizan automáticamente tickets en Jira.
- En la consola de Security Hub, usar las acciones personalizadas de Security Hub para escalar tickets manualmente en Jira.
- Asignar automáticamente tickets en Jira en función de las etiquetas de cuentas de AWS definidas en AWS Organizations. Si esta etiqueta no está definida, se asignan de forma predeterminada.
- Eliminar automáticamente los resultados de Security Hub que estén marcados como falsos positivos o riesgos aceptados en Jira.
- Cerrar automáticamente un ticket de Jira cuando su resultado relacionado esté archivado en Security Hub.
- Reabrir tickets de Jira cuando se repitan resultados de Security Hub.

Flujo de trabajo de Jira

La solución emplea un flujo de trabajo de Jira personalizado que permite a los desarrolladores gestionar y documentar los riesgos. A medida que el problema avanza en el flujo de trabajo, la integración bidireccional garantiza que el estado del ticket de Jira y el resultado de Security Hub se mantengan sincronizados en todos los flujos de trabajo de ambos servicios. Este flujo de trabajo es un derivado de SecDevOps Risk Workflow de Dinis Cruz, con licencia CC BY 4.0. Recomendamos añadir una condición de flujo de trabajo de Jira para que solo los miembros de su equipo de seguridad puedan cambiar el estado del ticket.

Para ver un ejemplo de ticket de Jira generado automáticamente por esta solución, consulte la sección de Información adicional de este patrón.

Requisitos previos y limitaciones

Requisitos previos

- Si desea implementar esta solución en un entorno de AWS con múltiples cuentas:
  - Su entorno de múltiples cuentas está activo y gestionado por AWS Organizations.
  - Security Hub está activado en sus cuentas de AWS.
  - En AWS Organizations, ha designado una cuenta de administrador de Security Hub.
  - Tiene un rol de IAM multicuenta con permisos `AWSOrganizationsReadOnlyAccess` para la cuenta de administración de AWS Organizations.
  - (Opcional) Ha etiquetado sus cuentas de AWS con `SecurityContactID`. Esta etiqueta se usa para asignar tickets de Jira a los contactos de seguridad definidos.
- Si desea implementar esta solución en una sola cuenta de AWS:
  - Dispone de una cuenta de AWS activa.
  - Security Hub está activado en sus cuentas de AWS.
- Una instancia de Jira Server

  Importante: esta solución es compatible con el uso de Jira Cloud. Sin embargo, Jira Cloud no admite la importación de flujos de trabajo XML, por lo que deberá volver a crear el flujo de trabajo manualmente en Jira.
- Permisos de administrador en Jira
- Uno de los siguientes tokens de Jira:

- Para Jira Enterprise, un token de acceso personal (PAT). Para obtener más información, consulte Uso de tokens de acceso personal (soporte de Atlassian).
- Para Jira Cloud, un token de la API de Jira. Para obtener más información, consulte Gestionar tokens de API (soporte de Atlassian).

Arquitectura

Esta sección ilustra la arquitectura de la solución en distintos escenarios, por ejemplo, cuando el desarrollador y el ingeniero de seguridad deciden aceptar el riesgo o deciden solucionar el problema.

Escenario 1: el desarrollador aborda el problema

1. Security Hub genera un resultado relacionado con un control de seguridad específico, como los del estándar de prácticas recomendadas de AWS Foundational Security.
2. Un CloudWatch evento de Amazon asociado al hallazgo y a la `CreateJIRA` acción inicia una función de AWS Lambda.
3. La función de Lambda usa su archivo de configuración y el campo `GeneratorId` del resultado para evaluar el escalado del resultado.
4. La función de Lambda determina que el resultado debe escalarse y obtiene la etiqueta de cuenta `SecurityContactID` de AWS Organizations en la cuenta de administración de AWS. Esta ID está asociada al desarrollador y se usa como ID de asignación del ticket de Jira.
5. La función de Lambda usa las credenciales almacenadas en AWS Secrets Manager para crear un ticket en Jira. Jira notifica al desarrollador.
6. El desarrollador aborda el problema de seguridad subyacente en el resultado y, en Jira, cambia el estado del ticket a `TEST FIX`.
7. Security Hub actualiza el resultado como `ARCHIVED` y se genera un nuevo evento. Este evento hace que la función de Lambda cierre automáticamente el ticket de Jira.

Escenario 2: el desarrollador decide aceptar el riesgo

1. Security Hub genera un resultado relacionado con un control de seguridad específico, como los del estándar de prácticas recomendadas de AWS Foundational Security.
2. Un CloudWatch evento asociado al hallazgo y a la `CreateJIRA` acción inicia una función Lambda.

3. La función de Lambda usa su archivo de configuración y el campo `GeneratorId` del resultado para evaluar el escalado del resultado.
4. La función de Lambda determina que el resultado debe escalarse y obtiene la etiqueta de cuenta `SecurityContactID` de AWS Organizations en la cuenta de administración de AWS. Esta ID está asociada al desarrollador y se usa como ID de asignación del ticket de Jira.
5. La función de Lambda usa las credenciales almacenadas en AWS Secrets Manager para crear un ticket en Jira. Jira notifica al desarrollador.
6. El desarrollador decide aceptar el riesgo y, en Jira, cambia el estado del ticket a `AWAITING RISK ACCEPTANCE`.
7. El ingeniero de seguridad revisa la solicitud y considera que la justificación empresarial es adecuada. El ingeniero de seguridad cambia el estado del ticket de Jira a `ACCEPTED RISK`. El ticket de Jira se cierra.
8. Un evento CloudWatch diario inicia la función Lambda de actualización, que identifica los tickets de JIRA cerrados y actualiza los hallazgos relacionados con Security Hub como. `SUPPRESSED`

Herramientas

- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- Amazon CloudWatch Events le ayuda a supervisar los eventos del sistema para sus recursos de AWS mediante el uso de reglas para hacer coincidir los eventos y dirigirlos a funciones o transmisiones.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Organizations es un servicio de administración de cuentas que le permite agrupar varias cuentas de AWS en una organización que usted crea y administra de manera centralizada.
- AWS Secrets Manager le permite reemplazar las credenciales codificadas en el código, incluidas las contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación.

- AWS Security Hub proporciona una visión completa de su estado de seguridad en AWS. También le permite comprobar si su entorno de AWS cumple con los estándares y las prácticas recomendadas del sector de seguridad.

Repositorio de código

El código de este patrón está disponible en GitHub el repositorio aws-securityhub-jira-software-integration. Incluye el código de muestra y el flujo de trabajo de Jira para esta solución.

Epics

Configure Jira

Tarea	Descripción	Habilidades requeridas
Importe el flujo de trabajo.	Como administrador de Jira, importe el archivo `issue-workflow.xml` a su instancia de Jira Server. Este archivo se encuentra en el repositorio aws-securityhub-jira-software-integration de GitHub. Para obtener más instrucciones, consulte Usar XML para crear un flujo de trabajo (documentación de Jira).	Administrador de Jira
Active y asigne el flujo de trabajo.	Los flujos de trabajo estarán inactivos hasta que los asigne a un esquema de flujo de trabajo. A continuación, asigne el esquema de flujo de trabajo a un proyecto. 1. En su proyecto, asegúrese de haber identificado un esquema de tipo de problema para el proyecto.	Administrador de Jira

Tarea	Descripción	Habilidades requeridas
	Puede crear un nuevo tipo de problema o seleccionar uno existente, como Bug. 2. Asigne el flujo de trabajo importado a un esquema de flujo de trabajo siguiendo las instrucciones de Activar un flujo de trabajo (documentación de Jira). 3. Asigne el esquema de flujo de trabajo a un proyecto siguiendo las instrucciones de Asociar un esquema de flujo de trabajo a un proyecto (documentación de Jira).	

Configure los parámetros de la solución

Tarea	Descripción	Habilidades requeridas
Configure los parámetros de la solución.	1. En la carpeta conf, abra `params_prod.shfile` . 2. Proporcione valores para los siguientes parámetros: • `ORG_ACCOUNT_ID` – LA ID de cuenta de su cuenta de administración de AWS Organizations. La solución lee las etiquetas de las cuentas y asigna los tickets a los contactos de seguridad	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	específicos definidos en dichas etiquetas de cuentas de AWS. • `ORG_ROLE` – El nombre del rol de IAM utilizado para acceder a la cuenta de administración de AWS Organizations. Este rol debe tener permisos de `OrganizationsReadOnlyAccess` . • `EXTERNAL_ID` – Un parámetro opcional si usa una ID externa para asumir el rol de IAM definido en `ORG_ROLE`. Para más información, consulte Cómo utilizar un ID externo (documentación de IAM). • `JIRA_DEFAULT_ASSIGNEE` – Esta es la ID de Jira a la que se asignan, de forma predeterminada, todos los problemas de seguridad. Esta asignación predeterminada se usa en caso de que la cuenta no esté etiquetada correctamente o no se pueda asumir el rol. • `JIRA_INSTANCE` – La dirección HTTPS de	

Tarea	Descripción	Habilidades requeridas
	su servidor de Jira en el siguiente formato: `team-<team-id>.atlassian.net/` • `JIRA_PROJECT_KEY` – El nombre de la clave de proyecto de Jira empleada para crear los tickets, como `SEC` o `TEST`. Este proyecto ya debe existir en Jira. • `ISSUE_TYPE` – El nombre del esquema de tipo de problema asignado al proyecto en Jira, como `Bug` o `Security Issue`. • `REGIONS` – Lista de códigos de región de AWS en los que desea implementar esta solución, por ejemplo `eu-west-1` . 3. Guarde y cierre el archivo de parámetros de la solución.	

Tarea	Descripción	Habilidades requeridas
Identifique los resultados que desea automatizar.	1. Abra la consola de Security Hub en https://console.aws.amazon.com/securityhub/ 2. En el panel de navegación de Security Hub, elija Resultados. 3. Seleccione el título del resultado. 4. Seleccione el ID del resultado. Esto muestra el JSON completo del resultado. 5. En el JSON, copie la cadena del campo `GeneratorId` . Este valor está en formato de resultados de seguridad de AWS (ASFF). Por ejemplo, `aws-foundational-security-best-practices/v/1.0.0/S3.1` corresponde a los resultados del control de seguridad S3.1 S3 Block Public Access setting should be enabled. 6. Repita estos pasos hasta que haya copiado todos los valores `GeneratorID` de los resultados que desee automatizar.	

Tarea	Descripción	Habilidades requeridas
Agregue los resultados al archivo de configuración.	1. En src/code, abra el archivo `config.jsonconfig` . 2. Pegue los valores `GeneratorID` que recuperó anteriormente en el parámetro `default`, usando comas para separar cada ID. 3. Guarde y cierre el archivo de configuración. En el siguiente ejemplo de código se muestra la automatización de los resultados `aws-foundational-security-best-practices/v/1.0.0/SNS.1` y `aws-foundational-security-best-practices/v/1.0.0/S3.1` . `{ "Controls" : { "eu-west-1": [ "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.22" ], "default": [ aws-foundational-security-best-practices/v/1.0.0/SNS.1,`	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	<pre>aws-foundational- security-best-p ractices/v/1.0.0/S3.1] } }</pre> Nota: Puede automatizar diferentes resultados para cada región de AWS. Una práctica recomendada para evitar la duplicación de resultados es seleccionar una sola región para automatiz ar la creación de controles relacionados con IAM.	

Implemente la integración

Tarea	Descripción	Habilidades requeridas
Implemente la integración.	En un terminal con línea de comandos, escriba el siguiente comando: <pre>./deploy.sh prod</pre>	Administrador de sistemas de AWS
Cargar credenciales de Jira en AWS Secrets Manager.	1. Abra la consola de Secrets Manager en https://console.aws.amazon.com/secretsmanager/. 2. En Secretos, elija Almacenar un secreto nuevo.	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	3. En Secret type (Tipo de secreto), elija Other type of secret (Otro tipo de secreto). 4. Si usa Jira Enterprise, en los pares clave/valor, haga lo siguiente: • En la primera fila, introduzca `auth` en el cuadro de claves y, a continuación, introduzca `token_auth` en el cuadro de valores. • Añada una segunda fila, introduzca `token` en el cuadro de claves y, a continuación, introduzca su token de acceso personal en el cuadro de valores. Si usa la nube Jira Cloud, para los Pares de claves/valores, haga lo siguiente: • En la primera fila, introduzca `auth` en el cuadro de claves y, a continuación, introduzca `basic_auth` en el cuadro de valores. • Añada una segunda fila, introduzca `token` en el cuadro de claves y, a continuación, introduzc	

Tarea	Descripción	Habilidades requeridas
	a su token de API en el cuadro de valores. • Añada una tercera fila, introduzca `email` en el cuadro de claves y, a continuación, escriba su dirección de correo electrónico en el cuadro de valores. 5. Seleccione Siguiente. 6. En Nombre del secreto, ingrese `Jira-Token` y, a continuación, en la parte inferior de la página, elija Siguiente. 7. En la página Rotación del secreto, mantenga Cómo desactivar la rotación automática y, a continuac ión, en la parte inferior de la página, elija Siguiente. 8. En la página Revisar, revise los detalles del secreto y, luego, elija Almacenar.	

Tarea	Descripción	Habilidades requeridas
Cree la acción personalizada Security Hub.	1. Para cada región de AWS, en la interfaz de línea de comandos de AWS (AWS CLI), utilice create-action-targetel comando para crear una acción `CreateJiraIssue` personalizada de Security Hub denominada. `aws securityhub create-action-target --name "CreateJiraIssue" --description "Create ticket in JIRA" --id "CreateJiraIssue" --region $<aws-region>` 2. Abra la consola de Security Hub en https://console.aws.amazon.com/securityhub/. 3. En el panel de navegación de Security Hub, elija Resultados. 4. En la lista de resultados, seleccione aquellos que desee escalar. 5. En el menú Acciones, elija `CreateJiraIssue` .	Administrador de sistemas de AWS

Recursos relacionados

- Conector de administración de servicios de AWS para Jira Service Management
- Estándar de prácticas recomendadas de AWS Foundational Security

Información adicional

Ejemplo de un ticket de Jira

Cuando se produce un resultado específico de Security Hub, esta solución crea automáticamente un ticket de Jira. El ticket contiene la información siguiente:

- Título: el título identifica el problema de seguridad en el siguiente formato:

```
AWS Security Issue :: <AWS account ID> :: <Security Hub finding title>
```

- Descripción: la sección de descripción del ticket indica el control de seguridad asociado al resultado, incluye un enlace al resultado en la consola de Security Hub y proporciona una breve descripción de cómo gestionar el problema de seguridad en el flujo de trabajo de Jira.

El siguiente es un ejemplo de ticket de Jira generado de manera automática.

Title (Título)	Problema de seguridad de AWS :: 012345678912 :: Lambda.1 Lambda function policies should prohibit public access.
Descripción	¿Cuál es el problema? Hemos detectado un resultado de seguridad en la cuenta de AWS 012345678912 de la que es responsable. Este control comprueba si la política de funciones de AWS Lambda adjuntada al recurso Lambda prohíbe el acceso público. Si la política de función de Lambda permite el acceso público, se produce un error en el control. <Enlace a resultado de Security Hub>

¿Qué debo hacer con el ticket?

- Acceda a la cuenta y verifique la configura ción. Confirme que está trabajando en el ticket moviéndolo a “Asignado para soluciona r”. Una vez solucionado, páselo a solución de prueba para que el equipo de seguridad valide la resolución el problema.
- Si cree que se debe aceptar el riesgo, muévalo a “Esperando aceptación del riesgo”. Esto requerirá la revisión de un ingeniero de seguridad.
- Si cree que es un falso positivo, cámbielo a “Marcar como falso positivo”. Un ingeniero de seguridad lo revisará y lo cerrará o reabrirá en consecuencia.

Cree un proceso para imágenes de contenedores reforzadas con Generador de imágenes de EC2 y Terraform

Creado por Mike Saintcross (AWS) y Andrew Ranes (AWS)

Repositorio de código: Terraform EC2 Image Builder Container Hardening Pipeline	Entorno: producción	Origen: Packer, Chef o Pure Ansible
Destino: Generador de imágenes EC2	Tipo R: renovar arquitectura	Carga de trabajo: código abierto
Tecnologías: seguridad , identidad, conformidad; DevOps	Servicios de AWS: Amazon EC2 Container Registry; Generador de imágenes de Amazon EC2	

Resumen

Este patrón crea un proceso de EC2 Image Builder que produce una imagen de contenedor base de Amazon Linux 2 reforzada. Terraform es una herramienta de infraestructura como código (IaC) para configurar y aprovisionar la infraestructura que se usa para crear imágenes de contenedores reforzadas. Esta receta le ayuda a implementar una imagen de contenedor de Amazon Linux 2 basada en Docker y reforzada según Red Hat Enterprise Linux (RHEL) 7 STIG versión 3 lanzamiento 7 – Medium. (Consulte STIG-Build-Linux-Medium versión 2022.2.1 en la sección Componentes de Linux STIG de la documentación del Generador de imágenes de EC2). Esta imagen se conoce como imagen dorada de contenedor.

La versión incluye dos EventBridge reglas de Amazon. Una regla inicia el proceso de imágenes de contenedor cuando el resultado de Amazon Inspector es Alto o Crítico, con el fin de sustituir las imágenes no seguras. Esta regla requiere que se habilite el escaneo mejorado de Amazon Inspector y Amazon Elastic Container Registry (Amazon ECR). La otra regla envía las notificaciones a una cola de Amazon Simple Queue Service (Amazon SQS) tras una inserción correcta de las imágenes en el repositorio de Amazon ECR, con el fin de que use siempre las últimas imágenes del contenedor.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS en la que pueda implementar la infraestructura.
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada para configurar sus credenciales de AWS para la implementación local.
- Terraform descargado y configurado según las instrucciones de la documentación de Terraform.
- Git (si aprovisiona desde una máquina local).
- Un rol en la cuenta de AWS que pueda usar para crear recursos de AWS.
- Todas las variables definidas en el archivo .tfvars. También puede definir todas las variables al aplicar la configuración de Terraform.

Limitaciones

- Esta solución crea una infraestructura de Amazon Virtual Private Cloud (Amazon VPC) que incluye una puerta de enlace NAT y una puerta de enlace de Internet para la conectividad a Internet desde su subred privada. No puede usar puntos de enlace de VPC, ya que el proceso de arranque de AWS Task Orchestrator and Executor () AWSTOE instala la versión 2 de la CLI de AWS desde Internet.

Versiones de producto

- Amazon Linux 2
- Versión 1.1 o posterior de la CLI de AWS

Arquitectura

Pila de tecnología de destino

Este patrón crea 43 recursos, incluidos:

- Dos buckets de Amazon Simple Storage Service (Amazon S3): uno para los archivos de los componentes del proceso y otro para el acceso al servidor y los registros de flujo de Amazon VPC
- Un repositorio de Amazon ECR

- Una nube privada virtual (VPC) que contiene una subred pública, una subred privada, tablas de enrutamiento, una puerta de enlace NAT y una puerta de enlace de Internet
- Proceso, receta y componentes del Generador de imágenes de EC2
- Una imagen de contenedor
- Una clave de AWS Key Management Service (AWS KMS) para el cifrado de imágenes
- Una cola de SQS
- Tres funciones: una para ejecutar la canalización de EC2 Image Builder, un perfil de instancia para EC2 Image Builder y otra para las reglas EventBridge
- Dos reglas EventBridge

Estructura del módulo Terraform

Para ver el código fuente, consulte el GitHub repositorio Terraform EC2 Image Builder Container Hardening Pipeline.

```
### components.tf
### config.tf
### dist-config.tf
### files
#   ###assumption-policy.json
### hardening-pipeline.tfvars
### image.tf
### infr-config.tf
### infra-network-config.tf
### kms-key.tf
### main.tf
### outputs.tf
### pipeline.tf
### recipes.tf
### roles.tf
### sec-groups.tf
### trigger-build.tf
### variables.tf
```

Detalles del módulo

- `components.tf` contiene un recurso de carga de Amazon S3 para cargar el contenido del directorio `/files`. También puede añadir aquí archivos YAML de componentes personalizados de forma modular.

- `/files` contiene los archivos `.yml` que definen los componentes usados en `components.tf`.
- `image.tf` contiene las definiciones del sistema operativo de la imagen base. Aquí es donde puede modificar las definiciones para crear un proceso de imagen base diferente.
- `infr-config.tf` y `dist-config.tf` contienen los recursos de la infraestructura de AWS mínima necesaria para crear y distribuir la imagen.
- `infra-network-config.tf` contiene la infraestructura de VPC mínima en la que implementar la imagen del contenedor.
- `hardening-pipeline.tfvars` contiene las variables de Terraform que se usarán en el momento de la aplicación.
- `pipeline.tf` crea y administra un proceso del Generador de imágenes EC2 en Terraform.
- `recipes.tf` es donde puede especificar diferentes combinaciones de componentes para crear recetas de contenedores.
- `roles.tf` contiene las definiciones de la política de AWS Identity and Access Management (IAM) para el perfil de instancia de Amazon Elastic Compute Cloud (Amazon EC2) y el rol de implementación del proceso.
- `trigger-build.tf`contiene EventBridge las reglas y los recursos de colas de SQS.

Arquitectura de destino

El diagrama ilustra el flujo de trabajo siguiente:

1. El Generador de imágenes EC2 crea una imagen de contenedor mediante la receta definida, que instala las actualizaciones del sistema operativo y aplica RHEL Medium STIG a la imagen base de Amazon Linux 2.
2. La imagen reforzada se publica en un registro privado de Amazon ECR y una EventBridge regla envía un mensaje a una cola de SQS cuando la imagen se ha publicado correctamente.
3. Si Amazon Inspector está configurado para un escaneo mejorado, escanea el registro de Amazon ECR.
4. Si Amazon Inspector genera un resultado de gravedad crítica o alta para la imagen, una EventBridge regla activa la canalización de EC2 Image Builder para que se ejecute de nuevo y publique una imagen recién reforzada.

Automatizar y escalar

- Este patrón describe cómo aprovisionar la infraestructura y construir el proceso en su equipo. Sin embargo, está pensado para ser utilizado a escala. En lugar de implementar los módulos de Terraform de forma local, puede usarlos en un entorno multicuenta, como un entorno de AWS Control Tower con Account Factory para Terraform. En ese caso, deberá usar un bucket de S3 con estado de backend para administrar los archivos de estado de Terraform en lugar de gestionar el estado de configuración de forma local.
- Para un uso a gran escala, implemente la solución en una cuenta central, como una cuenta de Shared Services o Common Services, desde un modelo de cuenta de Control Tower o zona de aterrizaje, y conceda permiso a las cuentas de los consumidores para acceder al repositorio de Amazon ECR y a la clave de AWS KMS. Para obtener más información sobre la configuración, consulte el artículo de Re:post ¿Cómo puedo permitir que una cuenta secundaria inserte o extraiga imágenes de mi repositorio de imágenes de Amazon ECR? Por ejemplo, en una máquina expendedora de cuentas o en Account Factory para Terraform, añada permisos a cada línea base de cuenta o línea base de personalización de cuenta para proporcionar acceso a ese repositorio de Amazon ECR y a la clave de cifrado.
- Una vez implementado el proceso de imágenes del contenedor, puede modificarlo mediante las características del Generador de imágenes EC2, como los componentes, que le ayudan a empaquetar más componentes en la compilación de Docker.
- La clave de AWS KMS que se usa para cifrar la imagen del contenedor debe compartirse entre las cuentas en las que se va a usar la imagen.
- Puede añadir compatibilidad con otras imágenes duplicando todo el módulo Terraform y modificando los siguientes atributos `recipes.tf`:
  - Modifique `parent_image = "amazonlinux:latest"` a otro tipo de imagen.
  - Modifique `repository_name` para que apunte a un repositorio de Amazon ECR existente. Esto crea otro proceso que implementa un tipo de imagen principal diferente en su repositorio de Amazon ECR existente.

Herramientas

Herramientas

- Terraform (aprovisionamiento de iAC)
- Git (si se aprovisiona localmente)
- CLI de AWS versión 1 o versión 2 (si se aprovisiona localmente)

Código

El código de este patrón se encuentra en el GitHub repositorio Terraform EC2 Image Builder Container Hardening Pipeline. Para usar el código de muestra, realice los pasos de la siguiente sección.

Epics

Aprovisione la infraestructura

Tarea	Descripción	Habilidades requeridas
Configure las credenciales locales.	Configure sus credenciales temporales de AWS. 1. Compruebe si la CLI de AWS está instalada: `$ aws --version aws-cli/1.16.249 Python/3.6.8...` • La versión de la CLI de AWS debe ser 1.1 o posterior. • Si no encuentra el comando, instale la CLI de AWS. 2. Ejecute `aws configure` y proporcione los siguientes valores: `$ aws configure AWS Access Key ID [**********xxxx]: <Your AWS access key ID> AWS Secret Access Key [**********xxx`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	x]: <Your AWS secret access key> Default region name: [us-east-1]: <Your desired Region for deployment> Default output format [None]: <Your desired output format>	

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	1. Clonar el repositorio proporcionado con este patrón: Puede usar HTTPS o Secure Shell (SSH). HTTPS: `git clone https://github.com/aws-samples/terraform-ec2-image-builder-container-hardening-pipeline` SSH: `git clone git@github.com:aws-samples/terraform-ec2-image-builder-container-hardening-pipeline.git` 2. Navegue hasta el directorio local que contiene esta solución: `cd terraform-ec2-image-builder-container-hardening-pipeline`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Actualice variables.	Actualice las variables del archivo `hardening-pipeline.tfvars` para adecuarlas a su entorno y configuración. Debe proporcionar su `account_id`. También debe modificar el resto de las variables para adaptarlas a la implementación deseada. Todas las variables son obligatorias. `account_id = "<DEPLOYMENT-ACCOUNT-ID>"` `aws_region = "us-east-1"` `vpc_name = "example-hardening-pipeline-vpc"` `kms_key_alias = "image-builder-container-key"` `ec2_iam_role_name = "example-hardening-instance-role"` `hardening_pipeline_role_name = "example-hardening-pipeline-role"` `aws_s3_ami_resources_bucket = "example-hardening-ami-resources-bucket-0123"` `image_name = "example-hardening-al2-container-image"`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	<pre>ecr_name = "example-hardening-container-repo" recipe_version = "1.0.0" ebs_root_vol_size = 10</pre> Aquí tiene una descripción de cada variable: • `account_id` – El número de cuenta de AWS en el que desea implementar la solución. • `aws_region` : la Región de AWS en la que desea implementar la solución. • `vpc_name` – El nombre de su infraestructura de VPC. • `kms_key_alias` – El nombre de la clave de AWS KMS que usará la configuración de la infraestructura del Generador de imágenes EC2. • `ec2_iam_role_name` – El nombre del rol que se usará como perfil de instancia de EC2. • `hardening_pipeline_role_name` – El nombre del rol que se usará para implementar el proceso de refuerzo.	

Tarea	Descripción	Habilidades requeridas
	• `aws_s3_ami_resources_bucket` – El nombre del bucket de S3 que alojará todos los archivos necesarios para crear las imágenes del proceso y el contenedor. • `image_name` – El nombre de la imagen del contenedor. Este valor debe tener entre 3 y 50 caracteres, y solo puede contener caracteres alfanuméricos y guiones. • `ecr_name` – El nombre del registro de Amazon ECR en el que se almacenan las imágenes del contenedor. • `recipe_version` : la versión de la receta de la imagen. El valor predeterminado es 1.0.0. • `ebs_root_vol_size` – El tamaño (en gigabytes) del volumen raíz de Amazon Elastic Block Store (Amazon EBS). El valor predeterminado es 10 gigabytes.	

Tarea	Descripción	Habilidades requeridas
Inicialice Terraform.	Tras actualizar los valores de las variables, puede inicializar el directorio de configuración de Terraform. Al inicializar el directorio de configuración, se descarga e instala el proveedor de AWS definido en la configuración. `terraform init` Aparecerá un mensaje indicando que Terraform se ha inicializado correctamente e identificando la versión del proveedor instalada.	AWS DevOps
Implemente la infraestructura y cree una imagen de contenedor.	Use el siguiente comando para inicializar, validar y aplicar los módulos de Terraform al entorno mediante las variables definidas en su archivo `.tfvars`: `terraform init && terraform validate && terraform apply -var-file *.tfvars -auto-approve`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Personalice el contenedor.	Puede crear una nueva versión de una receta de contenedor cuando el Generador de imágenes de EC2 haya implementado el proceso y la receta inicial. Puede añadir cualquiera de los más de 31 componentes disponibles en el Generador de imágenes EC2 para personalizar la compilación del contenedor. Para obtener más información, consulte la sección Componentes de Crear una nueva versión de una receta de contenedor en la documentación del Generador de imágenes EC2.	Administrador de AWS

Valide los recursos

Tarea	Descripción	Habilidades requeridas
Valide el aprovisionamiento de la infraestructura de AWS.	Una vez que haya completado correctamente su primer comando `apply` de Terraform, si está aprovisionando localmente, debería ver este fragmento en la terminal de su máquina local:	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`Apply complete! Resources: 43 added, 0 changed, 0 destroyed.`	
Valide los recursos individua les de la infraestructura de AWS.	Para validar los recursos individuales implementados, si aprovisiona de forma local, puede ejecutar el siguiente comando: `terraform state list` Este comando devuelve una lista de 43 recursos.	AWS DevOps

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Elimine la imagen de la infraestructura y el contenedo r.	Cuando haya terminado de trabajar con la configuración de Terraform, puede ejecutar el siguiente comando para eliminar los recursos: `terraform init && terraform validate && terraform destroy -var-file *.tfvars -auto-approve`	AWS DevOps

Solución de problemas

Problema	Solución
Error al validar las credenciales del proveedor	Al ejecutar los comandos `apply` o `destroy` de Terraform desde su equipo local, es posible que se produzca un error similar al siguiente: `Error: configuring Terraform AWS Provider: error validating provider credentials: error calling sts:GetCallerIdentity: operation error STS: GetCallerIdentity, https response error StatusCode: 403, RequestID: 123456a9-fbc1-40ed-b8d8-513d0133ba7f, api error InvalidClientTokenId: The security token included in the request is invalid.` Este error se debe a la caducidad del token de seguridad de las credenciales usadas en la configuración de la máquina local. Para resolver el error, consulte Cómo establecer y ver ajustes de configuración en la documentación de la CLI de AWS.

Recursos relacionados

- Tubería de endurecimiento de contenedores Terraform EC2 Image Builder (repositorio) GitHub
- Documentación de Generador de imágenes EC2
- Fábrica de cuentas de AWS Control Tower para Terraform (publicación del blog de AWS)
- Bucket de S3 de estado de backend (documentación de Terraform)
- Instalación o actualización de la versión más reciente de la CLI de AWS (documentación de la CLI de AWS)
- Descargar Terraform

Centralice la administración de claves de acceso de IAM en AWS Organizations mediante Terraform

Creado por Aarti Rajput (AWS), Chintamani Aphale (AWS), T.V.R.L.Phani Kumar Dadi (AWS), Pradip kumar Pandey (AWS), Mayuri Shinde (AWS) y Pratap Kumar Nanda (AWS)

Entorno: producción	Tecnologías: Seguridad, identidad, conformidad; Infraestructura	Servicios de AWS: Amazon EventBridge; AWS Lambda; AWS Organizations; AWS Secrets Manager; Amazon SES

Resumen

Hacer cumplir las normas de seguridad para las claves y contraseñas es una tarea esencial para todas las organizaciones. Una regla importante es rotar las claves de AWS Identity and Access Management (IAM) a intervalos regulares para reforzar la seguridad. Por lo general, las claves de acceso de AWS se crean y configuran localmente cuando los equipos desean acceder a AWS desde la interfaz de línea de comandos de AWS (AWS CLI) o desde aplicaciones ajenas a AWS. Para mantener una seguridad sólida en toda la organización, las claves de seguridad antiguas deben cambiarse o eliminarse una vez que se haya cumplido el requisito o a intervalos regulares. El proceso de gestionar la rotación de claves en varias cuentas de una organización lleva mucho tiempo y es tedioso. Este patrón le ayuda a automatizar el proceso de rotación mediante el uso de Account Factory for Terraform (AFT) y los servicios de AWS.

El patrón ofrece las siguientes ventajas:

- Administra los identificadores de las claves de acceso y las claves de acceso secretas de todas las cuentas de la organización desde una ubicación central.
- Rota automáticamente las variables `AWS_ACCESS_KEY_ID` y de `AWS_SECRET_ACCESS_KEY` entorno.
- Exige la renovación si las credenciales de los usuarios se ven comprometidas.

El patrón usa Terraform para implementar funciones de AWS Lambda, reglas de EventBridge Amazon y roles de IAM. Una EventBridge regla se ejecuta a intervalos regulares y llama a una

función Lambda que enumera todas las claves de acceso de los usuarios en función del momento en que se crearon. Las funciones Lambda adicionales crean un nuevo identificador de clave de acceso y una clave de acceso secreta si la clave anterior es anterior al período de rotación que haya definido (por ejemplo, 45 días) y lo notifican a un administrador de seguridad mediante Amazon Simple Notification Service (Amazon SNS) y Amazon Simple Email Service (Amazon SES). Los secretos se crean en AWS Secrets Manager para ese usuario, la clave de acceso secreta anterior se almacena en Secrets Manager y se configuran los permisos para acceder a la clave anterior. Para garantizar que la clave de acceso anterior ya no se utilice, se deshabilita después de un período de inactividad (por ejemplo, 60 días, que serían 15 días después de rotar las claves en nuestro ejemplo). Tras un período de almacenamiento inactivo (por ejemplo, 90 días o 45 días después de rotar las claves en nuestro ejemplo), las claves de acceso antiguas se eliminan de AWS Secrets Manager. Para obtener información detallada sobre la arquitectura y el flujo de trabajo, consulte la sección Arquitectura.

Requisitos previos y limitaciones

- Una landing zone para su organización creada con AWS Control Tower (versión 3.1 o posterior)
- Account Factory for Terraform (AFT) configurada con tres cuentas:
  - La cuenta de administración de la organización administra toda la organización desde una ubicación central.
  - La cuenta de administración AFT aloja la canalización de Terraform e implementa la infraestructura en la cuenta de implementación.
  - La cuenta de implementación implementa esta solución completa y administra las claves de IAM desde una ubicación central.
- Terraform, versión 0.15.0 o posterior, para aprovisionar la infraestructura en la cuenta de despliegue.
- Una dirección de correo electrónico configurada en Amazon Simple Email Service (Amazon SES).
- (Recomendado) Para mejorar la seguridad, implemente esta solución dentro de una subred privada (cuenta de implementación) dentro de una nube privada virtual (VPC). Puede proporcionar los detalles de la VPC y la subred al personalizar las variables (consulte Personalizar los parámetros de la canalización de código en la sección Epics).

Arquitectura

Repositorios AFT

Este patrón utiliza Account Factory for Terraform (AFT) para crear todos los recursos de AWS necesarios y la canalización de código para implementar los recursos en una cuenta de implementación. La canalización de código se ejecuta en dos repositorios:

- La personalización global contiene el código de Terraform que se aplicará a todas las cuentas registradas en AFT.
- Las personalizaciones de la cuenta contienen el código de Terraform que se ejecutará en la cuenta de implementación.

Detalles del recurso

Los CodePipeline trabajos de AWS crean los siguientes recursos en la cuenta de implementación:

- EventBridge Regla de AWS y regla configurada
- `account-inventory`Función Lambda
- `IAM-access-key-rotation`Función Lambda
- `Notification`Función Lambda
- Depósito de Amazon Simple Storage Service (Amazon S3) que contiene una plantilla de correo electrónico
- Política de IAM obligatoria

Arquitectura

En el siguiente diagrama se ilustra lo siguiente:

1. Una EventBridge regla llama a la función `account-inventory` Lambda cada 24 horas.
2. La función `account-inventory` Lambda consulta a AWS Organizations una lista de todos los identificadores, nombres de cuentas y correos electrónicos de cuentas de AWS.
3. La función `account-inventory` Lambda inicia una `IAM-access-key-auto-rotation` función Lambda para cada cuenta de AWS y le pasa los metadatos para su procesamiento adicional.
4. La función `IAM-access-key-auto-rotation` Lambda utiliza un rol de IAM asumido para acceder a la cuenta de AWS. El script de Lambda ejecuta una auditoría de todos los usuarios y sus claves de acceso de IAM en la cuenta.

5. El umbral de rotación de la clave de IAM (período de rotación) se configura como una variable de entorno cuando se implementa la función `IAM-access-key-auto-rotation` Lambda. Si se modifica el período de rotación, la función `IAM-access-key-auto-rotation` Lambda se vuelve a implementar con una variable de entorno actualizada. Puede configurar los parámetros para establecer el período de rotación, el período de inactividad de las claves antiguas y el búfer inactivo tras el cual se eliminarán las claves antiguas (consulte Personalización de los parámetros de la cadena de códigos en la sección Epics).
6. La función `IAM-access-key-auto-rotation` Lambda valida la antigüedad de la clave de acceso en función de su configuración. Si la antigüedad de la clave de acceso de IAM no ha superado el período de rotación que ha definido, la función Lambda no realiza ninguna otra acción.
7. Si la antigüedad de la clave de acceso de IAM ha superado el período de rotación que ha definido, la función `IAM-access-key-auto-rotation` Lambda crea una clave nueva y rota la clave existente.
8. La función Lambda guarda la clave anterior en Secrets Manager y limita los permisos al usuario cuyas claves de acceso no cumplan con los estándares de seguridad. La función Lambda también crea una política basada en recursos que permite que solo el principal de IAM especificado acceda al secreto y lo recupere.
9. La función `IAM-access-key-rotation` Lambda llama a la función Lambda`Notification`.
10. La función `Notification` Lambda consulta el bucket de S3 en busca de una plantilla de correo electrónico y genera dinámicamente mensajes de correo electrónico con los metadatos de actividad relevantes.
11. La función `Notification` Lambda solicita a Amazon SES que tome medidas adicionales.
12. Amazon SES envía un correo electrónico a la dirección de correo electrónico del propietario de la cuenta con la información pertinente.

Herramientas

Servicios de AWS

- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos. Este patrón requiere funciones y permisos de IAM.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la

capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.

- AWS Secrets Manager le permite reemplazar las credenciales codificadas en el código, incluidas las contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación.
- Amazon Simple Email Service (Amazon SES) facilita poder enviar y recibir correos electrónicos a través de los dominios y direcciones de correo electrónico propios.

Otras herramientas

- Terraform es una herramienta de infraestructura como código (IaC) HashiCorp que le ayuda a crear y administrar recursos locales y en la nube.

Repositorio de código

Las instrucciones y el código de este patrón están disponibles en el repositorio de rotación de claves de acceso de GitHub IAM. Puede implementar el código en la cuenta de implementación central de la Torre de Control Tower de AWS para gestionar la rotación de claves desde una ubicación central.

Prácticas recomendadas

- Para IAM, consulte las prácticas recomendadas de seguridad en la documentación de IAM.
- Para obtener información sobre la rotación de claves, consulte las directrices para actualizar las claves de acceso en la documentación de IAM.

Epics

Configure los archivos fuente

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	1. Clone el GitHub repositorio de rotación de claves de acceso de IAM: `$ git clone https://github.com/aws-samp`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`les/centralized-ia m-key-management-a ws-organizations-t erraform.git` 2. Confirme que su copia local del repositorio contiene tres carpetas: `$ cd Iam-Access-keys-Rotation` `$ ls` `org-account-cus tomization` `global-account-c ustomization` `account-custom ization`	

Configurar cuentas

Tarea	Descripción	Habilidades requeridas
Configure la cuenta de arranque.	Como parte del proceso de arranque de AFT, debe tener una carpeta llamada en su máquina local. `aft-boots trap` 1. Copie todos los archivos de Terraform manualmente de su GitHub org-account-customizationcarpeta local a su carpeta. `aft-boots trap`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	2. Ejecute los comandos de Terraform para configurar el rol multicuenta global en la cuenta de administración de AWS Control Tower: `$ cd aft-bootstrap` `$ terraform init` `$ terraform apply –auto-approve`	
Configure las personalizaciones globales.	Como parte de la configuración de la carpeta AFT, debe tener una carpeta llamada `aft-global-customizations` en su máquina local. 1. Copie manualmente todos los archivos de Terraform de su GitHub global-account-customizationcarpeta local a su `aft-global-customizations/terraform` carpeta. 2. Envía el código a AWS CodeCommit: `$ git add *` `$ git commit -m "message"` `$ git push`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Configure las personalizaciones de la cuenta.	Como parte de la configuración de la carpeta AFT, tiene una carpeta llamada `aft-account-customizations` en su máquina local. 1. Crea una carpeta con tu número de cuenta vendida. 2. Copia manualmente todos los archivos de Terraform de la carpeta de GitHub personalización de tu cuenta local a tu carpeta. `aft-account-customizations/<vended account>/terraform` 3. Envía el código a AWS CodeCommit: `$ git add *` `$ git commit -m "message"` `$ git push`	DevOps ingeniero

Personalice los parámetros de la canalización de códigos

Tarea	Descripción	Habilidades requeridas
Personalice los parámetros de la canalización de códigos que no sean de Terraform para todas las cuentas.	Cree un archivo llamado `input.auto.tfvars` en la `aft-global-customizations/terraform/` carpeta y proporcione los	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	datos de entrada necesarios. Consulte el archivo en el GitHub repositorio para ver los valores predeterminados.	

Tarea	Descripción	Habilidades requeridas
Personalice los parámetros de la canalización de códigos para la cuenta de despliegue.	Cree un archivo llamado `input.auto.tfvars` en la `aft-account-customizations/<AccountName>/terraform/` carpeta y envíe el código a AWS CodeCommit. Al enviar código a AWS, CodeCommit se inicia automáticamente la canalización del código. Especifique los valores de los parámetros en función de los requisitos de su organización, incluidos los siguientes (consulte el archivo del repositorio de Github para ver los valores predeterminados): • `s3_bucket_name` — Un nombre de bucket exclusivo para la plantilla de correo electrónico. • `s3_bucket_prefix` — Un nombre de carpeta dentro del depósito de S3. • `admin_email_address` — La dirección de correo electrónico del administrador que debe recibir la notificación. • `org_list_account` — El número de cuenta de la cuenta de administración.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	• `rotation_period` — El número de días después de los cuales una clave debe pasar de activa a inactiva. • `inactive_period` — El número de días después de los cuales se deben desactivar las llaves giradas. Este valor debe ser mayor que el valor de. `rotation_period` • `inactive_buffer` — El período de gracia entre la rotación y la desactivación de una clave. • `recovery_grace_period` — El período de gracia entre la desactivación y la eliminación de una clave. • `dry_run_flag` — Configúrelo en True si desea enviar una notificación al administrador con fines de prueba, sin rotar las claves. • `store_secrets_in_central_account` — Configúrelo en verdadero si desea almacenar el secreto en la cuenta de despliegue. Si la variable se establece en false (predeterminado), el secreto se almacenará en la cuenta del miembro.	

Tarea	Descripción	Habilidades requeridas
	• `credential_replication_region` — La región de AWS en la que desea implementar la función Lambda y los buckets S3 para la plantilla de correo electrónico. • `run_lambda_in_vpc` — Configúrelo en true para ejecutar la función Lambda dentro de la VPC. • `vpc_id`— El ID de VPC de la cuenta de despliegue, si quiere ejecutar la función Lambda dentro de la VPC. • `vpc_cidr`— El rango de CIDR de la cuenta de despliegue. • `subnet_id` — Los ID de subred de la cuenta de despliegue. • `create_smtp_endpoint` — Configúrelo en true si desea habilitar el punto final de correo electrónico.	

Validar la rotación de claves

Tarea	Descripción	Habilidades requeridas
Valide la solución.	1. Desde la consola de administración de AWS,	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	inicie sesión en la cuenta de implementación. 2. Abra la consola de IAM y compruebe si las credencia les de usuario (ID de clave de acceso y claves secretas) se rotan según lo especificado. 3. Tras rotar una clave de IAM, confirme lo siguiente: • El valor anterior se almacena en AWS Secrets Manager. • El nombre secreto está en el formato`Account_<account ID>_User_<username>_AccessKey` . • El usuario que especific ó en el `admin_ema il_address` parámetro recibe una notificación por correo electrónico sobre la rotación de claves.	

Amplíe la solución

Tarea	Descripción	Habilidades requeridas
Personalice la fecha de notificación por correo electrónico.	Si desea enviar notificaciones por correo electrónico un día específico antes de deshabili	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	tar la clave de acceso, puede actualizar la función `IAM-access-key-auto-rotation` Lambda con esos cambios: 1. Defina una variable llamada`notify-period` . 2. Añada una `if` condición `main.py` antes de desactivar la clave: `If (keyage>rotation-period-notify-period){ send_to_notifier(context, aws_account_id, account_name, resource_owner, resource_actions[resource_owner], dryrun, config.emailTemplateAudit) }`	

Solución de problemas

Problema	Solución
El trabajo de `account-inventory` Lambda falla `AccessDenied` al enumerar las cuentas.	Si se produce este problema, debe validar los permisos: 1. Inicia sesión en la cuenta recién vendida, abre la CloudWatch consola de Amazon y, a continuación, consulta el grupo `/aws/lamb`

Problema	Solución
	da/account-inventory-lambda de CloudWatch registros. 2. En los CloudWatch registros más recientes , identifica el número de cuenta que está causando el problema de acceso denegado. 3. Inicie sesión en la cuenta de administración de AWS Control Tower y confirme que allow-list-account se creó el rol. 4. Si el rol no existe, vuelva a ejecutar el código de Terraform mediante el terraform apply comando. 5. Seleccione la pestaña Cuenta de confianza y compruebe que la misma cuenta es de confianza.

Recursos relacionados

- Prácticas recomendadas de Terraform (documentación de Terraform)
- Prácticas recomendadas de seguridad en IAM (documentación de IAM)
- Mejores prácticas para la rotación de claves (documentación de IAM)

Registro centralizado y barrera de protección para varias cuentas

Creado por Ankush Verma (AWS) y Tracy (Pierce) Hickey (AWS)

Entorno: producción	Tecnologías: seguridad, identidad, cumplimiento; administración y gobierno	Servicios de AWS: AWS CloudFormation; AWS Config; Amazon CloudWatch; AWS CodePipeline GuardDuty; Amazon Lambda; Amazon Macie; AWS Security Hub; Amazon S3

Resumen

El enfoque que se incluye en este patrón es adecuado para los clientes que tienen varias cuentas de Amazon Web Services (AWS) en AWS Organizations y que ahora se enfrentan a dificultades a la hora de utilizar los servicios de AWS Control Tower, una zona de aterrizaje o máquinas expendedoras de cuentas para configurar barrera de protección básicas en sus cuentas.

Este patrón demuestra el uso de una arquitectura optimizada de varias cuentas para configurar el registro centralizado y los controles de seguridad estandarizados de una manera bien estructurada. Con la ayuda de CloudFormation plantillas de AWS CodePipeline, AWS y scripts de automatización, esta configuración se implementa en todas las cuentas que pertenecen a una organización.

La arquitectura de cuentas múltiples incluye las siguientes cuentas:

- Cuenta de registro centralizada: la cuenta en la que se almacenan todos los registros de flujos de la nube privada virtual (VPC), CloudTrail los registros de AWS, el registro de AWS Config y todos los CloudWatch registros de Amazon Logs (mediante suscripciones) de todas las demás cuentas.
- Cuenta de seguridad principal: la cuenta que servirá como cuenta principal para los siguientes servicios de seguridad que se administran en varias cuentas.
  - Amazon GuardDuty
  - AWS Security Hub
  - Amazon Macie
  - Amazon Detective

- Cuentas secundarias: las demás cuentas de la organización. Estas cuentas almacenan todos los registros útiles en la cuenta de registro centralizada. Las cuentas secundarias se unen a la cuenta de seguridad principal como miembros de los servicios de seguridad.

Tras lanzar la CloudFormation plantilla (adjunta), aprovisiona tres depósitos de Amazon Simple Storage Service (Amazon S3) en la cuenta de registro centralizada. Se utiliza un depósito para almacenar todos los registros relacionados con AWS (como los registros de VPC Flow Logs y AWS Config) de todas las cuentas. CloudTrail El segundo depósito sirve para almacenar las CloudFormation plantillas de todas las cuentas. El tercer bucket de Amazon S3 donde se almacenan los registros de acceso.

Una CloudFormation plantilla independiente crea la canalización que usa AWS CodeCommit. Una vez que el código actualizado se envía al CodeCommit repositorio, se encarga de lanzar los recursos y configurar los servicios de seguridad en todas las cuentas. Para obtener más información sobre la estructura de los archivos que se subirán al CodeCommit repositorio, consulta el archivo README.md (adjunto).

Requisitos previos y limitaciones

Requisitos previos

- Un ID de organización de AWS Organizations, con todas las cuentas unidas a la misma organización.
- Una dirección de correo electrónico activa para recibir notificaciones de Amazon Simple Notification Service (Amazon SNS).
- Cuotas confirmadas para los buckets de Amazon Simple Storage Service (Amazon S3) en cada una de sus cuentas. De forma predeterminada, cada cuenta tiene 100 buckets de S3. Si necesita buckets adicionales, solicite un aumento de cuota antes de implementar esta solución.

Limitaciones

Todas las cuentas deben formar parte de la misma organización. Si no utiliza AWS Organizations, debe modificar determinadas políticas, como la política de bucket de S3, para permitir el acceso desde los roles de AWS Identity and Access Management (IAM) de cada cuenta.

Nota: Mientras se implementa la solución, debe confirmar la suscripción a Amazon SNS. El mensaje de confirmación se envía a la dirección de correo electrónico que proporcionó durante el proceso de

implementación. De este modo, se enviarán algunos mensajes de alerta por correo electrónico a esta dirección de correo electrónico, ya que estas alarmas se activan cada vez que se crean o modifican políticas de roles de IAM en la cuenta. Durante el proceso de implementación, puede ignorar estos mensajes de alerta.

Arquitectura

Pila de tecnología de destino

- CloudWatch Alarmas y registros de Amazon
- CodeCommit Repositorio de AWS
- AWS CodePipeline
- AWS Config
- Amazon Detective
- Amazon GuardDuty
- Roles y permisos de IAM
- Amazon Macie
- Buckets de S3
- AWS Security Hub
- Amazon SNS

Arquitectura de destino

1. Otras cuentas registradas como cuentas secundarias de la cuenta de seguridad principal de los servicios de seguridad
2. Resultados de seguridad de todas las cuentas secundarias, incluida la cuenta principal

Recursos

Los siguientes recursos se aprovisionan automáticamente cuando el código actualizado se envía al CodeCommit repositorio de cada cuenta y región de AWS.

CloudFormation pila 1: registro de la pila principal

- Pila anidada 1: roles y políticas estándar de IAM

- Pila anidada 2: configuración de AWS Config en la cuenta

- Pila anidada 3: alarmas CloudWatch

    - SecurityGroupChangesAlarm

    - UnauthorizedAttemptAlarm

    - RootActivityAlarm

    - NetworkAclChangesAlarm

    - YO SOY UserManagementAlarm

    - LO SOY PolicyChangesAlarm

    - CloudTrailChangeAlarm

    - LO SOY CreateAccessKeyAlarm

  - Filtros métricos para crear métricas a partir de CloudTrail registros y usarlas para alarmas

  - Tema de SNS

CloudFormation pila 2: pila de barandillas principal

- Pila anidada 1: función de Lambda de AWS para configurar la política de contraseñas de la cuenta

- Pila anidada 2: reglas básicas de AWS Config

  - CIS- SecurityGroupsMustRestrictSshTraffic

  - OpenSecurityGroupRuleCheck junto con la función Lambda para la evaluación de reglas de grupos de seguridad

  - check-ec2- for-required-tag

  - check-for-unrestricted-ports

CloudFormation pila 3 — CloudWatch exportación de registros

- Exportación de CloudWatch registros de grupos de registros a Amazon S3 mediante una suscripción a Amazon Kinesis

Herramientas

- AWS CloudFormation: AWS CloudFormation utiliza plantillas para modelar y aprovisionar, de forma automatizada y segura, todos los recursos necesarios para sus aplicaciones en todas las regiones y cuentas de AWS.
- Amazon CloudWatch: Amazon CloudWatch monitorea los recursos de AWS y las aplicaciones que ejecuta en AWS en tiempo real. Puede utilizarlas CloudWatch para recopilar y realizar un seguimiento de las métricas, que son variables que puede medir para sus recursos y aplicaciones.
- AWS CodeCommit: AWS CodeCommit es un servicio de control de versiones hospedado por AWS. Puede utilizarlo CodeCommit para almacenar y gestionar de forma privada activos (como documentos, código fuente y archivos binarios) en la nube.
- AWS CodePipeline: AWS CodePipeline es un servicio de entrega continua que puede utilizar para modelar, visualizar y automatizar los pasos necesarios para lanzar su software.
- AWS Config: AWS Config brinda una visión detallada de la configuración de los recursos de AWS de su cuenta de AWS. Esto incluye cómo se relacionan los recursos entre sí y cómo se han configurado en el pasado, para que pueda ver cómo las configuraciones y las relaciones cambian a lo largo del tiempo.
- Amazon Detective lo ayuda a analizar, investigar e identificar rápidamente la causa raíz de resultados de seguridad o actividades sospechosas. Detective recopila automáticamente los datos de registro de sus recursos de AWS. A continuación, utiliza el machine learning, el análisis estadístico y la teoría de grafos para generar visualizaciones que lo ayuden a realizar investigaciones sobre la seguridad con mayor rapidez y de forma más eficaz.
- Amazon GuardDuty: Amazon GuardDuty es un servicio de monitoreo de seguridad continuo que analiza y procesa los registros de flujo, los registros de eventos de CloudTrail administración, CloudTrail los registros de eventos de datos y los registros del Sistema de nombres de dominio (DNS). Utiliza fuentes de información de amenazas, como listas de direcciones IP y dominios maliciosos, y aprendizaje automático para identificar la actividad inesperada y potencialmente no permitida, así como la actividad malintencionada en su entorno de AWS.
- AWS Identity and Access Management (IAM) es un servicio web que ayuda a controlar de forma segura el acceso a los recursos de AWS. Utilice IAM para controlar quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos.

- Amazon Macie automatiza la detección de información confidencial, como información de identificación personal (PII) y datos financieros, para proporcionarle una mejor comprensión de los datos que almacena su organización en Amazon S3.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos altamente escalable que se puede utilizar para una amplia gama de soluciones de almacenamiento, incluidos sitios web, aplicaciones móviles, copias de seguridad y lagos de datos.
- AWS Security Hub proporciona una visión completa de su estado de seguridad en AWS y lo ayuda a comprobar su entorno con los estándares y las prácticas recomendadas del sector de la seguridad.
- Amazon Simple Notification Service (Amazon SNS) es un servicio administrado con el que se ofrece la entrega de mensajes de los publicadores a los suscriptores (también conocido como productores y consumidores).

Epics

Paso 1: Configurar los roles de IAM en todas las cuentas

Tarea	Descripción	Habilidades requeridas
Ejecute la plantilla ChildAccount_IAM_Role_All_Accounts.yaml para crear el rol CloudFormation de IAM en la región us-east-1.	Para crear los roles y los permisos de IAM necesarios, debe lanzar manualmente esta plantilla en cada cuenta, una por una (cuenta de registro centralizada, cuenta de seguridad principal y todas las demás cuentas de AWS de la organización) en la región us-east-1. La plantilla `Childaccount_IAM_role_All_Accounts.yaml` se encuentra en el directorio `/templates/initial_deployment_templates` del paquete. El rol de IAM se	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	utiliza al realizar llamadas a la API para el aprovisionamiento y la configuración del resto de la arquitectura. Asegúrese de que el nombre del rol de IAM que se transfiere como parámetro sea coherente en todas las cuentas.	
En los parámetros de plantilla , proporcione el nombre del rol de IAM.	Indique la función de IAM que, en la cuenta de seguridad principal, puede asumir en todas las demás cuentas secundarias. CodeBuild El nombre del rol predeterminado es `security_execute_child_stack_role` .	Arquitecto de la nube
En los parámetros, proporcione el ID de cuenta de la cuenta de seguridad principal.	La cuenta de seguridad principal es la cuenta en la que se CodeBuild ejecuta.	Arquitecto de la nube

Paso 2: configurar buckets de S3 en la cuenta de registro centralizada

Tarea	Descripción	Habilidades requeridas
En la cuenta de registro centralizada, en us-east-1, ejecute la plantilla S3Buckets-Centralized- .yaml. LoggingAccount CloudFormation	Para crear los buckets de S3 en la cuenta de registro centralizada, inicie `S3Buckets-Centralized-LoggingAccount.yaml` . La plantilla se encuentra en el directorio `/templates/initial_deployment_templa`	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	`tes` del paquete. Los buckets de S3 almacenarán todos los registros, plantillas y registros de acceso a Amazon S3. Anote todos los nombres de los buckets de S3, que utilizará para modificar los archivos de parámetros en los siguientes pasos.	
En los parámetros de plantilla, proporcione el nombre del bucket de S3 para el almacenamiento de registros de AWS.	Escriba un nombre para el parámetro `S3 Bucket Name for Centralized Logging in Logging Account`. Este depósito actúa como una ubicación centralizada para almacenar los registros de AWS, como los registros de flujo y CloudTrail los registros, de todas las cuentas. Anote el nombre del bucket y el nombre de recurso de Amazon (ARN).	Arquitecto de la nube
Escriba el nombre del bucket de S3 para los registros de acceso.	Escriba el nombre del bucket de S3 para el parámetro `S3 Bucket Name for Access Logs in Logging Account`. Este bucket de S3 almacena los registros de acceso de Amazon S3.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Escriba el nombre del bucket de S3 para el almacenamiento de las plantillas.	Escriba el nombre del bucket de S3 para el parámetro `S3 Bucket Name for CloudFormation Template storage in Logging Account`.	Arquitecto de la nube
Proporcione el ID de organización de.	Para proporcionar acceso a los depósitos de S3 dentro de la organización, introduzca el ID de la organización en el parámetro `Organization Id for Non-AMS accounts`.	Arquitecto de la nube

Paso 3: implemente la infraestructura de CI/CD en la cuenta de seguridad principal

Tarea	Descripción	Habilidades requeridas
Inicie la plantilla security-guard-rails-codepipeline -Centralized- SecurityAccount .yml. CloudFormation	Para implementar la canalización de CI/CD, inicie manualmente la plantilla `security-guard-rails-codepipeline-Centralized-SecurityAccount.yml` en la cuenta de seguridad principal de us-east-1. La plantilla se encuentra en el directorio `/templates/initial_deployment_templates` del paquete. Esta canalización implementará toda la infraestructura en	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	todas las cuentas secundari as.	
Proporcione un nombre para el bucket de S3 que almacenará las plantillas en la cuenta de registro centraliz ada.	Introduzca el nombre del bucket de S3 que proporcio nó para el parámetro `S3 Bucket Name for the CloudFormation Template storage in Logging Account` en el paso 2.	Arquitecto de la nube
Proporcione el nombre del rol de IAM que se utilizará en las cuentas secundarias.	Introduzca el nombre que proporcionó para el parámetro `Name of the IAM role` en el paso 1.	Arquitecto de la nube
Proporcione una dirección de correo electrónico activa para recibir CodePipeline las notificaciones de errores.	Introduzca la dirección de correo electrónico que desee utilizar para recibir las notificac iones de CodePipeline fallos y otras notificaciones CloudWatch relacionadas con las alarmas.	Arquitecto de la nube

Paso 4: actualizar los archivos para incluir información de cuenta

Tarea	Descripción	Habilidades requeridas
Modifique AccountList.json.	En el archivo `Accountli st.json` , que se encuentra en el nivel superior del paquete, añada el número de la cuenta de seguridad principal y los números de	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	la cuenta secundaria. Tenga en cuenta que el campo `ChildAccountList` también incluye el número de la cuenta de seguridad principal. Vea un ejemplo en el archivo `deployment-instructions.md` del paquete.	
Modificar accounts.csv	En el archivo `accounts.csv`, que se encuentra en el nivel superior del paquete, añada todas las cuentas secundarias junto con el correo electrónico registrado en las cuentas. Vea el ejemplo en el archivo `deployment-instructions.md`:	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Modifique parameters.config.	En el archivo `parameters.config` , que se encuentra en la carpeta `/templates` , actualice los seis parámetros siguientes: • `pNotifyEmail` : la dirección de correo electrónico que proporcionaste al configurar la canalización (consulta el paso 3) • `pstackNameLogging` : El nombre de la CloudFormation pila para el registro centralizado • `pS3LogsBucket` : nombre del bucket de S3 donde se almacenarán los registros de todas las cuentas (consulte el paso 2) • `pBucketName` : ARN del bucket de S3 utilizado para almacenar los registros • `pTemplateBucketName` : el nombre de los buckets de S3 en los que se almacenarán las plantillas (consulte el paso 2) • `pAllowedAccounts` : ID de cuenta para las cuentas principal y secundaria	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	Para el resto de parámetros, puede mantener los valores predeterminados. Para ver un ejemplo, consulte el archivo `deployment-instructions.md` del paquete.	

Paso 5: Accede al CodeCommit repositorio y envía los archivos actualizados

Tarea	Descripción	Habilidades requeridas
Acceda al CodeCommit repositorio que creó en el paso 3.	En la sección de resultados de la CloudFormation pila de infraestructuras de CI/CD (lanzada en el paso 3), anote el nombre de la URL del CodeCommit repositorio. Cree un acceso al repositorio para que los archivos puedan insertarse en él para que la infraestructura se despliegue en todas las cuentas de destino. Para obtener más información, consulte Configuración de AWS CodeCommit.	Arquitecto de la nube
Envía los archivos al CodeCommit repositorio.	Instale Git en su equipo local. A continuación, ejecute los comandos de Git para clonar el repositorio vacío, copie los archivos de su portátil a la carpeta del repositorio y envíe los artefactos al repositorio. Compruebe los ejemplos de	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	comandos de Git en el archivo `deployment-instructions.md` del paquete. Para ver los comandos básicos de Git, consulte la sección Recursos relacionados.	

Paso 6: Confirma CodePipeline y CodeBuild estado

Tarea	Descripción	Habilidades requeridas
Confirme el estado de CodePipeline y CodeBuild.	Tras enviar los artefactos al CodeCommit repositorio, confirme que se ha iniciado la CodePipeline canalización que creó en el paso 3. A continuación, comprueba los CodeBuild registros para confirmar el estado o los errores.	Arquitecto de la nube

Recursos relacionados

- Implementación de CloudFormation plantillas de AWS
- Configuración para AWS CodeCommit
- Carga de archivos en buckets de S3
- Comandos básicos de Git

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Comprueba la versión de registro de acceso, HTTPS y TLS en una CloudFront distribución de Amazon

Entorno: producción	Tecnologías: entrega de contenido; seguridad, identidad, conformidad	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon SNS; AWS CloudWatch; CloudFormation Amazon; AWS Lambda		

Resumen

Este patrón comprueba una CloudFront distribución de Amazon para asegurarse de que utiliza HTTPS, utiliza la versión 1.2 o posterior de Transport Layer Security (TLS) y tiene habilitado el registro de acceso. CloudFront es un servicio ofrecido por Amazon Web Services (AWS) que acelera la distribución de su contenido web estático y dinámico, como .html, .css, .js y archivos de imagen, a sus usuarios. CloudFront entrega su contenido a través de una red mundial de centros de datos denominados ubicaciones perimetrales. Cuando un usuario solicita el contenido con el que estás publicando CloudFront, la solicitud se redirige a la ubicación perimetral que ofrezca la menor latencia (retraso de tiempo), de modo que el contenido se entregue con el mejor rendimiento posible.

Este patrón proporciona una función de AWS Lambda que se inicia cuando Amazon CloudWatch Events detecta la llamada a la CloudFront API CreateDistributionCreateDistributionWithTags, o. UpdateDistribution La lógica personalizada de la función Lambda evalúa todas CloudFront las distribuciones que se crearon o actualizaron en la cuenta de AWS. Envía una notificación de infracción mediante Amazon Simple Notification Service (Amazon SNS) si detecta las siguientes infracciones:

- Comprobaciones globales:
  - El certificado personalizado no usa TLS versión 1.2
  - El registro está deshabilitado para la distribución
- Comprobaciones de origen:

  - Origin no está configurado con TLS versión 1.2
  - La comunicación con Origin está permitida en un protocolo que no sea HTTPS
- Comprobaciones de comportamiento:
  - La comunicación de comportamiento predeterminada está permitida en un protocolo que no sea HTTPS
  - La comunicación por comportamiento personalizado está permitida en un protocolo que no sea HTTPS

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- La dirección de correo electrónico en la que desee recibir notificaciones de infracción

Limitaciones

- Este control de seguridad no comprueba las distribuciones de Cloudfront existentes, a menos que se haya realizado una actualización en la distribución.
- CloudFront se considera un servicio global y no está vinculado a una región de AWS específica. Sin embargo, el registro de las API de Amazon CloudWatch Logs y AWS Cloudtrail para los servicios globales se realiza en la región EE.UU. Este (Norte de Virginia) (`us-east-1`). Por lo tanto, esta forma de control de seguridad CloudFront debe implementarse y mantenerse en `us-east-1` ella. Esta implementación única monitorea todas las distribuciones para CloudFront. No implemente el control de seguridad en ninguna otra región de AWS. (La implementación en otras regiones provocará que no se inicien CloudWatch los eventos y la función Lambda, y no habrá notificaciones de SNS).
- Esta solución se ha sometido a pruebas exhaustivas con distribuciones de contenido CloudFront web. No cubre las distribuciones de streaming del protocolo de mensajería en tiempo real (RTMP).

Arquitectura

Pila de tecnología de destino

- Función de Lambda

- Tema de SNS
- EventBridge Regla de Amazon

Arquitectura de destino

Automatizar y escalar

- Si utiliza AWS Organizations, puede utilizar AWS Cloudformation StackSets para implementar la plantilla adjunta en varias cuentas que desee supervisar.

Herramientas

Servicios de AWS

- AWS CloudFormation: CloudFormation es un servicio que le ayuda a modelar y configurar los recursos de AWS mediante el uso de la infraestructura como código.
- Amazon EventBridge: EventBridge ofrece un flujo de datos en tiempo real desde sus propias aplicaciones, aplicaciones de software como servicio (SaaS) y servicios de AWS, y dirige esos datos a objetivos como las funciones Lambda.
- AWS Lambda: Lambda admite la ejecución de código sin aprovisionar ni administrar servidores.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos altamente escalable que se puede utilizar para una amplia gama de soluciones de almacenamiento, incluidos sitios web, aplicaciones móviles, copias de seguridad y lagos de datos.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) coordina y gestiona la entrega o el envío de mensajes entre publicadores y clientes, incluyendo los servidores web y las direcciones de correo electrónico. Los suscriptores reciben todos los mensajes publicados de los temas a los que están suscritos y todos los suscriptores de un tema reciben los mismos mensajes.

Código

El código adjunto incluye:

- Un archivo .zip con el código de Lambda (index.py)
- Una CloudFormation plantilla (archivo.yml) que se ejecuta para implementar el código Lambda

Epics

Cargue el control de seguridad

Tarea	Descripción	Habilidades requeridas
Cree el bucket de S3 para el código de Lambda.	En la consola Amazon S3, cree un bucket de S3 con un nombre único que no contenga barras diagonales iniciales. Un nombre de bucket de S3 es globalmente único y todas las cuentas de AWS comparten el espacio de nombres. El bucket de S3 debe estar en la región en la que se planea implementar el código de Lambda.	Arquitecto de la nube
Cargue el código de Lambda en el bucket de S3.	Cargue el código de Lambda (archivo cloudfront_ssl_log_lambda.zip) que se proporciona en la sección Adjuntos en el bucket de S3 que creó en el paso anterior.	Arquitecto de la nube

Implemente la plantilla CloudFormation

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation plantilla.	En la CloudFormation consola de AWS, en la misma región de AWS que el bucket de S3, implemente la CloudFormation plantilla (cloudfront-ssl-lo	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	gging.yml) que se proporciona en la sección de adjuntos.	
Especifique el nombre del bucket de S3.	En el parámetro de Bucket de S3, especifique el nombre del bucket de S3 que creó en la primera épica.	Arquitecto de la nube
Especifique el nombre de clave de Amazon S3 para el archivo Lambda.	Para el parámetro Clave de S3, especifique la ubicación en Amazon S3 del archivo .zip de código de Lambda en su bucket de S3. No incluya barras diagonales iniciales (por ejemplo, puede escribir lambda.zip o controls/lambda.zip).	Arquitecto de la nube
Proporcione una dirección de correo electrónico para la notificación.	Para el parámetro Correo electrónico de notificación, proporcione una dirección de correo electrónico en la que le gustaría recibir las notificaciones de infracción.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Defina el nivel de registro.	Para el parámetro Nivel de registro de Lambda, defina el nivel de registro de la función de Lambda. Elija uno de los valores siguientes: • INFO para recibir mensajes informativos detallados sobre el progreso de la aplicación. • ERROR para obtener información sobre los eventos de error que podrían seguir permitiendo que la aplicación siguiera ejecutándose. • ADVERTENCIA para obtener información sobre situaciones potencialmente peligrosas.	Arquitecto de la nube

Confirmar la suscripción

Tarea	Descripción	Habilidades requeridas
Confirmar la suscripción.	Cuando la CloudFormation plantilla se haya implement ado correctamente, se creará un nuevo tema de SNS y se enviará un mensaje de suscripción a la dirección de correo electrónico que proporcionó. Debe confirmar esta suscripción de correo	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	electrónico para recibir las notificaciones de infracciones.	

Recursos relacionados

- CloudFormation Información sobre AWS
- Creación de una pila en la CloudFormation consola de AWS (CloudFormation documentación)
- CloudFront registro (CloudFront documentación)
- Información sobre Amazon S3
- Información sobre AWS Lambda

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Compruebe si hay entradas de red de un solo host en las reglas de ingreso de grupos de seguridad para IPv4 e IPv6

Creado por SaiJeevan Devireddy (AWS), Ganesh Kumar (AWS) y John Reynolds (AWS)

Entorno: producción	Tecnologías: redes, seguridad, identidad, cumplimiento	Servicios de AWS: Amazon SNS; AWS CloudWatch; CloudFormation Amazon; AWS Lambda; Amazon VPC

Resumen

Este patrón proporciona un control de seguridad que le notifica cuando los recursos de Amazon Web Services (AWS) no cumplen sus especificaciones. Proporciona una función de AWS Lambda que busca entradas de red de un solo host en los campos de direcciones de origen del grupo de seguridad del protocolo de Internet versión 4 (IPv4) e IPv6. La función Lambda se inicia cuando Amazon CloudWatch Events detecta la llamada a la API Amazon Elastic Compute Cloud (Amazon EC2) AuthorizeSecurityGroupIngress. La lógica personalizada de la función de Lambda evalúa la máscara de subred del bloque CIDR de la regla de entrada del grupo de seguridad. Si se determina que la máscara de subred es distinta de /32 (IPv4) o /128 (IPv6), la función de Lambda envía una notificación de infracción mediante Amazon Simple Notification Service (Amazon SNS).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- La dirección de correo electrónico en la que desee recibir notificaciones de infracción

Limitaciones

- Esta solución de monitorización de la seguridad es regional, por lo que debe implementarse en cada región de AWS que se supervise.

Arquitectura

Pila de tecnología de destino

- Función de Lambda
- Tema de SNS
- EventBridge Regla de Amazon

Arquitectura de destino

Automatizar y escalar

- Si utiliza AWS Organizations, puede utilizar AWS Cloudformation StackSets para implementar esta plantilla en varias cuentas que desee supervisar.

Herramientas

Servicios de AWS

- AWS CloudFormation es un servicio que le ayuda a modelar y configurar los recursos de AWS mediante el uso de la infraestructura como código.
- Amazon EventBridge ofrece un flujo de datos en tiempo real desde sus propias aplicaciones, aplicaciones de software como servicio (SaaS) y servicios de AWS, y dirige esos datos a objetivos como las funciones Lambda.
- AWS Lambda admite la ejecución de código sin aprovisionar ni administrar servidores.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos altamente escalable que se puede utilizar para una amplia gama de soluciones de almacenamiento, incluidos sitios web, aplicaciones móviles, copias de seguridad y lagos de datos.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) coordina y gestiona la entrega o el envío de mensajes entre publicadores y clientes, incluyendo los servidores web y las direcciones de correo electrónico. Los suscriptores reciben todos los mensajes publicados de los temas a los que están suscritos y todos los suscriptores de un tema reciben los mismos mensajes.

Código

El código adjunto incluye:

- Un archivo .zip que contiene el código de control de seguridad Lambda (`index.py`)
- Una CloudFormation plantilla (`security-control.yml`archivo) que se ejecuta para implementar el código Lambda

Epics

Cargue el control de seguridad

Tarea	Descripción	Habilidades requeridas
Cree el bucket de S3 para el código Lambda	En la consola de Amazon S3, cree un bucket de S3 con un nombre único que no contenga barras diagonales en el inicio. Un nombre de bucket S3 es globalmente único y todas las cuentas de AWS comparten el espacio de nombres. Su bucket de S3 debe estar en la región de AWS en la que desea implementar la verificación de ingreso del grupo de seguridad.	Arquitecto de la nube
Cargue el código Lambda en el bucket de S3.	Cargue el código Lambda (archivo `security-control-lambda.zip`) que se proporciona en la sección Archivos adjuntos en el bucket S3 que creó en el paso anterior.	Arquitecto de la nube

Implemente la plantilla CloudFormation

Tarea	Descripción	Habilidades requeridas
Cambie la versión de Python.	Descarga la CloudFormation plantilla (`security-control.yml`) que se proporciona en la sección de adjuntos. Abra el archivo y modifique la versión de Python para que refleje la última versión compatible con Lambda (actualmente Python 3.9). Por ejemplo, puede buscar `python` en el código y cambiar el valor para `Runtime` de `python3.6` a `python3.9`. Para obtener la información más reciente sobre la compatibilidad con las versiones en tiempo de ejecución de Python, consulte la documentación de AWS Lambda.	Arquitecto de la nube
Implemente la CloudFormation plantilla de AWS.	En la CloudFormation consola de AWS, en la misma región de AWS que el bucket de S3, implemente la CloudFormation plantilla (`security-control.yml`).	Arquitecto de la nube
Especifique el nombre del bucket de S3.	En el parámetro de Bucket de S3, especifique el nombre del	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	bucket de S3 que creó en la primera épica.	
Especifique el nombre de clave de Amazon S3 para el archivo Lambda.	Para el parámetro Clave de S3, especifique la ubicación en Amazon S3 del archivo .zip de código Lambda en su bucket de S3. No incluya barras diagonales iniciales (por ejemplo, puede escribir `lambda.zip` o `controls/lambda.zip`).	Arquitecto de la nube
Proporcione una dirección de correo electrónico para la notificación.	Para el parámetro Correo electrónico de notificación, proporcione una dirección de correo electrónico en la que te gustaría recibir las notificaciones de infracción.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Defina el nivel de registro.	Para el parámetro Nivel de registro de Lambda, defina el nivel de registro de la función de Lambda. Elija uno de los valores siguientes: • INFO para recibir mensajes informativos detallados sobre el progreso de la aplicación. • ERROR para obtener información sobre los eventos de error que podrían seguir permitiendo que la aplicación siguiera ejecutándose. • ADVERTENCIA para obtener información sobre situaciones potencialmente peligrosas.	Arquitecto de la nube

Confirmar la suscripción

Tarea	Descripción	Habilidades requeridas
Confirmar la suscripción.	Cuando la CloudFormation plantilla se haya implement ado correctamente, se creará un nuevo tema de SNS y se enviará un mensaje de suscripción a la dirección de correo electrónico que proporcionó. Debe confirmar esta suscripción de correo	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	electrónico para recibir las notificaciones de infracciones.	

Recursos relacionados

- CloudFormation Información sobre AWS
- Creación de una pila en la CloudFormation consola de AWS (CloudFormation documentación de AWS)
- Grupos de seguridad para su VPC (documentación de Amazon VPC)
- Información sobre Amazon S3
- Información sobre AWS Lambda

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Elija un flujo de autenticación de Amazon Cognito para aplicaciones empresariales

Creado por Michael Daehnert (AWS) y Fabian Jahnke (AWS)

Entorno: producción	Tecnologías: seguridad, identidad, conformidad	Servicios de AWS: Amazon Cognito

Resumen

Amazon Cognito proporciona autenticación, autorización y administración de usuarios para aplicaciones web y móviles. Ofrece funciones beneficiosas para la autenticación de identidades federadas. Para ponerlo en marcha, los arquitectos técnicos deben decidir cómo quieren utilizar esas funciones.

Amazon Cognito admite varios flujos para las solicitudes de autenticación. Estos flujos definen la forma en que los usuarios pueden verificar su identidad. La decisión sobre qué flujo de autenticación utilizar depende de los requisitos específicos de la aplicación y puede resultar compleja. Este patrón le ayuda a decidir qué flujo de autenticación es el más adecuado para su aplicación empresarial. Asume que ya tiene conocimientos básicos de Amazon Cognito, OpenID Connect (OIDC) y la federación, y le guía a través de los detalles sobre los diferentes flujos de autenticación federada.

Esta solución está destinada a los responsables de la toma de decisiones técnicas. Le ayuda a comprender los diferentes flujos de autenticación y a adaptarlos a los requisitos de su aplicación. Los líderes técnicos deben recopilar la información necesaria para iniciar las integraciones de Amazon Cognito. Dado que las organizaciones empresariales se centran principalmente en la federación de SAML, este patrón incluye descripciones de los grupos de usuarios de Amazon Cognito con federación de SAML.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Funciones y permisos de AWS Identity and Access Management (IAM) con acceso total a Amazon Cognito

- (Opcional) Acceso a su proveedor de identidad (IdP), como Microsoft Entra ID, Active Directory Federation Service (AD FS) u Okta
- Un alto nivel de experiencia para su aplicación
- Conocimientos básicos de Amazon Cognito, OpenID Connect (OIDC) y federación

Limitaciones

- Este patrón se centra en los grupos de usuarios y los proveedores de identidades de Amazon Cognito. Para obtener información sobre los grupos de identidades de Amazon Cognito, consulte la sección Información adicional.

Arquitectura

Utilice la siguiente tabla como ayuda para elegir un flujo de autenticación. En esta sección se proporciona más información sobre cada flujo.

¿Necesita machine-to-machine autenticación?	¿Su aplicación es una aplicación basada en la web en la que la interfaz se representa en el servidor?	¿Su aplicación es una aplicación de una sola página (SPA) o una aplicación frontend basada en dispositivos móviles?	¿Su aplicación requiere tokens de actualización para poder utilizar la función de «mantenerme conectado»?	¿La interfaz ofrece un mecanismo de redireccionamiento basado en el navegador?	Flujo recomendado de Amazon Cognito
Sí	No	No	No	No	Flujo de credenciales de clientes
No	Sí	No	Sí	Sí	Flujo de códigos de autorización

No	No	Sí	Sí	Sí	Flujo de códigos de autorización con clave de prueba para el intercambio de códigos (PKCE)
No	No	No	No	No	Flujo de contraseñas del propietario del recurso*

* El flujo de contraseñas del propietario del recurso solo debe usarse si es absolutamente necesario. Para obtener más información, consulte la sección sobre el flujo de contraseñas del propietario del recurso en este patrón.

Flujo de credenciales de cliente

El flujo de credenciales de cliente es el más corto de los flujos de Amazon Cognito. Debe usarse si los sistemas o servicios se comunican entre sí sin la interacción del usuario. El sistema solicitante utiliza el ID del cliente y el secreto del cliente para recuperar un token de acceso. Como ambos sistemas funcionan sin la interacción del usuario, no se requiere ningún paso de consentimiento adicional.

En el siguiente diagrama se ilustra lo siguiente:

1. La aplicación 1 envía una solicitud de autenticación con el ID y el secreto del cliente al punto de conexión de Amazon Cognito y recupera un token de acceso.
2. La aplicación 1 usa este token de acceso para cada llamada posterior a la aplicación 2.
3. La aplicación 2 valida el token de acceso con Amazon Cognito.

Se debe usar este flujo:

- Para las comunicaciones entre aplicaciones sin interacción con el usuario

No se debe utilizar este flujo:

- Para cualquier comunicación en la que sea posible la interacción del usuario

Flujo de códigos de autorización

El flujo del código de autorización es para la autenticación clásica basada en la web. En este flujo, el backend gestiona todo el intercambio y el almacenamiento de los tokens. El cliente basado en un navegador no ve los tokens reales. Esta solución se utiliza para aplicaciones escritas en marcos como .NET Core, Jakarta Faces o Jakarta Server Pages (JSP).

El flujo del código de autorización es un flujo basado en la redirección. El cliente debe poder interactuar con el navegador web o un cliente similar. El cliente se redirige a un servidor de autenticación y se autentica en este servidor. Si el cliente se autentica correctamente, se redirige de nuevo al servidor.

En el siguiente diagrama se ilustra lo siguiente:

1. El cliente envía una solicitud al servidor web.
2. El servidor web redirige al cliente a Amazon Cognito mediante un código de estado HTTP 302. El cliente sigue automáticamente esta redirección hasta el inicio de sesión del IdP configurado.
3. El IdP comprueba si hay una sesión de navegador existente en el lado del IdP. Si no existe ninguna, el usuario recibe una solicitud para autenticarse proporcionando su nombre de usuario y contraseña. El IdP responde con un token SAML a Amazon Cognito.
4. Amazon Cognito logra el éxito con un token web JSON (JWT), específicamente un token de código. El servidor web llama a /oauth2/token para cambiar el token de código por un token de acceso. El servidor web envía el ID y el secreto del cliente a Amazon Cognito para su validación.
5. El token de acceso se utiliza para cada llamada posterior a otras aplicaciones.
6. Otras aplicaciones validan el token de acceso con Amazon Cognito.

Se debe utilizar este flujo:

- Si el usuario puede interactuar con el navegador web o el cliente. El código de la aplicación se ejecuta y renderiza en el servidor para garantizar que el navegador no conozca ningún secreto.

No se debe usar este flujo:

- Para aplicaciones de una sola página (SPA) o aplicaciones móviles, ya que se renderizan en el cliente y no deberían usar secretos del cliente.

Flujo de códigos de autorización con PKCE

El flujo de códigos de autorización con clave de prueba para el intercambio de códigos (PKCE) debe usarse para aplicaciones de una sola página y aplicaciones móviles. Es el sucesor del flujo implícito y es más seguro porque utiliza el PKCE. PKCE es una extensión de la concesión de códigos de autorización de OAuth 2.0 para clientes públicos. La PKCE evita el canje de los códigos de autorización interceptados.

En el siguiente diagrama se ilustra lo siguiente:

1. La aplicación crea un verificador de código y un desafío de código. Se trata de valores únicos y bien definidos que se envían a Amazon Cognito para consultarlos en el futuro.
2. La aplicación llama al punto final /oauth2/authorization de Amazon Cognito. Redirige automáticamente al usuario al inicio de sesión del IdP configurado.
3. El IdP comprueba si hay una sesión existente. Si no existe ninguna, el usuario recibe una solicitud para autenticarse proporcionando su nombre de usuario y contraseña. El IdP responde con un token SAML a Amazon Cognito.
4. Cuando Amazon Cognito devuelve correctamente un token de código, el servidor web llama a /oauth2/token para cambiar el token de código por un token de acceso.
5. El token de acceso se utiliza para cada llamada posterior a otras aplicaciones.
6. Las demás aplicaciones validan el token de acceso con Amazon Cognito.

Se debe utilizar este flujo:

- Para SPA o aplicaciones móviles

No se debe utilizar este flujo:

- Si el backend de la aplicación se encarga de la autenticación

Flujo de contraseñas del propietario del recurso

El flujo de contraseñas del propietario del recurso está destinado a aplicaciones sin capacidades de redireccionamiento. Se crea mediante la creación de un formulario de inicio de sesión en su propia aplicación. El inicio de sesión se comprueba en Amazon Cognito mediante una llamada a la CLI o al SDK, en lugar de depender de los flujos de redireccionamiento. La federación no es posible en este flujo de autenticación porque la federación requiere redireccionamientos basados en el navegador.

En el siguiente diagrama se ilustra lo siguiente:

1. El usuario introduce sus credenciales en un formulario de inicio de sesión proporcionado por la aplicación.
2. La interfaz de línea de comandos de AWS (AWS CLI) realiza admin-initiated-authuna llamada a Amazon Cognito.

   Nota: Como alternativa, puede utilizar los SDK de AWS en lugar de la CLI de AWS.
3. Amazon Cognito devuelve un token de acceso.
4. El token de acceso se utiliza para cada llamada posterior a otras aplicaciones.
5. Las demás aplicaciones validan el token de acceso con Amazon Cognito.

Se debe utilizar este flujo:

- Al migrar los clientes existentes que utilizan una lógica de autenticación directa (como la autenticación de acceso básica o la autenticación de acceso implícita) a OAuth mediante la conversión de las credenciales almacenadas en un token de acceso

No se debe utilizar este flujo:

- Si desea utilizar identidades federadas
- Si su aplicación admite redireccionamientos

Herramientas

Servicios de AWS

- Amazon Cognito ofrece autenticación, autorización y administración de usuarios para aplicaciones móviles y web.

Otras herramientas

- El depurador del token web JSON (JWT) es una herramienta de validación de JWT basada en la web.

Epics

Evalúe su solicitud

Tarea	Descripción	Habilidades requeridas
Defina los requisitos de autenticación.	Evalúe su aplicación de acuerdo con sus requisitos de autenticación específicos.	Desarrollador de aplicaciones, arquitecto de aplicaciones
Alinee los requisitos con los flujos de autenticación.	En la sección Arquitectura, utilice la tabla de decisiones y las explicaciones de cada flujo para elegir el flujo de autentica ción de Amazon Cognito.	Desarrollador de aplicaciones, AWS general, arquitecto de aplicaciones

Configurar el grupo de usuarios de Amazon Cognito

Tarea	Descripción	Habilidades requeridas
Cree un grupo de usuarios.	1. Inicie sesión en la consola de administración de AWS y, a continuación, abra la consola de Amazon Cognito.	AWS general

Tarea	Descripción	Habilidades requeridas
	2. Cree un nuevo grupo de usuarios de Cognito. Para obtener instrucciones, consulte Grupos de usuarios de Amazon Cognito. 3. Actualice la configuración y los atributos del grupo de usuarios según sea necesario. Por ejemplo, establezca una política de contraseñas para el grupo de usuarios. No cree clientes de aplicaciones todavía.	

Tarea	Descripción	Habilidades requeridas
(Opcional) Configure un proveedor de identidades.	1. Cree un proveedor de identidades SAML en el grupo de usuarios de Amazon Cognito. Para obtener instrucciones, consulte Añadir y administrar proveedores de identidad de SAML en un grupo de usuarios. 2. Configure su proveedor de identidad SAML externo para que funcione con la federación para los grupos de usuarios de Amazon Cognito. Para obtener más información, consulte Configuración de su proveedor de identidades SAML de terceros. Si utiliza AD FS, consulte Creación de una federación de AD FS para su aplicación web mediante grupos de usuarios de Amazon Cognito (entrada del blog de AWS).	AWS general, administrador de la federación

Tarea	Descripción	Habilidades requeridas
Cree un cliente de aplicaciones.	1. Cree un cliente de aplicaciones para el grupo de usuarios. Para obtener instrucciones, consulte Crear un cliente de aplicaciones. Tenga en cuenta lo siguiente: • Cambie la configuración según sea necesario, como la caducidad de los tokens. • Si su flujo de autenticación no requiere un secreto de cliente, desactive la casilla Generar secreto de cliente. 2. Elija la configuración del cliente de aplicaciones para cambiar su integración a un inicio de sesión de grupo de usuarios (nombre de usuario y contraseña) o un inicio de sesión federado a través de un IdP basado en SAML. 3. Habilite su IdP definiendo las URL y definiendo los flujos o ámbitos de OAuth según sea necesario.	AWS general

Integrar la aplicación con Amazon Cognito

Tarea	Descripción	Habilidades requeridas
Detalles de la integración de Amazon Cognito de Exchange.	Según el flujo de autentica ción, comparta la informaci ón de Amazon Cognito con la aplicación, como el ID del grupo de usuarios y el ID del cliente de la aplicación.	Desarrollador de aplicaciones, AWS general
Implemente la autenticación de Amazon Cognito.	Esto depende del flujo de autenticación que elija, del lenguaje de programación y de los marcos que utilice. Para ver algunos enlaces para empezar, consulte la sección de recursos relacionados.	Desarrollador de aplicaciones

Recursos relacionados

Documentación de AWS

- Flujo de autenticación de grupos de usuarios
- Verificar un token web JSON
- Acceda a los servicios de AWS desde una aplicación ASP.NET Core mediante los grupos de identidades de Amazon Cognito
- Marcos y SDK:
  - Autenticación Amazon Amplify
  - Ejemplos de proveedores de identidad de Amazon Cognito (documentación de AWS SDK for Java 2.x)
  - Autenticación de usuarios con Amazon Cognito (documentación de AWS SDK for .NET)

Publicaciones del blog de AWS

- Uso de cookies por parte de Authorization @Edge: protege tu CloudFront contenido de Amazon para que no lo descarguen usuarios no autenticados
- Creación de una federación de AD FS para su aplicación web mediante grupos de usuarios de Amazon Cognito

Socios de implementación

- Socios de AWS para soluciones de autenticación

Información adicional

PREGUNTAS FRECUENTES

¿Por qué está obsoleto el flujo implícito?

Desde el lanzamiento del marco OAuth 2.1, el flujo implícito se ha marcado como obsoleto por motivos de seguridad. Como alternativa, utiliza el flujo de códigos de autorización con el PKCE que se describe en la sección de arquitectura.

¿Qué sucede si Amazon Cognito no ofrece alguna de las funciones que necesito?

Los socios de AWS ofrecen diferentes integraciones para las soluciones de autenticación y autorización. Para obtener más información, consulte los socios de AWS para obtener información sobre las soluciones de autenticación.

¿Qué pasa con los flujos del grupo de identidades de Amazon Cognito?

Los grupos de usuarios de Amazon Cognito y las identidades federadas sirven para la autenticación. Los grupos de identidades de Amazon Cognito se utilizan para autorizar el acceso a los recursos de AWS mediante la solicitud de credenciales de AWS temporales. En este patrón no se describe el intercambio de los tokens de ID y de acceso para los grupos de identidades. Para obtener más información, consulte Cuál es la diferencia entre los grupos de usuarios y los grupos de identidades de Amazon Cognito y los escenarios comunes de Amazon Cognito.

Pasos siguientes

Este patrón proporciona una descripción general de los flujos de autenticación de Amazon Cognito. Como siguiente paso, es necesario elegir la implementación detallada del lenguaje de programación de la aplicación. Varios lenguajes ofrecen SDK y marcos, que puede usar con Amazon Cognito. Para obtener referencias útiles, consulte la sección de recursos relacionados.

Cree reglas personalizadas de AWS Config mediante las políticas de AWS CloudFormation Guard

Repositorio de código: aws-config-custom-rule-cloudformation-guard	Entorno: PoC o piloto	Tecnologías: seguridad, identidad, conformidad; administración y gobernanza
Servicios de AWS: AWS CloudFormation; AWS Config		

Resumen

Las reglas de AWS Config le ayudan a evaluar sus recursos de AWS y su estado de configuración objetivo. Existen dos tipos de reglas de AWS Config: administradas y personalizadas. Puede crear reglas personalizadas con las funciones de AWS Lambda o con AWS CloudFormation Guard (GitHub), un policy-as-code lenguaje.

Las reglas creadas con Guard proporcionan un control más detallado que las reglas administradas y, por lo general, son más fáciles de configurar que las reglas Lambda totalmente personalizadas. Este enfoque proporciona a los ingenieros y arquitectos la capacidad de crear reglas sin necesidad de conocer Python, Nodejs o Java, que son necesarios para implementar reglas personalizadas a través de Lamdba.

Este patrón proporciona plantillas, ejemplos de código y enfoques de implementación viables para ayudarlo a adoptar reglas personalizadas con Guard. Con este patrón, un administrador puede usar AWS Config para crear reglas de conformidad personalizadas con atributos de elementos de configuración. Por ejemplo, los desarrolladores pueden usar las políticas de Guard contra los elementos de configuración de AWS Config para monitorear continuamente el estado de los recursos implementados de AWS y de terceros, detectar infracciones de las reglas e iniciar automáticamente las correcciones.

Objetivos

Después de leer este patrón, debería poder:

- Comprenda cómo el código de políticas de Guard interactúa con el servicio AWS Config.

- Implemente el escenario 1, que es una regla personalizada de AWS Config que utiliza la sintaxis Guard para validar la conformidad de los volúmenes cifrados. Esta regla verifica que la unidad esté en uso y que el tipo de unidad sea gp3.
- Implemente el escenario 2, que es una regla personalizada de AWS Config que utiliza la sintaxis Guard para validar la GuardDuty conformidad de Amazon. Esta regla verifica que las GuardDuty grabadoras tengan habilitadas las protecciones Amazon S3 y Amazon EKS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- AWS Config, configure en su cuenta de AWS

Limitaciones

- Las reglas personalizadas de Guard solo pueden consultar pares clave-valor en un registro JSON de un elemento de configuración de destino

Arquitectura

La sintaxis de Guard se aplica a una regla de AWS Config como política personalizada. AWS Config captura el JSON jerárquico de cada uno de los recursos especificados. El JSON del elemento de configuración de AWS Config contiene pares clave-valor. Estos atributos se utilizan en la sintaxis de Guard como variables que se asignan a su valor correspondiente.

A continuación se explica la sintaxis de Guard. Las variables del elemento de configuración JSON se utilizan y van precedidas de un `%` carácter.

```
# declare variable
let <variable name> = <'value'>

# create rule and assign condition and policy
    rule <rule name> when
        <CI json key> == <"CI json value"> {
            <top level CI json key>.<next level CI json key> == %<variable name>
        }
```

Escenario 1: volúmenes de Amazon EBS

El escenario 1 implementa una regla personalizada de AWS Config que utiliza la sintaxis Guard para validar la conformidad de los volúmenes cifrados. Esta regla verifica que la unidad esté en uso y que el tipo de unidad sea gp3.

El siguiente es un ejemplo de un elemento de configuración de AWS Config para el escenario 1. Hay tres pares clave-valor en este elemento de configuración que se utilizan como variables en la política de Guard: `volumestatusvolumeencryptionstatus`, y. `volumetype` Además, la `resourceType` clave se usa como filtro en la política de Guard.


```
{
  "version": "1.3",
  "accountId": "111111111111",
  "configurationItemCaptureTime": "2023-01-15T19:04:45.402Z",
  "configurationItemStatus": "ResourceDiscovered",
  "configurationStateId": "4444444444444",
  "configurationItemMD5Hash": "",
  "arn": "arn:aws:ec2:us-west-2:111111111111:volume/vol-222222222222",
  "resourceType": "AWS::EC2::Volume",
  "resourceId": "vol-222222222222",
  "awsRegion": "us-west-2",
  "availabilityZone": "us-west-2b",
  "resourceCreationTime": "2023-01-15T19:03:22.247Z",
  "tags": {},
  "relatedEvents": [],
  "relationships": [
    {
      "resourceType": "AWS::EC2::Instance",
      "resourceId": "i-33333333333333333",
      "relationshipName": "Is attached to Instance"
    }
  ],
  "configuration": {
    "attachments": [
      {
        "attachTime": "2023-01-15T19:03:22.000Z",
        "device": "/dev/xvda",
        "instanceId": "i-33333333333333333",
        "state": "attached",
        "volumeId": "vol-222222222222",
        "deleteOnTermination": true,
        "associatedResource": null,
```

```
        "instanceOwningService": null
      }
    ],
    "availabilityZone": "us-west-2b",
    "createTime": "2023-01-15T19:03:22.247Z",
    "encrypted": false,
    "kmsKeyId": null,
    "outpostArn": null,
    "size": 8,
    "snapshotId": "snap-55555555555555555",
    "state": "in-use",
    "volumeId": "vol-222222222222",
    "iops": 100,
    "tags": [],
    "volumeType": "gp2",
    "fastRestored": null,
    "multiAttachEnabled": false,
    "throughput": null,
    "sseType": null
  },
  "supplementaryConfiguration": {}
}
```

El siguiente es un ejemplo del uso de la sintaxis de Guard para definir las variables y las reglas en el escenario 1. En el siguiente ejemplo:

- Las tres primeras líneas definen las variables mediante el `let` comando. Se les asigna un nombre y un valor que se derivan de los atributos del elemento de configuración.
- El bloque de `compliancecheck` reglas agrega una dependencia condicional de cuándo que busca un par `resourceType` clave-valor que coincida. `AWS::EC2::Volume` Si se encuentra una coincidencia, la regla pasa por el resto de los atributos de JSON y busca coincidencias en las tres condiciones siguientes: `stateencrypted`, y. `volumeType`

```
let volumestatus = 'available'
let volumetype = 'gp3'
let volumeencryptionstatus = true

    rule compliancecheck when
        resourceType == "AWS::EC2::Volume" {
            configuration.state == %volumestatus
            configuration.encrypted == %volumeencryptionstatus
```

```
            configuration.volumeType == %volumetype
        }
```

Para ver la política personalizada completa de CloudFormation Guard que implementa esta regla personalizada, consulta awsconfig-guard-cft.yaml o awsconfig-guard-tf-ec2vol.json en el repositorio de código. GitHub Para ver HashiCorp el código de Terraform que implementa esta política CloudFormation personalizada en Guard, consulta awsconfig-guard-tf-example.json en el repositorio de código.

Escenario 2: cumplimiento GuardDuty

El escenario 2 implementa una regla personalizada de AWS Config que utiliza la sintaxis Guard para validar la GuardDuty conformidad de Amazon. Esta regla verifica que las GuardDuty grabadoras tengan habilitadas las protecciones Amazon S3 y Amazon EKS. También verifica que los GuardDuty resultados se publiquen cada 15 minutos. Este escenario podría implementarse en todas las cuentas y regiones de AWS de una organización (en AWS Organizations).

El siguiente es un ejemplo de un elemento de configuración de AWS Config para el escenario 2. Hay tres pares clave-valor en este elemento de configuración que se utilizan como variables en la política de Guard: `FindingPublishingFrequency`, `S3Logs`, y. `Kubernetes` Además, la `resourceType` clave se usa como filtro en la política.

```
{
  "version": "1.3",
  "accountId": "111111111111",
  "configurationItemCaptureTime": "2023-11-27T13:34:28.888Z",
  "configurationItemStatus": "OK",
  "configurationStateId": "7777777777777",
  "configurationItemMD5Hash": "",
  "arn": "arn:aws:guardduty:us-
west-2:111111111111:detector/66666666666666666666666666666666",
  "resourceType": "AWS::GuardDuty::Detector",
  "resourceId": "66666666666666666666666666666666",
  "resourceName": "66666666666666666666666666666666",
  "awsRegion": "us-west-2",
  "availabilityZone": "Regional",
  "resourceCreationTime": "2020-02-17T02:48:04.511Z",
  "tags": {},
  "relatedEvents": [],
  "relationships": [],
  "configuration": {
    "Enable": true,
```

```
    "FindingPublishingFrequency": "FIFTEEN_MINUTES",
    "DataSources": {
      "S3Logs": {
        "Enable": true
      },
      "Kubernetes": {
        "AuditLogs": {
          "Enable": true
        }
      }
    },

    "Id": "66666666666666666666666666666666",
    "Tags": []
  },
  "supplementaryConfiguration": {
    "CreatedAt": "2020-02-17T02:48:04.511Z"
  }
}
```

El siguiente es un ejemplo del uso de la sintaxis de Guard para definir las variables y las reglas en el escenario 2. En el siguiente ejemplo:

- Las tres primeras líneas definen las variables mediante el `let` comando. Se les asigna un nombre y un valor que se derivan de los atributos del elemento de configuración.
- El bloque de `compliancecheck` reglas agrega una dependencia condicional de cuándo que busca un par `resourceType` clave-valor que coincida. `AWS::GuardDuty::Detector` Si se encuentra una coincidencia, la regla pasa por el resto de los atributos de JSON y busca coincidencias en las tres condiciones siguientes: `S3Logs.Enable``Kubernetes.AuditLogs.Enable`, y. `FindingPublishingFrequency`

```
let s3protection = true
let kubernetesprotection = true
let publishfrequency = 'FIFTEEN_MINUTES'

    rule compliancecheck when
        resourceType == "AWS::GuardDuty::Detector" {
            configuration.DataSources.S3Logs.Enable == %s3protection
            configuration.DataSources.Kubernetes.AuditLogs.Enable ==
 %kubernetesprotection
            configuration.FindingPublishingFrequency == %publishfrequency
```

```
        }
```

Para ver la política personalizada completa de CloudFormation Guard que implementa esta regla personalizada, consulta awsconfig-guard-cft-gd.yaml en el repositorio de código. GitHub Para ver el código de HashiCorp Terraform que implementa esta política personalizada en Guard, consulta awsconfig-guard-tf-gd.json en el repositorio de código. CloudFormation

Herramientas

Servicios de AWS

- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- AWS Config proporciona una visión detallada de los recursos de su cuenta de AWS y de cómo están configurados. Le ayuda a identificar cómo se relacionan los recursos entre sí y cómo han cambiado sus configuraciones a lo largo del tiempo.

Otras herramientas

- HashiCorp Terraform es una herramienta de código abierto de infraestructura como código (IaC) que le ayuda a utilizar el código para aprovisionar y gestionar la infraestructura y los recursos de la nube.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub AWS Config with CloudFormation Guard. Este repositorio de código contiene ejemplos de los dos escenarios descritos en este patrón.

Epics

Creación de reglas personalizadas de AWS Config

Tarea	Descripción	Habilidades requeridas
(Opcional) Seleccione pares clave-valor para la regla.	Complete estos pasos si va a definir una política de Guard personalizada. Si utiliza uno de los ejemplos de políticas	Administrador de AWS, ingeniero de seguridad

Tarea	Descripción	Habilidades requeridas
	para el escenario 1 o 2, omita estos pasos. 1. Inicie sesión en la consola de administración de AWS y abra la consola de AWS Config en https://console.aws.amazon.com/config/. 2. En el menú de navegación de la izquierda, elija Recursos. 3. En el inventario de recursos, elija el tipo de recurso para el que quiere crear una regla personalizada de AWS Config. 4. Elija Ver detalles. 5. Elija Ver elemento de configuración (JSON). Esta sección se amplía para mostrar el elemento de configuración en formato JSON. 6. Identifique los pares clave-valor para los que desea crear una regla personalizada de AWS Config.	

Tarea	Descripción	Habilidades requeridas
Cree la regla personalizada.	Con los pares clave-valor que identificó anteriormente o con uno de los ejemplos de políticas de Guard proporcionados, siga las instrucciones de Creating AWS Config Custom Policy Rules para crear una regla personalizada.	Administrador de AWS, ingeniero de seguridad
Valide la regla personalizada.	Realice una de las siguientes acciones para validar la regla de protección personalizada: • Introduzca el siguiente comando en la interfaz de línea de comandos de AWS (AWS CLI). `cfn-guard validate -r guard-s3.guard -d s3bucket-prod-pass.json` • Siga las instrucciones del modo Detective en Evaluation Your Resources with AWS Config Rules para implementar la regla en AWS Config. Confirme que la sintaxis de Guard coincide correctamente con los recursos correspondientes de la cuenta o el archivo de destino.	Administrador de AWS, ingeniero de seguridad

Resolución de problemas

Problema	Solución
Pruebe la política de CloudFormation Guard fuera de AWS Config	Las pruebas unitarias se pueden realizar en su dispositivo local o en un entorno de desarroll o integrado (IDE), como un IDE de AWS Cloud9. Para realizar pruebas unitarias, haga lo siguiente: 1. Instale la CLI de AWS CloudFormation Guard y sus dependencias. 2. Guarde un ejemplo de CI con formato JSON en su estación de trabajo como un archivo.j son. 3. Guarde la GuardDuty política en su estación de trabajo como un archivo.guard. 4. En la CLI de Guard, introduzca el siguiente comando para validar el archivo JSON de muestra mediante la política de Guard. `cfn-guard validate \` `-r guard-s3.guard \` `-d s3bucket-prod-pass.json`
Depurar una regla personalizada de AWS Config	En su política de Guard, cambie el `EnableDeb ugLogDelivery` valor `atrue`. El valor predeterminado es `false`. Los mensajes de registro se almacenan en Amazon CloudWatch.

Recursos relacionados

Documentación de AWS

- Creación de reglas de políticas personalizadas de AWS Config (documentación de AWS Config)
- Redacción de reglas de AWS CloudFormation CloudFormation Guard (documentación de Guard)

Publicaciones de blog y talleres de AWS

- Presentación de AWS CloudFormation Guard 2.0 (entrada del blog de AWS)

Otros recursos

- AWS CloudFormation Guard (GitHub)
- CloudFormation Documentación de Guard CLI (GitHub)

Crear un informe consolidado de los resultados de seguridad de Prowler en varias cuentas de AWS

Repositorio de código: evaluación de seguridad de múltiples cuentas mediante prowler	Entorno: producción	Tecnologías: seguridad, identidad, conformidad
Carga de trabajo: código abierto	Servicios de AWS: AWS CloudFormation; Amazon EC2; AWS Identity and Access Management	

Resumen

Prowler (GitHub) es una herramienta de línea de comandos de código abierto que puede ayudarle a evaluar, auditar y supervisar sus cuentas de Amazon Web Services (AWS) para comprobar si cumplen las mejores prácticas de seguridad. En este patrón, despliega Prowler de forma centralizada Cuenta de AWS en su organización, gestionada por Prowler y, a continuación AWS Organizations, utiliza Prowler para realizar una evaluación de seguridad de todas las cuentas de la organización.

Si bien existen muchos métodos para implementar y utilizar Prowler para realizar una evaluación, esta solución se ha diseñado para una implementación rápida, un análisis completo de todas las cuentas de la organización o de las cuentas objetivo definidas, y la elaboración de informes accesibles sobre los problemas de seguridad. En esta solución, cuando Prowler completa la evaluación de seguridad de todas las cuentas de la organización, consolida los resultados. También filtra cualquier mensaje de error esperado, como los errores relacionados con las restricciones que impiden a Prowler escanear los buckets de Amazon Simple Storage Service (Amazon S3) en las cuentas aprovisionadas a través de AWS Control Tower. Los resultados filtrados y consolidados se presentan en una plantilla de Microsoft Excel que se incluye con este patrón. Puede utilizar este informe para identificar posibles mejoras en los controles de seguridad de su organización.

Esta solución se diseñó teniendo en cuenta lo siguiente:

- Las AWS CloudFormation plantillas reducen el esfuerzo necesario para implementar los AWS recursos en este patrón.

- Puede ajustar los parámetros de las CloudFormation plantillas y del script prowler_scan.sh en el momento de la implementación para personalizar las plantillas para su entorno.
- Las velocidades de evaluación e informes de Prowler se optimizan mediante el procesamiento paralelo de los resultados agregados Cuentas de AWS, los informes consolidados con las soluciones recomendadas y las visualizaciones generadas automáticamente.
- El usuario no necesita monitorizar el progreso del escaneo. Cuando se completa la evaluación, se notifica al usuario a través de un tema de Amazon Simple Notification Service (Amazon SNS) para que pueda recuperar el informe.
- La plantilla de informe le ayuda a leer y evaluar solo los resultados relevantes para toda la organización.

Requisitos previos y limitaciones

Requisitos previos

- Y Cuenta de AWS para alojar servicios y herramientas de seguridad, gestionados como una cuenta de miembro de una organización en. AWS Organizations En este patrón, esta cuenta se denomina cuenta de seguridad.
- En la cuenta de seguridad, debe tener una subred privada con acceso saliente a Internet. Para obtener instrucciones, consulte VPC con servidores en subredes privadas y NAT en la documentación de Amazon Virtual Private Cloud (Amazon VPC). Puede establecer el acceso a Internet mediante una puerta de enlace NAT aprovisionada en una subred pública.
- Acceso a la cuenta AWS Organizations de administración o a una cuenta para la que se hayan delegado permisos de CloudFormation administrador. Para obtener instrucciones, consulte Registrar un administrador delegado en la CloudFormation documentación.
- Habilite el acceso confiable entre AWS Organizations y. CloudFormation Para obtener instrucciones, consulte Habilitar el acceso confiable con AWS Organizations en la CloudFormation documentación.

Limitaciones

- El objetivo Cuentas de AWS debe gestionarse como una organización en AWS Organizations. Si no la utiliza AWS Organizations, puede actualizar la CloudFormation plantilla ProwlerExecIAM-Role.yaml y el script prowler_scan.sh para su entorno. En su lugar, proporciona una lista de Cuenta de AWS identificadores y regiones en las que desea ejecutar el script.

- La CloudFormation plantilla está diseñada para implementar la instancia de Amazon Elastic Compute Cloud (Amazon EC2) en una subred privada con acceso saliente a Internet. El AWS Systems Manager agente (SSM Agent) requiere acceso saliente para llegar al punto final del AWS Systems Manager servicio, y usted necesita acceso saliente para clonar el repositorio de código e instalar las dependencias. Si desea utilizar una subred pública, debe modificar la plantilla prowler-resources.yaml para asociar una Dirección IP elástica a la instancia de EC2.

Versiones de producto

- Prowler versión 3.0 o posterior

Arquitectura

El diagrama muestra el proceso siguiente:

1. Con el administrador de sesiones, una capacidad de AWS Systems Manager, el usuario se autentica en la instancia EC2 y ejecuta el script prowler_scan.sh. Este script del intérprete de comandos lleva a cabo los pasos del 2 al 8.
2. La instancia EC2 asume el rol de IAM de `ProwlerEC2Role`, que concede permisos para acceder al bucket de S3 y para asumir los roles de IAM de `ProwlerExecRole` en las demás cuentas de la organización.
3. La instancia EC2 asume el rol de IAM de `ProwlerExecRole` en la cuenta de administración de la organización y genera una lista de las cuentas de la organización.
4. La instancia EC2 asume el rol de IAM `ProwlerExecRole` en las cuentas de los miembros de la organización (denominadas cuentas de carga de trabajo en el diagrama de arquitectura) y realiza una evaluación de seguridad en cada cuenta. Los resultados se almacenan como archivos CSV y HTML en la instancia EC2.

   Nota: Los archivos HTML son el resultado de la evaluación de Prowler. Debido a la naturalez a del HTML, no se concatenan, procesan ni utilizan directamente en este patrón. Sin embargo, pueden resultar útiles para revisar los informes de cuentas individuales.

5. La instancia EC2 procesa todos los archivos CSV para eliminar los errores conocidos y esperados y consolida los resultados restantes en un solo archivo CSV.

6. La instancia EC2 ejecuta el script generateVisualizations.py. Este script procesa el archivo CSV de los resultados agregados y genera archivos PNG de gráficos y tablas que pueden ayudarle a comprender los resultados y a informar sobre ellos. También crea un archivo HTML que contiene información sobre el escaneo y los archivos PNG.
7. La instancia EC2 empaqueta los resultados de las cuentas individuales, los resultados agregados y las visualizaciones generadas en un archivo zip.
8. La instancia de EC2 carga el archivo .zip en el bucket de S3.
9. Una EventBridge regla detecta la carga del archivo y utiliza un tema de Amazon SNS para enviar un correo electrónico al usuario en el que se le notifica que la evaluación ha finalizado.
10. El usuario descarga el archivo zip del bucket de S3. El usuario importa los resultados a la plantilla de Excel y revisa los resultados.

Herramientas

Servicios de AWS

- Amazon Elastic Compute Cloud (Amazon EC2) brinda capacidad de computación escalable en la Nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, AWS Lambda funciones, puntos de enlace de invocación HTTP que utilizan destinos de API o buses de eventos en otros. Cuentas de AWS
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS Organizationses un servicio de administración de cuentas que le ayuda a consolidar múltiples cuentas Cuentas de AWS en una organización que usted crea y administra de forma centralizada.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Systems Manager le ayuda a administrar las aplicaciones y la infraestructura que se ejecutan en la Nube de AWS. Simplifica la administración de aplicaciones y recursos, reduce el tiempo

necesario para detectar y resolver problemas operativos y le ayuda a administrar sus AWS recursos de forma segura y a escala. Este patrón utiliza Session Manager, una capacidad de Systems Manager.

Otras herramientas

- Prowler es una herramienta de línea de comandos de código abierto que le ayuda a evaluar, auditar y supervisar sus cuentas para comprobar si cumplen las mejores prácticas de seguridad y otros marcos y AWS estándares de seguridad.

Repositorio de código

El código de este patrón está disponible en la evaluación de seguridad GitHub multicuenta del repositorio Prowler. El repositorio de código contiene los siguientes archivos:

- prowler_scan.sh: este script bash se utiliza para iniciar una evaluación de seguridad de Prowler de varios, Cuentas de AWS en paralelo. Como se define en Prowler-Resources.yaml CloudFormationtemplate, este script se implementa automáticamente en la carpeta de la instancia EC2. `usr/local/prowler`
- Prowler-Resources.yaml: usa esta plantilla para crear una pila en la cuenta de seguridad de la organización. CloudFormation Esta plantilla implementa todos los recursos necesarios para esta cuenta a fin de respaldar la solución. Esta pila debe implementarse antes que la plantilla IAM-Role.yaml. ProwlerExec No se recomienda implementar estos recursos en una cuenta que aloje cargas de trabajo de producción críticas.

  Nota: Si esta pila se elimina y se vuelve a implementar, debe volver a crear el conjunto de pilas `ProwlerExecRole` para recuperar las dependencias entre cuentas entre los roles de IAM.

- IAM- ProwlerExec Role.yaml: usa esta CloudFormation plantilla para crear un conjunto de pilas que despliegue la función de `ProwlerExecRole` IAM en todas las cuentas de la organización, incluida la cuenta de administración.
- generateVisualizations.py: el script prowler_scan.sh llama automáticamente a este script de Python para generar visualizaciones basadas en los resultados agregados y las incluye en el archivo .zip almacenado en el bucket de S3. Este script crea los siguientes archivos:
  - `FailuresByAccount-<date>.png`: gráfico de barras que ilustra las comprobaciones de Prowler fallidas para cada cuenta

- `FailuresByService-<date>.png`— Gráfico de barras que ilustra las comprobaciones de Prowler fallidas de cada una Servicio de AWS
- `ProcessedResultsByFailureSeverityCount-<date>.png`: gráfico de barras que ilustra la distribución de las comprobaciones de Prowler fallidas para cada nivel de gravedad (crítico, alto, medio, bajo e informativo)
- `ResultsByFail-<date>.png`: gráfico circular de las comprobaciones de Prowler fallidas por gravedad
- `ResultsBySeverity-<date>.png`: gráfico circular de todos los controles de Prowler (aprobados y no aprobados) por gravedad
- `ProwlerReport.html`: archivo HTML único con todas las imágenes incluidas

- prowler3-report-template.xlsm: utilice esta plantilla de Excel para procesar las conclusiones de Prowler. Las tablas dinámicas del informe proporcionan funciones de búsqueda, gráficos y resultados consolidados.

Epics

Preparación para la implementación

Tarea	Descripción	Habilidades requeridas
Clone el repositorio de código.	1. En una interfaz de la línea de comandos, cambie el directorio de trabajo a la ubicación en la que desee almacenar los archivos de muestra. 2. Escriba el siguiente comando: `git clone https://github.com/aws-samples/multi-account-security-assessment-via-prowler.git`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Revise las plantillas.	1. En el repositorio clonado, abra los archivos Prowler-Resources.yaml e IAM-Role.yaml. ProwlerExec 2. Revise los recursos creados por estas plantilla s y ajuste las plantilla s según sea necesario para su entorno. Para obtener más información, consulta Cómo trabajar con CloudFormation plantillas en la documentación. 3. Guarde y cierre los archivos Prowler-Resources.yaml e IAM- Role.yaml. ProwlerEx ec	AWS DevOps

Crea las CloudFormation pilas

Tarea	Descripción	Habilidades requeridas
Aprovisione recursos en la cuenta de seguridad.	Con la plantilla prowler-r esources.yaml, se crea una CloudFormation pila que despliega todos los recursos necesarios en la cuenta de seguridad. Para obtener instrucciones, consulta Cómo crear una pila en la documentación. CloudForm ation Tenga en cuenta lo siguiente al implementar esta plantilla:	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	1. En la página Especificar plantilla, seleccione Plantilla lista y, a continuación, cargue el archivo prowler-resources.yaml. 2. En la página Especificar detalles de pila, en Nombre de la pila, introduzca `Prowler-Resources`. 3. En la sección Parámetros, introduzca lo siguiente: • `VPCId`: seleccione una VPC en la cuenta. • `SubnetId`: seleccione una subred privada que tenga acceso a Internet. Nota: Si selecciona una subred pública, a la instancia EC2 no se le asignará una dirección IP pública porque la CloudFormation plantilla, de forma predeterminada, no aprovisiona ni adjunta una dirección IP elástica. • `InstanceType`: seleccione un tamaño de instancia en función del número de evaluaciones paralelas: • Para 10, elija `r6i.large`.	

Tarea	Descripción	Habilidades requeridas
	• Para 12, elija `r6i.xlarge` . • Para 14 a 18 años, elija `r6i.2xlarge` . • `InstanceImageId` : deje el valor predeterminado para Amazon Linux. • `KeyPairName` : si utiliza SSH para acceder, especifique el nombre de un par de claves existente. • `PermittedSSHInbound` : si utiliza SSH para el acceso, especifique un bloque CIDR permitido. Si no utiliza SSH, mantenga el valor predeterminado de `127.0.0.1` . • `BucketName` : El valor predeterminado es `prowler-output-<accountID>-<region>` . Puede modificarlo según sea necesario. Si especifica un valor personalizado, el ID de cuenta y la región se añaden automáticamente al valor especificado.	

Tarea	Descripción	Habilidades requeridas
	• `EmailAddress` : especifique una dirección de correo electrónico para una notificación de Amazon SNS cuando Prowler complete la evaluación y cargue el archivo .zip en el bucket de S3. Nota: La configuración de la suscripción a SNS debe confirmarse antes de que Prowler complete la evaluación o no se enviará ninguna notificac ión. • `IAMProwlerEC2Role` -: mantenga el nombre predeterminado a menos que sus convenciones de nomenclatura requieran un nombre diferente para este rol de IAM. • `IAMProwlerExecRole` — Mantenga el valor predeterminado a menos que se utilice otro nombre al implementar el archivo IAM-Role.yaml. ProwlerExec • `Parallelism` : especifique el número de evaluaciones paralelas	

Tarea	Descripción	Habilidades requeridas
	que se van a realizar. Asegúrese de que el valor del parámetro `InstanceType` admite este número de evaluaciones paralelas. • `FindingOutput` : si desea excluir los resultados de los pases, seleccione `FailOnly`. Esto reduce significativamente el tamaño de la salida y se centra en las comprobaciones que podrían necesitar ser resueltas. Si desea incluir los resultados de las aprobaciones, seleccione `FailAndPass` . 4. En la página de revisión, seleccione Los siguientes recursos requieren capacidades: [AWS::IAM::Role] y, a continuación, elija Create Stack. 5. Una vez que la pila se haya creado correctamente, en la CloudFormation consola, en la pestaña Outputs, copia el `ProwlerEC2Role` Amazon Resource Name (ARN). Este ARN se utiliza más adelante al implement	

Tarea	Descripción	Habilidades requeridas
	ar el archivo IAM-Role. yaml. ProwlerExec	

Tarea	Descripción	Habilidades requeridas
Facilitar el rol de IAM en las cuentas de los miembros.	En la cuenta AWS Organizations de administración o en una cuenta con permisos de administrador delegados CloudFormation, utilice la plantilla ProwlerExecIAM-Role.yaml para crear un conjunto de pilas. CloudFormation El conjunto de pilas implementa el rol de IAM de `ProwlerExecRole` para todas las cuentas de miembros de la organización. Para obtener instrucciones, consulta Cómo crear un conjunto de pilas con permisos administrados por el servicio en la documentación. CloudFormation Tenga en cuenta lo siguiente al implementar esta plantilla: 1. En Preparar plantilla, selecciona La plantilla está lista y, a continuación, carga el archivo IAM-Role.yaml. ProwlerExec 2. En la página Especificar StackSet detalles, asigne un nombre al conjunto de pilas. `IAM-ProwlerExecRole` 3. En la sección Parámetros, introduzca lo siguiente:	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	• `AuthorizedARN` : introduzca el ARN de `ProwlerEC2Role` que copió al crear la pila de `Prowler-Resources` . • `ProwlerExecRoleNam e` : mantenga el valor predeterminado de `ProwlerExecRole` a menos que se haya utilizado otro nombre al implementar el archivo Prowler-Resources.yaml. 4. En Permisos, seleccione Permisos administrados por servicios. 5. En la página Cómo establecer opciones de implementación, en Destinos de implement ación, seleccione Implementación en organización y acepte todos los valores predeterm inados. Nota: Si quiere que las pilas se desplieguen en todas las cuentas de los miembros de forma simultánea, establece el número Máximo de cuentas simultáneas y la Tolerancia a errores en un valor alto, por ejemplo `100`.	

Tarea	Descripción	Habilidades requeridas
	6. En Regiones de despliegue, elija el Región de AWS lugar en el que se despliega la instancia EC2 de Prowler. Como los recursos de IAM son globales y no regionales, se implementa el rol de IAM en todas las regiones activas. 7. En la página de revisión, seleccione Acepto que AWS CloudFormation podría crear recursos de IAM con nombres personalizados y, a continuación, elija Crear. StackSet 8. Supervise la pestaña Instancias de pila (para ver el estado de las cuentas individuales) y la pestaña Operaciones (para ver el estado general) para determinar cuándo se ha completado la implementación.	

Tarea	Descripción	Habilidades requeridas
Facilite el rol de IAM en la cuenta de administración.	Con la plantilla ProwlerExecIAM-Role.yaml, se crea una CloudFormation pila que implementa la función de `ProwlerExecRole` IAM en la cuenta de administración de la organización. El conjunto de pilas que creó anteriormente no implementa el rol de IAM en la cuenta de administración. Para obtener instrucciones, consulta Cómo crear una pila en la documentación. CloudFormation Tenga en cuenta lo siguiente al implementar esta plantilla: 1. En la página Especificar plantilla, elija La plantilla está lista y, a continuación, cargue el archivo ProwlerExecIAM-Role.yaml. 2. En la página Especificar detalles de pila, en Nombre de la pila, introduzca `IAM-ProwlerExecRole` . 3. En la sección Parámetros, introduzca lo siguiente: • `AuthorizedARN` : introduzca el ARN de `ProwlerEC2Role` que copió al crear la pila de `Prowler-Resources` .	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	• `ProwlerExecRoleNam e` : mantenga el valor predeterminado de `ProwlerExecRole` a menos que se haya utilizado otro nombre al implementar el archivo Prowler-Resources.yaml. 4. En la página de revisión, seleccione Los siguiente s recursos requieren capacidades: [AWS::IAM ::Role] y, a continuación, elija Crear pila.	

Realice la evaluación de seguridad de Prowler

Tarea	Descripción	Habilidades requeridas
Ejecute el escaneo.	1. Inicie sesión en la cuenta de seguridad de la organización. 2. Con el administrador de sesiones, conéctese a la instancia EC2 de Prowler que aprovisionó anteriorm ente. Para obtener instrucci ones, consulte Conexión a la instancia de Linux mediante Session Manager. Si no puede conectars e, consulte la sección de solución de problemas de este patrón.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	3. Navegue hasta `usr/local/prowler` , y luego abra el archivo prowler_scan.sh. 4. Revise y modifique los parámetros y variables ajustables de este script según sea necesario para su entorno. Para obtener más informaci ón sobre las opciones de personalización, consulte los comentarios al principio del script. Por ejemplo, en lugar de obtener una lista de todas las cuentas de los miembros de la organizac ión a partir de la cuenta de administración, puede modificar el script para especificar Cuenta de AWS los ID Regiones de AWS que desea escanear, o puede hacer referencia a un archivo externo que contenga estos parámetros. 5. Guarde y cierre el archivo prowler_scan.sh. 6. Introduzca los comandos siguientes. Esto ejecuta el script prowler_scan.sh. `sudo -i` `screen`	

Tarea	Descripción	Habilidades requeridas
	`cd /usr/local/prowler` `./prowler_scan.sh` Tenga en cuenta lo siguiente: • El comando screen permite que el script continúe ejecutándose en caso de que se agote el tiempo de espera de la conexión o se pierda el acceso a la consola. • Cuando comience el escaneo, puede forzar la separación de la pantalla pulsando Ctrl +A D. La pantalla se separa y puede cerrar la conexión de la instancia y permitir que la evaluación continúe. • Para reanudar una sesión separada, conéctese a la instancia, introduzca `sudo -i` y, a continuación, introduzca `screen -r`. • Para supervisar el progreso de las evaluaciones de las cuentas individuales, puede navegar hasta el directorio de `usr/local/`	

Tarea	Descripción	Habilidades requeridas
	`prowler` e introducir el comando `tail -f output/stdout-<account-id>` . 7. Espera a que Prowler complete los escaneos en todas las cuentas. El script evalúa varias cuentas al mismo tiempo. Cuando se complete la evaluación en todas las cuentas, recibirá una notificación si especificó una dirección de correo electrónico al implementar el archivo Prowler-Resources.yaml.	

Tarea	Descripción	Habilidades requeridas
Recupera los resultados de Prowler.	1. Descargue el archivo `prowler-output-<assessDate>.zip` del bucket `prowler-output-<accountID>-<region>` . Para obtener instrucciones, consulte Descargar un objeto en la documentación de Amazon S3. 2. Elimine todos los objetos del bucket, incluido el archivo que ha descargado. Esta es una práctica recomendada para optimizar los costes y garantizar que se puede eliminar la `Prowler-Resources` CloudFormation pila en cualquier momento. Para obtener instrucciones, consulte Eliminar objetos en la documentación de Amazon S3.	AWS general
Detenga la instancia EC2.	Para evitar la facturación mientras la instancia está inactiva, detenga la instancia EC2 que ejecuta Prowler. Para obtener instrucciones, consulte Detener e iniciar las instancias en la documentación de Amazon EC2.	AWS DevOps

Creación de un informe de los resultados

Tarea	Descripción	Habilidades requeridas
Importe los resultados.	1. En Excel, abra el archivo prowler-report-template.xlsx y, a continuación, seleccione la hoja de trabajo CSV de Prowler. 2. Elimine todos los datos de la muestra, incluida la fila del encabezado. Si se le pregunta si desea eliminar la consulta asociada a los datos que se van a eliminar, elija No. La eliminación de la consulta puede afectar a la funcionalidad de las tablas dinámicas de la plantilla de Excel. 3. Extraiga el contenido del archivo .zip que ha descargado del bucket de S3. 4. En Excel, abra el archivo prowler-fullorgresults-accessdeniedfiltered.txt. Le recomendamos que utilice este archivo porque ya se han eliminado los errores más comunes y no procesables, como los `Access Denied` errores relacionados con los intentos de escaneo de AWS Control Tower	AWS general

Tarea	Descripción	Habilidades requeridas
	recursos. Si desea obtener los resultados sin filtrar, abra en su lugar el archivo prowler-fullorgresults.txt. 5. Seleccione la columna A. 6. Si usas Windows, escriba Ctrl+C, o si usa macOS, escriba Cmd+C. Esto copia todos los datos al portapapeles. 7. En la plantilla de informe de Excel, en la hoja de trabajo CSV de Prowler, seleccione la celda A1. 8. Si usas Windows, escriba Ctrl+V, o si usa macOS, escriba Cmd+V. De este modo, se pegan los resultados en el informe. 9. Confirme que estén seleccionadas todas las celdas que contienen los datos pegados. Si no es así, seleccione la columna A. 10. En la pestaña Datos, seleccione Texto a columnas. 11. En el panel, haga lo siguiente: • Para el paso 1, seleccion e Delimitado.	

Tarea	Descripción	Habilidades requeridas
	• En el paso 2, para Delimitadores, elija punto y coma. En el panel Vista previa de datos, confirme que los datos se están separando en columnas. • Para el paso 3, elija Finalizar. 12. Confirme que los datos de texto estén delimitados en varias columnas. 13. Guarde el informe de Excel con un nuevo nombre. 14. Busque y elimine cualquier error `Access Denied` en los resultados. Para obtener instrucciones sobre cómo eliminarlos mediante programación, consulte Eliminar errores mediante programación en la sección Información adicional.	

Tarea	Descripción	Habilidades requeridas
Finalice el informe.	1. Elija la hoja de trabajo Resultados y, a continuación, seleccione la celda A17. Esta celda es el encabezado de la tabla dinámica. 2. En la cinta, en PivotTable Herramientas, elija Analizar y, a continuación, en Actualizar, elija Actualizar todo. Esto actualiza las tablas dinámicas con el nuevo conjunto de datos. 3. De forma predeterminada, Excel no muestra Cuenta de AWS los números correctamente. Para corregir el formato de los números, haga lo siguiente: • En la hoja de trabajo de Resultados, abra el menú contextual (haga clic con el botón derecho) de la columna A y, a continuación, elija Formatear celdas. • Elija Número y, en decimales, introduzca `0`. • Seleccione Ok. Nota: Si un Cuenta de AWS número comienza con uno o más ceros, Excel los elimina automáticamente.	AWS general

Tarea	Descripción	Habilidades requeridas
	Si ve un número de cuenta que tiene menos de 12 dígitos en el informe, los dígitos que faltan son ceros al principio del número. 4. (Opcional) Puede contraer los campos para facilitar la lectura de los resultados. Haga lo siguiente: • En la hoja de trabajo Resultados, si mueve el cursor a la línea entre las filas 18 y 19 (el espacio entre el encabezad o crítico y el primer hallazgo), el icono del cursor cambia a una pequeña flecha que apunta hacia abajo. • Haga clic para seleccion er todos los campos de búsqueda. • Abra el menú contextua l (haga clic con el botón derecho), busque Expandir/Contraer y, a continuación, elija Contraer. 5. Para obtener más informaci ón sobre la evaluació n, consulte las hojas de trabajo sobre los Resultados, la Gravedad	

Tarea	Descripción	Habilidades requeridas
	y la Aprobación de la evaluación. 6. En el archivo zip de la carpeta `Results-Visualizaton-<date-of-scan>` , revise los gráficos y tablas que se generan automáticamente y que puede utilizar para mejorar sus informes con visualizaciones.	

(Opcional) Actualizar Prowler o los recursos del repositorio de código

Tarea	Descripción	Habilidades requeridas
Actualice Prowler.	Si desea actualizar Prowler a la versión más reciente, haga lo siguiente: 1. Conéctese a la instancia de EC2 de Prowler mediante el Administrador de sesiones. Para obtener instrucciones, consulte Conexión a la instancia de Linux mediante Session Manager. 2. Introduzca el siguiente comando. `sudo -i` `pip3 install --upgrade prowler`	AWS general

Tarea	Descripción	Habilidades requeridas
Actualice el script prowler_scan.sh.	Si quiere actualizar el script prowler_scan.sh a la última versión del repositorio, haga lo siguiente: 1. Conéctese a la instancia de EC2 de Prowler mediante el Administrador de sesiones. Para obtener instrucciones, consulte Conexión a la instancia de Linux mediante Session Manager. 2. Introduzca el siguiente comando. `sudo -i` 3. Desplácese hasta el directorio de scripts de Prowler. `cd /usr/local/prowler` 4. Introduzca el siguiente comando para guardar el script local de forma que pueda combinar los cambios personalizados en la versión más reciente. `git stash` 5. Introduzca el siguiente comando para obtener la	AWS general

Tarea	Descripción	Habilidades requeridas
	versión más reciente del script. `git pull` 6. Introduzca el siguiente comando para combinar el script personalizado con la versión más reciente del script. `git stash pop` Nota: Es posible que recibas advertencias relacionadas con cualquier archivo generado localmente que no esté en el GitHub repositorio, como la búsqueda de informes. Puede ignorarlos siempre que el archivo prowler_scan.sh muestre que los cambios guardados localmente se han vuelto a combinar.	

(Opcional) Limpieza

Tarea	Descripción	Habilidades requeridas
Elimine todos los recursos implementados.	Puede dejar los recursos implementados en las cuentas. Si cierra la instancia EC2 cuando no está en uso y deja el bucket de S3 vacío,	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	se reducen los costos de mantenimiento de los recursos para futuros escaneos. Si desea desaprovisionar todos los recursos, haga lo siguiente: 1. Elimine la pila `IAM-ProwlerExecRole` aprovisionada en la cuenta de administración. Para obtener instrucciones, consulta Eliminar una pila en la CloudFormation documentación. 2. Elimine el conjunto de pilas `IAM-ProwlerExecRole` aprovisionado en la cuenta de administración de la organización o en la cuenta de administrador delegado. Para obtener instrucciones, consulte Eliminar un conjunto de pilas en la CloudFormation documentación. 3. Elimine todos los objetos del bucket de S3 `prowler-output` . Para obtener instrucciones, consulte Eliminar objetos en la documentación de Amazon S3.	

Tarea	Descripción	Habilidades requeridas
	4. Elimine la pila `Prowler-Resources` aprovisionada en la cuenta de seguridad. Para obtener instrucciones, consulte Eliminar una pila en la CloudFormation documentación.	

Resolución de problemas

Problema	Solución
No se puede conectar a la instancia de EC2 mediante Session Manager.	El agente SSM debe poder comunicarse con el punto de conexión de Systems Manager. Haga lo siguiente: 1. Valide que la subred en la que se implement a la instancia EC2 tenga acceso a Internet. 2. Reinicie la instancia EC2.
Al implementar el conjunto de pilas, la CloudFormation consola le solicitará que lo haga`Enable trusted access with AWS Organizations to use service-managed permissions` .	Esto indica que no se ha habilitado el acceso de confianza entre AWS Organizations y CloudFormation. Se requiere acceso de confianza para implementar el conjunto de pilas gestionado por servicios. Seleccione el botón para activar el acceso de confianza. Para obtener más información, consulte Habilitar el acceso confiable en la CloudFormation documentación.

Recursos relacionados

AWS documentación

- Implementación de controles de seguridad en AWS (Guía AWS prescriptiva)

Otros recursos

- Merodeador () GitHub

Información adicional

Eliminar errores mediante programación

Si los resultados contienen errores de `Access Denied`, debe eliminarlos de los resultados. Por lo general, estos errores se deben a una influencia externa en los permisos que impiden que Prowler evalúe un recurso en particular. Por ejemplo, algunas comprobaciones fallan al revisar los depósitos de S3 aprovisionados a través de ellos. AWS Control Tower Puede extraer estos resultados mediante programación y guardar los resultados filtrados como un archivo nuevo.

Los siguientes comandos eliminan las filas que contienen una sola cadena de texto (un patrón) y, a continuación, envían los resultados a un archivo nuevo.

- Para Linux o macOS (Grep)

```
grep -v -i "Access Denied getting bucket" myoutput.csv > myoutput_modified.csv
```

- Para Windows () PowerShell

```
Select-String -Path myoutput.csv -Pattern 'Access Denied getting bucket' -NotMatch >
 myoutput_modified.csv
```

Los siguientes comandos eliminan las filas que coinciden con más de una cadena de texto y, a continuación, envían los resultados a un archivo nuevo.

- Para Linux o macOS (utiliza un tubo de escape entre las cadenas)

```
grep -v -i 'Access Denied getting bucket\|Access Denied Trying to Get' myoutput.csv >
 myoutput_modified.csv
```

- Para Windows (usa una coma entre las cadenas)

```
Select-String -Path myoutput.csv -Pattern 'Access Denied getting bucket', 'Access
 Denied Trying to Get' -NotMatch > myoutput_modified.csv
```

Ejemplos de informes

La siguiente imagen es un ejemplo de la hoja de trabajo sobre los resultados del informe sobre los resultados consolidados de Prowler.

La siguiente imagen es un ejemplo de la hoja de trabajo Pasar Fallar del informe sobre los resultados consolidados de Prowler. (De forma predeterminada, los resultados de las aprobaciones se excluyen de la salida).

La siguiente imagen es un ejemplo de la hoja de trabajo sobre la Gravedad del informe sobre los resultados consolidados de Prowler.

Eliminar volúmenes de Amazon Elastic Block Store (Amazon EBS) no utilizados con AWS Config y AWS Systems Manager

Documento creado por Sankar Sangubotla (AWS)

Entorno: PoC o piloto	Tecnologías: seguridad, identidad y cumplimiento; administración y gobierno; administración de costos	Servicios de AWS: AWS Config; AWS Systems Manager

Resumen

El ciclo de vida de un volumen de Amazon Elastic Block Store (Amazon EBS) suele ser independiente del ciclo de vida de la instancia de Amazon Elastic Compute Cloud (Amazon EC2) a la que está conectado. A menos que seleccione la opción Delete on Termination (Eliminar al finalizar) en el momento del lanzamiento, cuando finaliza la instancia de EC2 se desconecta el volumen de EBS pero no lo elimina. Especialmente en los entornos de desarrollo y pruebas, en los que es habitual lanzar y finalizar instancias de EC2, esto puede provocar una gran cantidad de volúmenes de EBS sin utilizar. Los volúmenes de EBS acumulan cargos en la cuenta de Amazon Web Services (AWS), independientemente de si se utilizan o no. Eliminar estos volúmenes puede ayudar a optimizar los costos de las cuentas de AWS. Además, eliminar los volúmenes de EBS no utilizados es una práctica recomendada de seguridad para evitar el acceso a los datos no utilizados y potencialmente confidenciales de esos volúmenes.

AWS Config puede ayudar a corregir de forma manual o automática los recursos no conformes. Este patrón describe cómo configurar una regla de AWS Config y una acción correctora automática que elimine los volúmenes de Amazon EBS no utilizados de la cuenta. La acción correctora es un manual de procedimientos predefinido para la automatización, una función de AWS Systems Manager. Puede configurar el manual de procedimientos para crear una instantánea del volumen antes de eliminarlo.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.

- AWS Identity and Access Management (IAM) permite ejecutar el manual de procedimientos `AWSConfigRemediation-DeleteUnusedEBSVolume` de AWS Automation, una funcionalidad de AWS Systems Manager. Para obtener más información, consulte Permisos de IAM necesarios en AWSConfigRemediation- DeleteUnused EBSVolume.
- Uno o más volúmenes de Amazon EBS sin utilizar.

Limitaciones

- Los volúmenes de Amazon EBS no utilizados deben estar en el estado `available`.

Arquitectura

Pila de tecnología

- AWS Config
- Amazon EBS
- Systems Manager
- Automatización de Systems Manager

Arquitectura de destino

1. La regla AWS Config evalúa los volúmenes de EBS.
2. La regla devuelve una lista de recursos conformes y no conformes. Se determina que los volúmenes de EBS que se encuentran en el estado `available`, que son volúmenes no utilizados, son no conformes.
3. AWS Config inicia automáticamente el manual de procedimientos de automatización.
4. Si está configurado, Systems Manager crea instantáneas de los volúmenes no utilizados antes de eliminarlos.
5. Systems Manager elimina los volúmenes de EBS no utilizados.

Automatizar y escalar

Puede aplicar esta solución en todas las cuentas de su organización. Para obtener más información, consulte Managing rules across all accounts in your organization (Administrar las reglas de todas las cuentas de la organización) en la documentación de AWS Config.

Herramientas

- AWS Config brinda una visión detallada de la configuración de los recursos de AWS y de cómo están configurados. Ayuda a identificar cómo se relacionan los recursos entre sí y cómo han cambiado sus configuraciones a lo largo del tiempo.
- AWS Systems Manager le permite administrar las aplicaciones y la infraestructura que se ejecutan en la nube de AWS. Systems Manager simplifica la administración de aplicaciones y recursos, reduce el tiempo requerido para detectar y resolver problemas operativos y ayuda a utilizar y administrar los recursos a gran escala.
- Automatización de AWS Systems Manager simplifica las tareas habituales de mantenimiento, implementación y corrección de muchos servicios de AWS.

Epics

Configurar la regla de AWS Config

Tarea	Descripción	Habilidades requeridas
Cree un rol para el manual de procedimientos de automatización.	Cree un rol denominado `AssumeRole` . Systems Manager Automation utiliza este rol para ejecutar el manual de procedimientos. Para obtener instrucciones, consulte Configuring a service role (assume role) access for automations (Configurar el acceso de un rol de servicio [rol de asunción] para automatizaciones) en la documentación de Systems Manager.	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
Active la grabadora AWS Config.	Siga las instrucciones de Setting Up AWS Config with the Console (Configurar AWS Config con la consola) en la documentación de AWS Config para asegurarse de que AWS Config se esté ejecutando y de que esté configurado para registrar los volúmenes de Amazon EBS.	Administrador de sistemas de AWS
Ejecute la regla.	1. Siga las instrucciones de Evaluating your resources (Evaluar los recursos) en la documentación de AWS Config para ejecutar la regla `ec2-volume-inuse-check` . Espere a que finalice la evaluación. 2. En la página Rules (Reglas), seleccione la regla `ec2-volume-inuse-check` y, a continuación, en Resources in scope (Recursos incluidos en el ámbito de aplicación), seleccione Noncompliant (No conformes). 3. Confirme que haya uno o más volúmenes de Amazon EBS sin utilizar en los resultados de la evaluación.	Administrador de sistemas de AWS

Configure la corrección automática de los volúmenes de Amazon EBS no utilizados

Tarea	Descripción	Habilidades requeridas
Agregue la acción correctora automática.	1. En la página Rules (Reglas), seleccione la regla `ec2-volume-inuse-check` . 2. Siga las instrucciones de Setting up automatic remediation (Configurar la corrección automática) en la documentación de AWS Config. Tenga en cuenta lo siguiente: 3. En la sección Remediation action details (Detalles de la acción correctora), seleccione `AWSConfigRemediation-DeleteUnusedEBSVolume` . • Seleccione el parámetro ID de recurso y, a continuación, en la lista, elija. VolumeId En tiempo de ejecución, este parámetro se sustituye por el ID del volumen de EBS no compatible. • En la sección Parameters, proporcione valores para los parámetros siguientes: • `CreateSnapshot` : (Opcional) Si se establece en `true`, la	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	automatización crea una instantánea del volumen de EBS antes de eliminarlo. • `AutomationAssumeRole` : Especifique el nombre de recurso de Amazon (ARN) del rol de servicio `AssumeRole` que creó anteriormente.	
Pruebe la corrección automática para la regla de AWS Config.	1. En la consola de AWS Config, en la página Rules (Reglas), seleccione la regla `ec2-volume-inuse-check` . 2. En el menú Actions (Acciones), seleccione Re-evaluate (Volver a evaluar). 3. Permita que la regla evalúe los recursos no conformes y, a continuación, confirme que se eliminen los volúmenes de Amazon EBS no utilizados.	Administrador de sistemas de AWS

Solución de problemas

Problema	Solución
AWS Config no refleja con precisión el estado de los recursos.	A veces, AWS Config no actualiza el estado de los recursos. Apague la grabadora y vuelva

Problema	Solución
	a encenderla en la página Settings de AWS Config. La grabadora captura el estado de los recursos. En el caso de recursos creados o eliminados recientemente, es posible que la grabadora tarde algún tiempo en reflejar el estado actual. Para obtener más informaci ón sobre los estados del volumen de EBS, consulte Volume state en la documentación de Amazon EC2.

Recursos relacionados

- AWSConfigRemediation- Libro de ejecución de DeleteUnused EBS Volume
- regla ec-2 volume-inuse-check
- Remediating noncompliant AWS resources with AWS Config rules (Corregir recursos de AWS no conformes con reglas de AWS Config)

Implemente y gestione los controles de la Torre de Control de AWS mediante AWS CDK y AWS CloudFormation

Creado por Iker Reina Fuente (AWS) e Ivan Girardi (AWS)

Repositorio de código: -cdk aws-control-tower-controls	Entorno: producción	Tecnologías: seguridad, identidad, conformidad; nativo en la nube; infraestructura; administración y gobernanza
Servicios de AWS: AWS CloudFormation; Torre de Control de AWS; AWS Organizations; AWS CDK		

Resumen

Este patrón describe cómo usar AWS CloudFormation y el AWS Cloud Development Kit (AWS CDK) para implementar y administrar controles preventivos, detectivescos y proactivos de la Torre de Control de AWS como infraestructura como código (IaC). Un control (también conocido como barrera de protección) es una regla de alto nivel que proporciona gobernanza continua para su entorno general de AWS Control Tower. Por ejemplo, puede usar controles para exigir registrarse en sus cuentas de AWS y, a continuación, configurar notificaciones automáticas si se producen eventos específicos relacionados con la seguridad.

AWS Control Tower ayuda a implementar controles preventivos, de detección y proactivos que regulen sus recursos de AWS y supervisen el cumplimiento en varias cuentas de AWS. Cada control aplica una única regla. En este patrón, debe utilizar la plantilla de IaC proporcionada para especificar qué controles desea implementar en su entorno.

Los controles de AWS Control Tower se aplican a toda una unidad organizativa (OU), y el control afecta a todas las cuentas de AWS de la OU. Por lo tanto, cuando los usuarios realicen cualquier acción en cualquier cuenta de su zona de aterrizaje, la acción queda sujeta a los controles que rigen la OU.

La implementación de los controles de AWS Control Tower ayuda a establecer una base de seguridad sólida para su AWS landing zone. Al usar este patrón para implementar los controles como IaC o AWS CDK, puede estandarizar los controles en su landing zone CloudFormation e implementarlos y administrarlos de manera más eficiente. Esta solución utiliza cdk_nag para analizar la aplicación AWS CDK durante la implementación. Esta herramienta comprueba si la aplicación cumple con las prácticas recomendadas de AWS.

Para implementar los controles de la Torre de Control de AWS como iAC, también puede usar HashiCorp Terraform en lugar de AWS CDK. Para obtener más información, consulte Implementación y administración de los controles de AWS Control Tower mediante Terraform.

Público objetivo

Este patrón se recomienda para los usuarios que tengan experiencia con AWS Control Tower CloudFormation, AWS CDK y AWS Organizations.

Requisitos previos y limitaciones

Requisitos previos

- Cuentas de AWS activas administradas como una organización en AWS Organizations y en una zona de aterrizaje de AWS Control Tower. Para obtener instrucciones, consulte Crear una estructura de cuentas (AWS Well-Architected Labs).
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada.
- Administrador de paquetes de nodos (npm), instalado y configurado para AWS CDK.
- Requisitos previos para AWS CDK.
- Permisos para asumir un rol existente de AWS Identity and Access Management (IAM) en una cuenta de implementación.
- Permisos para asumir un rol de IAM en la cuenta de administración de la organización que se pueden utilizar para iniciar AWS CDK. El rol debe tener permisos para modificar e implementar CloudFormation los recursos. Para obtener más información, consulte Proceso de arranque en la documentación de AWS CDK.
- Permisos para crear roles y políticas de IAM en la cuenta de administración de la organización. Para obtener más información, consulte Permisos necesarios para acceder a los recursos de IAM en la documentación de IAM.
- Aplique el control basado en la política de control de servicio (SCP) con el identificador CT.CLOUDFORMATION.PR.1. Este SCP debe estar activado para implementar controles

proactivos. Para obtener instrucciones, consulte No permitir la administración de tipos de recursos, módulos y enlaces en el CloudFormation registro de AWS.

Limitaciones

- Este patrón proporciona instrucciones para implementar esta solución en todas las cuentas de AWS, desde una cuenta de implementación hasta la cuenta de administración de la organización. Para realizar pruebas, puede implementar esta solución directamente en la cuenta de administración, pero las instrucciones para esta configuración no se proporcionan de forma explícita.

Versiones de producto

- Python, versión 3.9 o posterior
- npm versión 8.9.0 o posterior

Arquitectura

Arquitectura de destino

En esta sección se ofrece información general sobre esta solución y la arquitectura establecida en el código de ejemplo. El siguiente diagrama muestra los controles implementados en las distintas cuentas de la OU.

Los controles de AWS Control Tower se clasifican según su comportamiento y sus directrices.

Existen tres tipos principales de comportamientos de control:

1. Los controles preventivos están diseñados para evitar que se produzcan acciones. Se implementan con políticas de control de servicio (SCP) en AWS Organizations. El estado de una medida de seguridad preventiva es uno de los siguientes: aplicado o no habilitado. Las medidas de seguridad preventivas se admiten en todas las regiones de AWS.
2. Los controles de Detective están diseñados para detectar eventos específicos cuando se producen y registrar la acción CloudTrail. Se implementan con las reglas AWS Config. El estado de una medida de seguridad de detección es uno de los siguientes: limpio, infraccióno no

habilitado. Los controles de detección solo se aplican en las regiones de AWS compatibles con AWS Control Tower.

3. Los controles proactivos analizan los recursos que AWS aprovisionaría CloudFormation y comprueban si cumplen con las políticas y los objetivos de su empresa. Los recursos que no sean conformes no se aprovisionarán. Se implementan con los CloudFormation ganchos de AWS. El estado de un control proactivo es PASS, FAIL o SKIP.

Las directrices de los controles se refieren a la práctica recomendada relativa a cómo aplicar cada control a las unidades organizativas. AWS Control Tower ofrece tres categorías de directrices: obligatorias, altamente recomendadas y opcionales. La directriz de un control es independiente de su comportamiento. Para obtener más información, consulte Directrices y comportamiento de control.

Herramientas

Servicios de AWS

- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura de la nube de AWS en código. El kit de herramientas de AWS CDK es la herramienta principal para interactuar con la aplicación de AWS CDK.
- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- AWS Config proporciona una visión detallada de los recursos de su cuenta de AWS y de cómo están configurados. Le ayuda a identificar cómo se relacionan los recursos entre sí y cómo han cambiado sus configuraciones a lo largo del tiempo.
- AWS Control Tower le ayuda a configurar y regular un entorno de cuentas múltiples de AWS siguiendo las prácticas recomendadas prescriptivas.
- AWS Organizations es un servicio de administración de cuentas que le permite agrupar varias cuentas de AWS en una organización que usted crea y administra de manera centralizada.

Otras herramientas

- cdk_nag es una herramienta de código abierto que utiliza una combinación de paquetes de reglas para comprobar si las aplicaciones del AWS Cloud Development Kit (AWS CDK) cumplen las prácticas recomendadas.
- npm es un registro de software que se ejecuta en un entorno Node.js y se utiliza para compartir o tomar prestados paquetes y administrar la implementación de paquetes privados.

- Python es un lenguaje de programación informático de uso general.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub Implementar controles de la Torre de Control de AWS mediante AWS CDK. El archivo cdk.json se utiliza para interactuar con la aplicación AWS CDK y el archivo package.json se utiliza para instalar los paquetes npm.

Prácticas recomendadas

- Siga el principio del privilegio mínimo (documentación de IAM). Los ejemplos de política de IAM y de política de confianza proporcionados en este patrón incluyen los permisos mínimos necesarios, y las pilas de AWS CDK creadas en la cuenta de administración están restringidas por estos permisos.
- Siga las Prácticas recomendadas para los administradores de AWS Control Tower (documentación de AWS Control Tower).
- Siga las Prácticas recomendadas para desarrollar e implementar una infraestructura de nube con AWS CDK (documentación de AWS CDK).
- Al iniciar la AWS CDK, personalice la plantilla de arranque para que defina las políticas y las cuentas de confianza que deben poder leer y escribir en cualquier recurso de la cuenta de administración. Para obtener más información, consulte Personalización del proceso de arranque.
- Utilice herramientas de análisis de código, como cfn_nag, para escanear las plantillas generadas. CloudFormation La herramienta cfn-nag busca patrones en las CloudFormation plantillas que puedan indicar que la infraestructura no es segura. También puedes usar cdk-nag para comprobar tus CloudFormation plantillas mediante el módulo cloudformation-include.

Epics

Preparación para habilitar los controles

Tarea	Descripción	Habilidades requeridas
Crear el rol de IAM en la cuenta de administración.	1. Cree una política de IAM en la cuenta de administración con los permisos definidos en la Política de IAM, en	DevOps ingeniero, AWS general

Tarea	Descripción	Habilidades requeridas
	la sección Información adicional. Para obtener más información, consulte Creación de políticas de IAM en la documentación de IAM. Tome nota del nombre de recurso de Amazon (ARN) de la política. A continuación se muestra un ejemplo de ARN. `arn:aws:iam::<MANAGEMENT-ACCOUNT-ID>:policy/<POLICY-NAME>` 2. Cree un rol de IAM en la cuenta de administración, adjunte la política de permisos de IAM que ha creado en el paso anterior y adjunte la política de confianza personalizada de la Política de confianza en la sección Información adicional. Para obtener instrucciones, consulte Creación de un rol mediante políticas de confianza personalizadas en la documentación de IAM. A continuación se muestra un ejemplo de ARN para el nuevo rol.	

Tarea	Descripción	Habilidades requeridas
	`arn:aws:iam::<MANAGEMENT-ACCOUNT-ID>:role/<ROLE-NAME>`	

Tarea	Descripción	Habilidades requeridas
Arrancar el AWS CDK.	1. En la cuenta de administración, asuma un rol que tenga permisos para arrancar el AWS CDK. 2. Introduzca el siguiente comando, reemplazando lo siguiente: • `<MANAGEMENT-ACCOUNT-ID>` es el ID de la cuenta de administración de la organización. • `<AWS-CONTROL-TOWER-REGION>` es la región de AWS en la que se implementa el Control Tower. Para obtener la lista completa de códigos de región, consulte Puntos de conexión regionales en la Referencia general de AWS. • `<DEPLOYMENT-ACCOUNT-ID>` es el ID de la cuenta de implementación. • `<DEPLOYMENT-ROLE-NAME>` es el nombre del rol de IAM que está utilizando en la cuenta de implementación. • `<POLICY-NAME>` es el nombre de la política que	DevOps ingeniero, AWS general, Python

Tarea	Descripción	Habilidades requeridas
	ha creado en la cuenta de administración. `$ npx cdk bootstrap aws://<MANAGEMENT-ACCOUNT-ID>/<AWS-CONTROL-TOWER-REGION> \ --trust arn:aws:iam::<DEPLOYMENT-ACCOUNT-ID>:role/<DEPLOYMENT-ROLE-NAME> \ --cloudformation-execution-policies arn:aws:iam::<MANAGEMENT-ACCOUNT-ID>:policy/<POLICY-NAME>`	
Clonar el repositorio.	En un shell de bash, ingrese el siguiente comando: Esto clona los controles de la Torre de Control de AWS mediante el repositorio CDK de AWS desde GitHub. `git clone https://github.com/aws-samples/aws-control-tower-controls-cdk.git`	DevOps ingeniero, AWS general

Tarea	Descripción	Habilidades requeridas
Editar el archivo de configuración de AWS CDK.	1. En el repositorio clonado, abra el archivo constants.py. 2. En el parámetro `ACCOUNT_ID`, introduzca el ID de su cuenta de administración. 3. En el parámetro `<AWS-CONTROL-TOWER-REGION>`, introduzca la región de AWS en la que se implementa AWS Control Tower. 4. En el parámetro `ROLE_ARN`, introduzca el ARN del rol que ha creado en la cuenta de administración. 5. En la sección `GUARDRAILS_CONFIGURATION`, en el parámetro `Enable-Control`, introduzca los identificadores de API de los controles. Introduzca el identificador entre comillas dobles y separe los diversos identificadores con comas. Cada control tiene un identificador de API único para cada Región en la que está disponible AWS Control Tower. Para buscar el identificador del control, haga lo siguiente:	

Tarea	Descripción	Habilidades requeridas
	a. En las Tablas de metadatos de los controles, localice el control que desee activar. b. En la columna Identificadores de la API de control, por región, localice el identificador de API de la región en la que va a realizar la llamada a la API, por ejemplo `arn:aws:controltower:us-east-1::control/AWS-GR_ENCRYPTED_VOLUMES` . c. Extraiga el identificador de control del identificador regional, por ejemplo `AWS-GR_ENCRYPTED_VOLUMES` . 6. En la sección `GUARDRAILS_CONFIGURATION` , en el parámetro `OrganizationalUnitIds` , introduzca el ID de la unidad organizativa en la que quiere habilitar el control, por ejemplo `ou-1111-11111111` . Introduzca el identificador entre comillas dobles y separe los identificadores	

Tarea	Descripción	Habilidades requeridas
	múltiples con comas. Para obtener más información sobre cómo recuperar los ID de una OU, consulte Visualización de los detalles de una OU. 7. Guarde y cierre el archivo constants.py. Para ver un ejemplo de un archivo constants.py actualizado, consulte la sección Información adicional de este patrón.	

Habilite los controles en la cuenta de administración

Tarea	Descripción	Habilidades requeridas
Asumir el rol de IAM en la cuenta de implementación.	En la cuenta de implementación, asuma el rol de IAM que tiene permisos para implementar las pilas de AWS CDK en la cuenta de administración. Para obtener más información sobre cómo asumir un rol de IAM en la AWS CLI, consulte Uso de un rol de IAM en la AWS CLI.	DevOps ingeniero, AWS general
Activar el entorno.	Si utiliza Linux o MacOS: 1. Especifique el siguiente comando para crear un entorno virtual.	DevOps ingeniero, AWS general

Tarea	Descripción	Habilidades requeridas
	``$ python3 -m venv .venv``` 2. Una vez creado el entorno virtual, introduzca el siguiente comando para activarlo. ```$ source .venv/bin/activate``` Si utiliza Windows: 1. Especifique el siguiente comando para activar un entorno virtual. ```% .venv\Scripts\activate.bat```	
Instalar las dependencias.	Una vez activado el entorno virtual, introduzca el siguiente comando para ejecutar el script install_deps.sh. Este script instala las dependencias requeridas. ```$ ./scripts/install_deps.sh```	DevOps ingeniero, AWS general, Python

Tarea	Descripción	Habilidades requeridas
Implemente la pila.	Introduzca los siguientes comandos para sintetizar e implementar la CloudForm ation pila. `$ npx cdk synth` `$ npx cdk deploy`	DevOps ingeniero, AWS general, Python

Recursos relacionados

Documentación de AWS

- Acerca de los controles (documentación de AWS Control Tower)
- Biblioteca de controles (documentación de AWS Control Tower)
- Comandos del kit de herramientas de AWS CDK (documentación de AWS CDK)
- Implementación y administración de los controles de AWS Control Tower mediante Terraform (Recomendaciones de AWS)

Otros recursos

- Python

Información adicional

Ejemplo de archivo constants.py

El siguiente es un ejemplo de un archivo constants.py.

```
ACCOUNT_ID = 111122223333
AWS_CONTROL_TOWER_REGION = us-east-2
ROLE_ARN = "arn:aws:iam::111122223333:role/CT-Controls-Role"
GUARDRAILS_CONFIGURATION = [
    {
        "Enable-Control": {
            "AWS-GR_ENCRYPTED_VOLUMES",
```

```
            ...
        },
        "OrganizationalUnitIds": ["ou-1111-11111111", "ou-2222-22222222"...],
    },
    {
        "Enable-Control": {
            "AWS-GR_SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED",
            ...
        },
        "OrganizationalUnitIds": ["ou-2222-22222222"...],
    },
]
```

Política de IAM

El siguiente ejemplo de política permite realizar las acciones mínimas necesarias para habilitar o deshabilitar los controles de AWS Control Tower al implementar pilas de AWS CDK desde una cuenta de implementación a la cuenta de administración.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "controltower:EnableControl",
                "controltower:DisableControl",
                "controltower:GetControlOperation",
                "controltower:ListEnabledControls",
                "organizations:AttachPolicy",
                "organizations:CreatePolicy",
                "organizations:DeletePolicy",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DetachPolicy",
                "organizations:ListAccounts",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListChildren",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPoliciesForTarget",
                "organizations:ListRoots",
                "organizations:UpdatePolicy",
```

```
                "ssm:GetParameters"
            ],
            "Resource": "*"
        }
    ]
}
```

Política de confianza

La siguiente política de confianza personalizada permite que un rol de IAM específico en la cuenta de implementación asuma el rol de IAM en la cuenta de administración. Sustituya lo siguiente:

- <DEPLOYMENT-ACCOUNT-ID> es el ID de la cuenta de implementación
- <DEPLOYMENT-ROLE-NAME> es el nombre del rol en la cuenta de implementación que tiene permitido asumir el rol en la cuenta de administración

```
{
    “Version”: “2012-10-17”,
    “Statement”: [
        {
            “Effect”: “Allow”,
            “Principal”: {
                “AWS”: “arn:aws:iam::<DEPLOYMENT-ACCOUNT-ID>:role/<DEPLOYMENT-ROLE-
NAME>”
            },
            “Action”: “sts:AssumeRole”,
            “Condition”: {}
        }
    ]
}
```

Implementación y administración de los controles de AWS Control Tower mediante Terraform

Creado por Iker Reina Fuente (AWS) e Ivan Girardi (AWS)

Repositorio de código: Implemente y gestione los controles de la Torre de Control de AWS mediante Terraform	Entorno: producción	Tecnologías: seguridad, identidad, conformidad; nativo en la nube; infraestructura; administración y gobernanza
Carga de trabajo: código abierto	Servicios de AWS: AWS Organizations; AWS Control Tower	

Resumen

Este patrón describe cómo utilizar los controles de la Torre de Control Tower de AWS, HashiCorp Terraform y la infraestructura como código (IaC) para implementar y administrar controles de seguridad preventivos, de detección y proactivos. Un control (también conocido como barrera de protección) es una regla de alto nivel que proporciona gobernanza continua para su entorno general de AWS Control Tower. Por ejemplo, puede usar controles para exigir registrarse en sus cuentas de AWS y, a continuación, configurar notificaciones automáticas si se producen eventos específicos relacionados con la seguridad.

AWS Control Tower ayuda a implementar controles preventivos, de detección y proactivos que regulen sus recursos de AWS y supervisen el cumplimiento en varias cuentas de AWS. Cada control aplica una única regla. En este patrón, debe utilizar la plantilla de IaC proporcionada para especificar qué controles desea implementar en su entorno.

Los controles de AWS Control Tower se aplican a toda una unidad organizativa (OU), y el control afecta a todas las cuentas de AWS de la OU. Por lo tanto, cuando los usuarios realicen cualquier acción en cualquier cuenta de su zona de aterrizaje, la acción queda sujeta a los controles que rigen la OU.

La implementación de los controles de AWS Control Tower ayuda a establecer una base de seguridad sólida para su AWS landing zone. Al usar este patrón para implementar los controles como IaC a través de Terraform, puede estandarizar los controles en su zona de aterrizaje e implementarlos y administrarlos de manera más eficiente.

Para implementar los controles de AWS Control Tower como IaC, también puede usar AWS Cloud Development Kit (AWS CDK) en lugar de Terraform. Para obtener más información, consulte Implementación y administración de los controles de la Torre de Control de AWS mediante AWS CDK y AWS CloudFormation.

Público objetivo

Este patrón se recomienda para los usuarios que tengan experiencia con AWS Control Tower, Terraform y AWS Organizations.

Requisitos previos y limitaciones

Requisitos previos

- Cuentas de AWS activas administradas como una organización en AWS Organizations y en una zona de aterrizaje de AWS Control Tower. Para obtener instrucciones, consulte Crear una estructura de cuentas (AWS Well-Architected Labs).
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada.
- Un rol de AWS Identity and Access Management (IAM) en la cuenta de administración que tiene permisos para implementar este patrón. Para obtener más información sobre los permisos necesarios y un ejemplo de política, consulte Permisos con privilegios mínimos para el rol de IAM en la sección de Información adicional de este patrón.
- Permisos para asumir el rol de IAM en la cuenta de administración.
- Aplique el control basado en la política de control de servicio (SCP) con el identificador CT.CLOUDFORMATION.PR.1. Este SCP debe estar activado para implementar controles proactivos. Para obtener instrucciones, consulte No permitir la administración de tipos de recursos, módulos y enlaces en el CloudFormation registro de AWS.
- Terraform CLI, instalada (documentación de Terraform).
- Terraform AWS Provider, configurado (documentación de Terraform).
- Backend de Terraform, configurado (documentación de Terraform).

Versiones de producto

- AWS Control Tower versión 3.0 o posterior
- Terraform versión 1.5 o posterior
- Terraform AWS Provider versión 4.67 o posterior

Arquitectura

Arquitectura de destino

En esta sección se ofrece información general sobre esta solución y la arquitectura establecida en el código de ejemplo. El siguiente diagrama muestra los controles implementados en las distintas cuentas de la OU.

Los controles de AWS Control Tower se clasifican según su comportamiento y su orientación.

Existen tres tipos principales de comportamientos de control:

1. Los controles preventivos están diseñados para evitar que se produzcan acciones. Se implementan con políticas de control de servicio (SCP) en AWS Organizations. El estado de una medida de seguridad preventiva es uno de los siguientes: aplicado o no habilitado. Las medidas de seguridad preventivas se admiten en todas las regiones de AWS.
2. Los controles de Detective están diseñados para detectar eventos específicos cuando se producen y registrar la acción CloudTrail. Se implementan con las reglas AWS Config. El estado de una medida de seguridad de detección es uno de los siguientes: limpio, infraccióno no habilitado. Los controles de detección solo se aplican en las regiones de AWS compatibles con AWS Control Tower.
3. Los controles proactivos analizan los recursos que AWS aprovisionaría CloudFormation y comprueban si cumplen con las políticas y los objetivos de su empresa. Los recursos que no sean conformes no se aprovisionarán. Se implementan con los CloudFormation ganchos de AWS. El estado de un control proactivo es PASS, FAIL o SKIP.

Las directrices de los controles se refieren a la práctica recomendada relativa a cómo aplicar cada control a las unidades organizativas. AWS Control Tower ofrece tres categorías de directrices: obligatorias, altamente recomendadas y opcionales. La directriz de un control es independiente de su comportamiento. Para obtener más información, consulte Directrices y comportamiento de control.

Herramientas

Servicios de AWS

- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- AWS Config proporciona una visión detallada de los recursos de su cuenta de AWS y de cómo están configurados. Le ayuda a identificar cómo se relacionan los recursos entre sí y cómo han cambiado sus configuraciones a lo largo del tiempo.
- AWS Control Tower le ayuda a configurar y regular un entorno de cuentas múltiples de AWS siguiendo las prácticas recomendadas prescriptivas.
- AWS Organizations es un servicio de administración de cuentas que le permite agrupar varias cuentas de AWS en una organización que usted crea y administra de manera centralizada.

Otras herramientas

- HashiCorp Terraform es una herramienta de código abierto de infraestructura como código (IaC) que le ayuda a utilizar el código para aprovisionar y gestionar la infraestructura y los recursos de la nube.

Repositorio de código

El código de este patrón está disponible en el repositorio de Terraform para GitHub implementar y administrar los controles de la Torre de Control de AWS.

Prácticas recomendadas

- Los roles de IAM usados para implementar esta solución deben cumplir con el principio de privilegio mínimo (documentación de IAM).
- Siga las prácticas recomendadas para los administradores de AWS Control Tower (documentación de AWS Control Tower).

Epics

Página de administración de cuentas en la consola de

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	En un shell de bash, ingrese el siguiente comando: Esto clona los controles de implementación y administración de la Torre de Control de AWS mediante el repositorio Terraform de GitHub. `git clone https://github.com/aws-samples/aws-control-tower-controls-terraform.git`	DevOps ingeniero
Edite el archivo de configuración del backend de Terraform.	1. En el repositorio clonado, abra el archivo backend.tf. 2. Edite el archivo para establecer la configuración del backend de Terraform. La configuración que defina en este archivo depende de su entorno. Para obtener más información, consulte la sección Configuración del backend (documentación de Terraform). 3. Guarde y cierre el archivo backend.tf.	DevOps ingeniero, Terraform

Tarea	Descripción	Habilidades requeridas
Edite el archivo de configuración del proveedor de Terraform.	1. En el repositorio clonado, abra el archivo provider.tf. 2. Edite el archivo para establecer la configuración del proveedor de Terraform. Para obtener más información, consulte Configuración del proveedor (documentación de Terraform). Defina la región de AWS como la región en la que está disponible la API de AWS Control Tower. 3. Guarde y cierre el archivo provider.tf.	DevOps ingeniero, Terraform

Tarea	Descripción	Habilidades requeridas
Edite el archivo de configuración.	1. En el repositorio clonado, abra el archivo variables.tfvars. 2. En la sección `controls`, en el parámetro `control_names` , introduzca el identificador de la API de control. Cada control tiene un identificador de API único para cada región en la que está disponible AWS Control Tower. Para buscar el identificador del control, haga lo siguiente: a. En las Tablas de metadatos de los controles, localice el control que desee activar. b. En la columna Identificadores de la API de control, por región, localice el identificador de API de la región en la que va a realizar la llamada a la API, por ejemplo `arn:aws:controltower:us-east-1::control/AWS-GR_AUDIT_BUCKET_ENCRYPTION_ENABLED` .	DevOps ingeniero, AWS general, Terraform

Tarea	Descripción	Habilidades requeridas
	c. Extraiga el identificador de control del identificador regional, por ejemplo `AWS-GR_AUDIT_BUCKET_ENCRYPTION_ENABLED` . 3. En la sección `controls`, en el parámetro `organizational_unit_ids` , introduzca el ID de la unidad organizativa en la que quiere habilitar el control, por ejemplo `ou-1111-11111111` . Introduzca el identificador entre comillas dobles y separe los identificadores múltiples con comas. Para obtener más información sobre cómo recuperar los ID de una OU, consulte Visualización de los detalles de una OU. 4. Guarde y cierre el archivo variables.tfvars. Para ver un ejemplo de un archivo variables.tfvars actualizado, consulte la sección de información adicional de este patrón.	

Tarea	Descripción	Habilidades requeridas
Asuma el rol de IAM de la cuenta de administración	En la cuenta de administración, asuma el rol de IAM que tiene permisos para implementar el archivo de configuración de Terraform. Para obtener más información sobre los permisos necesarios y un ejemplo de política, consulte Permisos con privilegios mínimos para el rol de IAM en la sección de Información adicional. Para obtener más información sobre cómo asumir un rol de IAM en AWS CLI, consulte Uso de un rol de IAM en AWS CLI.	DevOps ingeniero, AWS general

Tarea	Descripción	Habilidades requeridas
Implementación del archivo de configuración	1. Ingrese el comando siguiente para inicializar Terraform. `$ terraform init -upgrade` 2. Introduzca el comando siguiente para obtener una vista previa de los cambios en comparación con el estado actual. `$ terraform plan -var-file="variables.tfvars"` 3. Revise los cambios de configuración en el plan de Terraform y confirme que desea implementar estos cambios en la organización. 4. Ingrese el comando siguiente para implementar los recursos. `$ terraform apply -var-file="variables.tfvars"`	DevOps ingeniero, AWS general, Terraform

(Opcional) Inhabilite los controles en la cuenta de administración de AWS Control Tower

Tarea	Descripción	Habilidades requeridas
Ejecute el comando de destrucción.	Ingrese el comando siguiente para eliminar los recursos implementados por este patrón. `$ terraform destroy -var-file="variables.tfvars"`	DevOps ingeniero, AWS general, Terraform

Solución de problemas

Problema	Solución
Error de `Error: creating ControlTower Control ValidationException: Guardrail <control ID> is already enabled on organizational unit <OU ID>`	El control que intenta activar ya está activado en la unidad organizativa de destino. Este error puede producirse si un usuario habilitó el control manualmente a través de la consola de administración de AWS, a través de AWS Control Tower o a través de AWS Organizations. Para implementar el archivo de configuración de Terraform, puede usar cualquiera de las siguientes opciones. Opción 1: actualizar el archivo de estado actual de Terraform Puede importar el recurso al archivo de estado actual de Terraform. Al volver a ejecutar el comando `apply`, Terraform omitirá este recurso. Haga lo siguiente para importar el recurso al estado actual de Terraform:

Problema	Solución
	1. En la cuenta de administración de AWS Control Tower, introduzca el siguiente comando para recuperar una lista de los nombres de recursos de Amazon (ARN) de las OU, donde `<root-ID>` es la raíz de la organización. Para obtener más informaci ón sobre cómo recuperar este ID, consulte Visualización de los detalles de la raíz. `aws organizations list-orga nizational-units-for-parent -- parent-id <root-ID>` 2. Para cada unidad organizativa devuelta en el paso anterior, introduzca el siguiente comando, donde <OU-ARN> es el ARN de la unidad organizativa. `aws controltower list-enabled-contr ols --target-identifier <OU-ARN>` 3. Copie los ARN y realice la importación de Terraform en el módulo correspon diente para que se incluya en el estado de Terraform. Para obtener instrucciones, consulte Importación (documentación de Terraform). 4. Repita los pasos de Implementar la configuración en la sección Epics.. Opción 2: deshabilitar el control Si trabaja en un entorno que no es de producción, puede deshabilitar el control en la consola. Vuelva a habilitarlo al repetir los pasos de Implementar la configuración en la

Problema	Solución
	sección Epics.. Este enfoque no se recomiend a para entornos de producción porque hay un período de tiempo en el que el control estará deshabilitado. Si desea utilizar esta opción en un entorno de producción, puede implement ar controles temporales, como la aplicación temporal de un SCP en AWS Organizations.

Recursos relacionados

Documentación de AWS

- Acerca de los controles (documentación de AWS Control Tower)
- Acerca de los controles (documentación de AWS Control Tower)
- Implemente y gestione los controles de la Torre de Control de AWS mediante AWS CDK y AWS CloudFormation (AWS Prescriptive Guidance)

Otros recursos

- Terraform
- Documentación de Terraform CLI

Información adicional

Ejemplo de archivo variables.tfvars

A continuación se muestra un ejemplo de un archivo variables.tfvars actualizado.

```
controls = [
    {
        control_names = [
            "AWS-GR_ENCRYPTED_VOLUMES",
            ...
        ],
        organizational_unit_ids = ["ou-1111-11111111", "ou-2222-22222222"...],
```

```
    },
    {
        control_names = [
            "AWS-GR_SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED",
            ...
        ],
        organizational_unit_ids = ["ou-1111-11111111"...],
    },
]
```

Permisos con privilegios mínimos para el rol de IAM

Este patrón de APG requiere que asuma un rol de IAM en la cuenta de administración. La práctica recomendada es asumir un rol con permisos temporales y limitar los permisos según el principio del privilegio mínimo. El siguiente ejemplo de política permite realizar las acciones mínimas necesarias para habilitar o deshabilitar los controles de AWS Control Tower.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "controltower:EnableControl",
                "controltower:DisableControl",
                "controltower:GetControlOperation",
                "controltower:ListEnabledControls",
                "organizations:AttachPolicy",
                "organizations:CreatePolicy",
                "organizations:DeletePolicy",
                "organizations:DescribeOrganization",
                "organizations:DetachPolicy",
                "organizations:ListAccounts",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListChildren",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPoliciesForTarget",
                "organizations:ListRoots",
                "organizations:UpdatePolicy"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

Implemente una canalización que detecte simultáneamente los problemas de seguridad en varios entregables de código

Repositorio de códigos: Pipeline de escaneo de código simple	Entorno: PoC o piloto	Tecnologías: seguridad , identidad, conformidad; DevOps
Servicios de AWS: AWS CloudFormation CodeBuild ; AWS CodeCommit; AWS CodePipeline		

Resumen

La canalización simple de escaneo de código (SCSP) permite crear con dos clics una canalización de análisis de código que ejecuta en paralelo las herramientas de seguridad de código abierto estándares del sector. Esto permite a los desarrolladores comprobar la calidad y la seguridad de su código sin tener que instalar herramientas ni siquiera saber cómo ejecutarlas. Esto le ayuda a reducir las vulnerabilidades y los errores de configuración en los entregables de código. También reduce la cantidad de tiempo que su organización dedica a instalar, investigar y configurar las herramientas de seguridad.

Antes del SCSP, el escaneo de código con este conjunto particular de herramientas requería que los desarrolladores localizaran, instalaran y configuraran manualmente las herramientas de análisis de software. Incluso si se instalan localmente, all-in-one las herramientas, como Automated Security Helper (ASH), requieren configurar un contenedor Docker para poder funcionar. Sin embargo, con SCSP, un conjunto de herramientas de análisis de código estándar del sector se ejecuta automáticamente en el. Nube de AWS Con esta solución, utilizas Git para impulsar las entregas de código y, a continuación, recibes un resultado visual con at-a-glance información sobre los errores en las comprobaciones de seguridad.

Requisitos previos y limitaciones

- Un activo Cuenta de AWS
- Uno o más entregables de código que desee escanear para detectar problemas de seguridad

- AWS Command Line Interface (AWS CLI), instalado y configurado
- Python versión 3.0 o posterior y pip versión 9.0.3 o posterior, instaladas
- Git, instalado
- Instale git-remote-codecommit en su estación de trabajo local

Arquitectura

Pila de tecnología de destino

- AWS CodeCommit repositorio
- AWS CodeBuild proyecto
- AWS CodePipeline oleoducto
- Bucket de Amazon Simple Storage Service (Amazon S3)
- AWS CloudFormation plantilla

Arquitectura de destino

El SCSP para el análisis de código estático es un DevOps proyecto diseñado para proporcionar información de seguridad sobre el código entregable.

1. En el AWS Management Console, inicie sesión en el destino Cuenta de AWS. Confirme que se encuentra en el Región de AWS lugar donde desea implementar la canalización.
2. Utilice la CloudFormation plantilla del repositorio de código para implementar la pila SCSP. Esto crea un CodeCommit repositorio y un CodeBuild proyecto nuevos.

   Nota: Como opción de implementación alternativa, puedes usar una existente CodeCommi t proporcionando el nombre de recurso de Amazon (ARN) del repositorio como parámetro durante el despliegue de la pila.

3. Clone el repositorio en su estación de trabajo local y, a continuación, añada los archivos a sus respectivas carpetas del repositorio clonado.
4. Usa Git para añadir, confirmar y enviar los archivos al CodeCommit repositorio.
5. Al empujarlos al CodeCommit repositorio, se inicia un CodeBuild trabajo. El CodeBuild proyecto utiliza las herramientas de seguridad para escanear los entregables de código.

6. Revise el resultado de la canalización. Las herramientas de seguridad que detecten problemas relacionados con el nivel de error provocarán acciones fallidas en el proceso. Corrija estos errores o elimínelos como falsos positivos. Revisa los detalles del resultado de la herramienta en los detalles de la acción en el bucket S3 de la canalización CodePipeline o en él.

Herramientas

Servicios de AWS

- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y administrarlos a lo largo de su ciclo de vida en todas Cuentas de AWS las regiones.
- AWS CodeBuildes un servicio de compilación totalmente gestionado que le ayuda a compilar código fuente, ejecutar pruebas unitarias y producir artefactos listos para su implementación.
- AWS CodeCommites un servicio de control de versiones que te ayuda a almacenar y gestionar de forma privada los repositorios de Git, sin necesidad de gestionar tu propio sistema de control de código fuente.

Otras herramientas

Para obtener una lista completa de las herramientas que SCSP utiliza para escanear los entregables de código, consulta el léame de SCSP. GitHub

Repositorio de código

El código de este patrón está disponible en el repositorio Simple Code Scanning Pipeline (SCSP) de. GitHub

Epics

Implemente el SCSP

Tarea	Descripción	Habilidades requeridas
Cree la CloudFormation pila.	1. Inicie sesión en la AWS Management Console. 2. En la consola, confirme que se encuentra en la región	AWS DevOps, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	de destino en la que desea implementar la solución. Para obtener más información, consulte Elegir una región. 3. Elija el siguiente enlace. Esto abre el asistente de creación rápida de pilas CloudFormation. https://console.aws.amazon.com/cloudformation/home?#/stacks/create/review?templateURL=https://proservetools.s3.amazonaws.com/cft/scsp-pipeline-stack.template.json&stackName = SimpleCode ScanPipeline 4. En el asistente de creación rápida de pilas, revise la configuración de los parámetros de la pila y realice las modificaciones necesarias según su caso de uso. 5. Seleccione Acepto que AWS CloudFormation podría crear recursos de IAM y, a continuación, elija Create stack. Esto crea un CodeCommit repositorio, una CodePipel	

Tarea	Descripción	Habilidades requeridas
	ine canalización, varias definiciones de CodeBuild trabajos y un bucket de S3. Las compilaciones, las ejecuciones y los resultado s del escaneo se copian en este depósito. Una vez que la CloudFormation pila se haya desplegado por completo, SCSP estará listo para su uso.	

Utilice la canalización

Tarea	Descripción	Habilidades requeridas
Examine los resultados de la gammagrafía.	1. En la consola de Amazon S3, en Buckets, elige la canalización de códigos simple: eliminar recursos pipelinereso bucket. 2. Elija el directorio scan_resu lts y, a continuación, elija la carpeta con la fecha de digitalización más reciente. 3. Revise los archivos de registro de esta carpeta para revisar cualquier problema detectado por las herramientas de seguridad utilizadas en el proceso. Las herramientas de seguridad que detecten problemas de nivel de error darán lugar a `failed`	Desarrollador de aplicaciones, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	acciones en proceso. Si se trata de falsos positivos, es necesario corregirlos o suprimirlos. Nota: También puede ver los detalles del resultado de la herramienta (tanto para los escaneos aprobados como para los que no) en la CodePipeline consola, en la sección Detalles de las acciones.	

Resolución de problemas

Problema	Solución
HashiCorp No se están escaneando Terraform ni sus AWS CloudFormation archivos.	Asegúrese de que los archivos Terraform (.tf) y CloudFormation (.yml, .yaml o .json) estén ubicados en las carpetas correspondientes del repositorio clonado. CodeCommit
El `git clone` comando está fallando.	Asegúrese de haber instalado `git-remote-codecommit` y de que su CLI tenga acceso a AWS las credenciales que tienen permisos para leer el CodeCommit repositorio.
Un error de simultaneidad, como`Project-level concurrent build limit cannot exceed the account-level concurrent build limit of 1 .`	Vuelva a ejecutar la canalización pulsando el botón Release Change de la CodePipeline consola. Se trata de un problema conocido que parece ser más común las primeras veces que se ejecuta la canalización.

Recursos relacionados

Proporcione comentarios sobre el proyecto SCSP.

Información adicional

PREGUNTAS FRECUENTES

¿El proyecto SCSP es igual al de Automated Security Helper (ASH)?

No. Use ASH cuando desee una herramienta CLI que ejecute herramientas de escaneo de código mediante contenedores. El Auxiliar de Seguridad Automatizado (ASH) es una herramienta diseñada para reducir la probabilidad de que se produzca una infracción de seguridad en la nueva configuración de código, infraestructura o recursos de IAM. ASH es una utilidad de línea de comandos que se puede ejecutar localmente. El uso local requiere que un entorno de contenedores esté instalado y operativo en el sistema.

Utilice SCSP cuando desee una canalización de configuración más sencilla que la de ASH. SCSP no requiere instalaciones locales. El SCSP está diseñado para ejecutar comprobaciones de forma individual en una canalización y mostrar los resultados por herramienta. SCSP también evita gran parte de la sobrecarga que supone la configuración de Docker y es independiente del sistema operativo (SO).

¿SCSP es solo para equipos de seguridad?

No, cualquiera puede implementar la canalización para determinar qué partes de su código no superan las comprobaciones de seguridad. Por ejemplo, los usuarios que no son usuarios de seguridad pueden usar SCSP para comprobar su código antes de revisarlo con sus equipos de seguridad.

¿Puedo usar SCSP si estoy trabajando con otro tipo de repositorio, como GitLab GitHub, o Bitbucket?

Puedes configurar un repositorio git local para que apunte a dos repositorios remotos diferentes. Por ejemplo, puedes clonar un GitLab repositorio existente, crear una instancia de SCSP (especificando CloudFormation las carpetas Terraform y AWS Config Rules Development Kit (AWS RDK), si es necesario) y, a continuación, utilizarla `git remote add upstream <SCSPGitLink>` para apuntar también el repositorio local al repositorio de CodeCommit SCSP. Esto permite enviar primero los cambios de código a SCSP, validarlos y, después, tras realizar cualquier actualización adicional para corregir los hallazgos, enviarlos al repositorio o a Bitbucket GitLab. GitHub Para obtener más

información sobre varios controles remotos, consulta Enviar confirmaciones a un repositorio de Git adicional (entrada AWS del blog).

> Nota: Ten cuidado con las desviaciones, por ejemplo, evita realizar cambios a través de las interfaces web.

Contribuye y añade tus propias acciones

La configuración del SCSP se mantiene como un GitHub proyecto, que contiene el código fuente de la aplicación SCSP AWS Cloud Development Kit (AWS CDK) . Para añadir comprobaciones adicionales a la canalización, es necesario actualizar la AWS CDK aplicación y, a continuación, sintetizarla o desplegarla en el destino en el que Cuenta de AWS se ejecutará la canalización. Para ello, comience por clonar el GitHub proyecto SCSP y, a continuación, busque el archivo de definición de la pila en la `lib` carpeta.

Si quieres añadir una marca adicional, la `StandardizedCodeBuildProject` clase del AWS CDK código facilita la adición de acciones. Proporciona el nombre, la descripción `install` o los `build` comandos. AWS CDK crea el CodeBuild proyecto utilizando valores predeterminados razonables. Además de crear el proyecto de construcción, es necesario añadirlo a las CodePipeline acciones de la fase de construcción. Al diseñar una nueva comprobación, la acción debería realizarse `FAIL` si la herramienta de digitalización detecta problemas o no se ejecuta. La acción debería `PASS` realizarse si la herramienta de digitalización no detecta ningún problema. Para ver un ejemplo de configuración de una herramienta, revise el código de la `Bandit` acción.

Para obtener más información sobre las entradas y salidas esperadas, consulte la documentación del repositorio.

Si agrega acciones personalizadas, debe implementar SCSP mediante `cdk deploy` o `cdk synth + CloudFormation deploy`. Esto se debe a que los propietarios del repositorio mantienen la CloudFormation plantilla de pila de creación rápida.

Implemente controles de acceso basados en atributos de detección para subredes públicas mediante AWS Config

Creado por Alberto Menendez (AWS)

Entorno: PoC o piloto	Tecnologías: seguridad, identidad, conformidad; redes	Servicios de AWS: AWS Config; Amazon SNS

Resumen

Las arquitecturas de redes perimetrales distribuidas se basan en la seguridad perimetral de la red que se ejecuta junto con las cargas de trabajo de sus nubes privadas virtuales (VPC). Esto proporciona una escalabilidad sin precedentes en comparación con el enfoque centralizado más común. Si bien la implementación de subredes públicas en las cuentas de carga de trabajo puede ofrecer beneficios, también presenta nuevos riesgos de seguridad porque aumenta la superficie expuesta a ataques. Se recomienda implementar únicamente los recursos de Elastic Load Balancing (ELB), como los equilibradores de carga de aplicaciones o las puertas de enlace NAT, en las subredes públicas de estas VPC. El uso de equilibradores de carga y puertas de enlace NAT en subredes públicas dedicadas le ayuda a implementar un control detallado del tráfico entrante y saliente.

Le recomendamos que implemente controles preventivos y de detección para limitar los tipos de recursos que se pueden implementar en las subredes públicas. Para obtener más información sobre el uso del control de acceso basado en atributos (ABAC) para implementar controles preventivos en las subredes públicas, consulte Implementación de controles de acceso preventivos basados en atributos para las subredes públicas. Si bien son eficaces en la mayoría de las situaciones, es posible que estos controles preventivos no aborden todos los casos de uso posibles. Por lo tanto, este patrón se basa en el enfoque ABAC y le ayuda a configurar alertas sobre los recursos no conformes que se despliegan en las subredes públicas. La solución comprueba si las interfaces de red elásticas pertenecen a un recurso que no está permitido en las subredes públicas.

Para lograrlo, este patrón utiliza las reglas personalizadas de AWS Config y ABAC. La regla personalizada procesa la configuración de una interface de red elástica cada vez que se crea o modifica. En un nivel superior, esta regla realiza dos acciones para determinar si la interfaz de red es compatible:

1. Para determinar si la interfaz de red está dentro del ámbito de aplicación de la regla, la regla comprueba si la subred tiene etiquetas de AWS específicas que indican que es una subred pública. Por ejemplo, esta etiqueta podría ser. `IsPublicFacing=True`
2. Si la interfaz de red se implementa en una subred pública, la regla comprueba qué servicio de AWS creó este recurso. Si el recurso no es un recurso ELB o una puerta de enlace NAT, marca el recurso como no conforme.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- AWS Config, configurado en la cuenta de carga de trabajo
- Permisos para implementar los recursos necesarios en la cuenta de carga de trabajo
- Una VPC con subredes públicas
- Etiquetas aplicadas correctamente para identificar las subredes públicas de destino
- (Opcional) Una organización de AWS Organizations
- (Opcional) Una cuenta de seguridad central que sea la administradora delegada de AWS Config y AWS Security Hub

Arquitectura

Arquitectura de destino

En el siguiente diagrama se ilustra lo siguiente:

1. Cuando se implementa o modifica un recurso de interfaz de red elástica (`AWS::EC2::NetworkInterface`), AWS Config captura el evento y la configuración.
2. AWS Config compara este evento con la regla personalizada utilizada para evaluar la configuración.
3. Se invoca la función AWS Lambda asociada a esta regla personalizada. La función evalúa el recurso y aplica la lógica especificada para determinar si la configuración del recurso es`COMPLIANT`, `NON_COMPLIANT` o. `NOT_APPLICABLE`

4. Si se determina que un recurso existe`NON_COMPLIANT`, AWS Config envía una alerta a través de Amazon Simple Notification Service (Amazon SNS).

> Nota: Si esta cuenta es una cuenta de miembro de AWS Organizations, puede enviar los datos de conformidad a una cuenta de seguridad central a través de AWS Config o AWS Security Hub.

Lógica de evaluación de funciones Lambda

El siguiente diagrama muestra la lógica aplicada por la función Lambda para evaluar la conformidad de la elastic network interface.

Automatizar y escalar

Este patrón es una solución detectivesca. También puede complementarlo con una regla de corrección para resolver automáticamente cualquier recurso que no cumpla con las normas. Para obtener más información, consulte Cómo corregir los recursos no conformes con las reglas de AWS Config.

Puede escalar esta solución de la siguiente manera:

- Exigir la aplicación de las etiquetas de AWS correspondientes que establezca para identificar las subredes públicas. Para obtener más información, consulte las políticas de etiquetas en la documentación de AWS Organizations.
- Configurar una cuenta de seguridad central que aplique la regla personalizada de AWS Config a todas las cuentas de carga de trabajo de la organización. Para obtener más información, consulte Automatizar el cumplimiento de la configuración a escala en AWS (entrada del blog de AWS).
- Integración de AWS Config con AWS Security Hub para capturar, centralizar y notificar a escala. Para obtener más información, consulte Configuración de AWS Config en la documentación de AWS Security Hub.

Herramientas

- AWS Config proporciona una visión detallada de los recursos de su cuenta de AWS y de cómo están configurados. Le ayuda a identificar cómo se relacionan los recursos entre sí y cómo han cambiado sus configuraciones a lo largo del tiempo.
- Elastic Load Balancing (ELB) distribuye el tráfico entrante de aplicaciones o redes entre varios destinos. Así, por ejemplo, puede distribuir el tráfico a través de instancias de Amazon Elastic Compute Cloud (Amazon EC2), contenedores y direcciones IP de una o varias zonas de disponibilidad.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esta red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Prácticas recomendadas

Para obtener más ejemplos y prácticas recomendadas para desarrollar reglas de AWS Config personalizadas, consulte el repositorio oficial de reglas de AWS Config en GitHub.

Epics

Implementar la solución

Tarea	Descripción	Habilidades requeridas
Crear la función de Lambda.	1. Inicie sesión en la consola de administración de AWS y, a continuación, abra la consola de AWS Lambda.	AWS general

Tarea	Descripción	Habilidades requeridas
	2. En la página Functions (Funciones), seleccione Create function (Crear función). 3. Seleccione Crear desde cero. 4. En el panel de información básica, en Nombre de la función, introduzca un nombre. 5. En Tiempo de ejecución, seleccione Python 3.12. 6. Deje la arquitectura establecida en x86_64. 7. Elija Crear función. 8. Elija la pestaña Código. 9. En el explorador de archivos, elija lambda_function.py. 10. Pegue el código de ejemplo que se proporciona en la sección de información adicional de este patrón en la pestaña lambda_function.py. Personalice el código de ejemplo para identificar cualquier lógica de evaluación personalizada de la `evaluate_change_notification_compliance` función. 11. Elija Implementar.	

Tarea	Descripción	Habilidades requeridas
Añada permisos a la función de ejecución de la función Lambda.	1. Seleccione Funciones en el panel de navegación. 2. Elija la función que acaba de crear. 3. Elija Configuration (Configuración) y, a continuación, seleccione Permissions (Permisos). 4. Elija el nombre del rol para abrirlo en la consola de AWS Identity and Access Management (IAM). 5. En Políticas de permisos, elija Agregar permisos y, a continuación, elija Crear política en línea. 6. Elija JSON. 7. Pegue la siguiente política en el editor de políticas. Esto permite a la función Lambda: • Obtenga los detalles de las etiquetas de subred. • Envíe el resultado de la conformidad a AWS Config. `{ "Version": "2012-10-17", "Statement": [ {`	AWS general

Tarea	Descripción	Habilidades requeridas
	<pre>"Action": ["config:PutEvaluations", "ec2:DescribeSubnets"], "Resource": "*", "Effect": "Allow" }] }</pre> 8. Elija Siguiente. 9. Escriba un nombre para la política y elija Create policy (Crear política).	
Recupere la función de Lambda Amazon Resource Name (ARN).	1. Abra la consola Lambda. 2. Seleccione Funciones en el panel de navegación. 3. Elija la función que acaba de crear. 4. En la sección Descripción general de la función, en ARN de la función, copia el valor.	AWS general

Tarea	Descripción	Habilidades requeridas
Cree la regla personalizada de AWS Config.	1. Abra la consola de AWS Config en https://console.aws.amazon.com/config/. 2. En la página Rules (Reglas), seleccione Add rule (Añadir regla). 3. En la página Especificar el tipo de regla, elija Crear regla Lambda personalizada y, a continuación, elija Siguiente. 4. En la página Configurar regla, haga lo siguiente: a. Introduzca un nombre y una descripción. b. Para el ARN de la función AWS Lambda, pegue el ARN que copió anteriormente. c. Para Tipo de desencadenador, elija Cuando cambia la configuración. d. En Alcance de los cambios, seleccione Recursos. e. En Tipo de recurso, elija AWS EC2 NetworkInterface. f. Elija Siguiente. 5. En la página Revisar y crear, compruebe la regla y,	AWS general

Tarea	Descripción	Habilidades requeridas
	a continuación, seleccione Guardar.	
Configura las notificaciones.	1. Siga las instrucciones de Creación de un tema de Amazon SNS para crear un tema de Amazon SNS. 2. Siga las instrucciones del tema Suscribirse a un Amazon SNS para configurar un punto de conexión que reciba notificaciones del tema Amazon SNS. 3. Siga las instrucciones de Cómo puedo recibir una notificación cuando un recurso de AWS no es conforme mediante AWS Config para configurar una EventBridge regla de Amazon personalizada para sus recursos no conformes.	AWS general

Pruebe la solución

Tarea	Descripción	Habilidades requeridas
Cree un recurso que cumpla con las normas.	1. Siga las instrucciones siguientes para crear uno de los recursos compatibles en una subred pública: • Cree una puerta de enlace NAT	AWS general

Tarea	Descripción	Habilidades requeridas
	• Cómo empezar con los balanceadores de carga de red • Creación de un equilibrador de carga de aplicación 2. Una vez creado el recurso, la regla personalizada de AWS Config evalúa las interfaces de red elásticas asociadas al recurso. Marca estas interfaces de red como `COMPLIANT` . Puede ver los recursos en AWS Config siguiendo estos pasos: a. Abra la consola de AWS Config en https://console.aws.amazon.com/config/. b. En la página de reglas, elija su regla. c. En la página de detalles de la regla, ve al final de la página. d. En Recursos incluidos en el ámbito de aplicación, selecciona Cumple. Confirme que ve los ID de las interfaces de red que se crearon. e. Para obtener más información sobre la	

Tarea	Descripción	Habilidades requeridas
	configuración de la interfaz de red, elija el ID del recurso.	

Tarea	Descripción	Habilidades requeridas
Cree un recurso que no cumpla con las normas.	1. Siga las instrucciones siguientes para crear un recurso no compatible en una subred pública: • Lance una instancia de Amazon EC2 • Creación de una instancia de base de datos de Amazon Relational Database Service (Amazon RDS) • Crear un punto final de VPC 2. Una vez creado el recurso, la regla personalizada de AWS Config evalúa las interfaces de red elásticas asociadas al recurso. Marca estas interfaces de red como `NON_COMPLIANT` . Puede ver los recursos en AWS Config siguiendo estos pasos: a. Abra la consola de AWS Config en https://console.aws.amazon.com/config/. b. En la página de reglas, elija su regla. c. En la página de detalles de la regla, ve al final de la página.	AWS general

Tarea	Descripción	Habilidades requeridas
	d. En Recursos incluidos en el ámbito de aplicación, selecciona NonCompliant. Confirme que ve los ID de las interfaces de red que se crearon. e. Para obtener más información sobre la configuración de la interfaz de red, elija el ID del recurso. 3. Confirme que recibe la notificación en el punto de conexión que configuró en Amazon SNS.	
Cree un recurso que no sea aplicable.	1. En una subred privada, cree cualquier recurso que requiera una interface de red elástica. 2. Una vez creado el recurso, la regla personalizada de AWS Config evalúa las interfaces de red elásticas asociadas al recurso. Marca estas interfaces de red como`NOT_APPLICABLE` . Estos recursos no se muestran en la consola de AWS Config.	AWS general

Recursos relacionados

Documentación de AWS

- Configuración de AWS Config
- Reglas personalizadas de AWS Config
- ABAC para AWS
- Implemente controles de acceso preventivos basados en atributos para las subredes públicas

Otros recursos de AWS

- Automatice el cumplimiento de la configuración a escala en AWS
- Arquitecturas de inspección distribuida con el Equilibrador de carga de puerta de enlace

Información adicional

El siguiente es un ejemplo de función Lambda que se proporciona con fines de demostración.

```
import boto3
import json
import os

# Init clients
config_client = boto3.client('config')
ec2_client = boto3.client('ec2')

def lambda_handler(event, context):

    # Init values
    compliance_value = 'NOT_APPLICABLE'
    invoking_event = json.loads(event['invokingEvent'])
    configuration_item = invoking_event['configurationItem']

    status = configuration_item['configurationItemStatus']
    eventLeftScope = event['eventLeftScope']

    # First check if the event configuration applies. Ex. resource event is not delete
    if (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope:
        compliance_value = evaluate_change_notification_compliance(configuration_item)


    config_client.put_evaluations(
       Evaluations=[
           {
```

```
                'ComplianceResourceType': invoking_event['configurationItem']
['resourceType'],
                'ComplianceResourceId': invoking_event['configurationItem']
['resourceId'],
                'ComplianceType': compliance_value,
                'OrderingTimestamp': invoking_event['configurationItem']
['configurationItemCaptureTime']
            },
        ],
        ResultToken=event['resultToken'])

# Function with the logs to evaluate the resource
def evaluate_change_notification_compliance(configuration_item):
    is_in_scope = is_in_scope_subnet(configuration_item['configuration']['subnetId'])

    if (configuration_item['resourceType'] != 'AWS::EC2::NetworkInterface') or not
 is_in_scope:
        return 'NOT_APPLICABLE'

    else:
        alb_condition = configuration_item['configuration']['requesterId'] in ['amazon-
elb']
        nlb_condition = configuration_item['configuration']['interfaceType'] in
 ['network_load_balancer']
        nat_gateway_condition = configuration_item['configuration']['interfaceType'] in
 ['nat_gateway']

        if alb_condition or nlb_condition or nat_gateway_condition:
            return 'COMPLIANT'
    return 'NON_COMPLIANT'

# Function to check if elastic network interface is in public subnet
def is_in_scope_subnet(eni_subnet):

    subnet_description = ec2_client.describe_subnets(
        SubnetIds=[eni_subnet]
    )

    for subnet in subnet_description['Subnets']:
        for tag in subnet['Tags']:
            if tag['Key'] == os.environ.get('TAG_KEY') and tag['Value'] ==
 os.environ.get('TAG_VALUE'):
                return True
```

```
    return False
```

Implemente controles de acceso preventivos basados en atributos para las subredes públicas

Creado por Joel Alfredo Núñez González (AWS) y Samuel Ortega Sancho (AWS)

Entorno: PoC o piloto	Tecnologías: seguridad, identidad, conformidad; redes; entrega de contenido	Servicios de AWS: AWS Organizations; AWS Identity and Access Management

Resumen

En las arquitecturas de red centralizadas, las nubes privadas virtuales (VPC) periféricas y de inspección concentran todo el tráfico entrante y saliente, como el tráfico que entra y sale de Internet. Sin embargo, esto puede crear cuellos de botella o provocar que se alcancen los límites de las Service quotas de AWS. La implementación de la seguridad periférica de la red junto con las cargas de trabajo de sus VPC proporciona una escalabilidad sin precedentes en comparación con el enfoque centralizado más común. Esto se denomina arquitectura de periferia distribuida.

Si bien la implementación de subredes públicas en las cuentas de carga de trabajo puede ofrecer beneficios, también presenta nuevos riesgos de seguridad porque aumenta la superficie expuesta a ataques. Se recomienda implementar únicamente los recursos de Elastic Load Balancing (ELB), como los equilibradores de carga de aplicaciones o las puertas de enlace NAT, en las subredes públicas de estas VPC. El uso de equilibradores de carga y puertas de enlace NAT en subredes públicas dedicadas le ayuda a implementar un control detallado del tráfico entrante y saliente.

El control de acceso basado en atributos (ABAC) es la práctica de crear permisos detallados basados en los atributos del usuario, como el departamento, el puesto de trabajo y el nombre del equipo. Para obtener más información, consulte ABAC para AWS. ABAC puede proporcionar barreras para las subredes públicas en las cuentas de carga de trabajo. Esto ayuda a los equipos de aplicaciones a ser ágiles, sin comprometer la seguridad de la infraestructura.

Este patrón describe cómo ayudar a proteger las subredes públicas mediante la implementación de ABAC mediante una política de control de servicios (SCP) en AWS Organizations y políticas en AWS Identity and Access Management (IAM). El SCP se aplica a una cuenta de miembro de una organización o a una unidad organizativa (OU). Estas políticas de ABAC permiten a los usuarios

implementar pasarelas NAT en las subredes de destino e impiden que desplieguen otros recursos de Amazon Elastic Compute Cloud (Amazon EC2), como instancias EC2 e interfaces de red elásticas.

Requisitos previos y limitaciones

Requisitos previos

- Una organización en AWS Organizations
- Acceso administrativo a la cuenta raíz de AWS Organizations
- En la organización, una cuenta de miembro activa o una unidad organizativa para probar el SCP

Limitaciones

- El SCP de esta solución no impide que los servicios de AWS que utilizan un rol vinculado a un servicio implementen recursos en las subredes de destino. Algunos ejemplos de estos servicios son Elastic Load Balancing (ELB), Amazon Elastic Container Service (Amazon ECS) y Amazon Relational Database Service (Amazon RDS). Para obtener más información, consulte Efectos de SCP en los permisos en la documentación de AWS Organizations. Implemente controles de seguridad para detectar estas excepciones.

Arquitectura

Pila de tecnología de destino

- SCP aplicado a una cuenta o unidad organizativa de AWS en AWS Organizations
- Las siguientes roles de IAM:
  - `AutomationAdminRole`: Se utiliza para modificar las etiquetas de subred y crear recursos de VPC después de implementar el SCP
  - `TestAdminRole`: Se utiliza para comprobar si el SCP impide que otros responsables de IAM, incluidos los que tienen acceso administrativo, realicen las acciones reservadas para `AutomationAdminRole`

Arquitectura de destino

1. El rol de IAM de `AutomationAdminRole` se crea en la cuenta de destino. Este rol tiene permisos para administrar los recursos de red. Tenga en cuenta los siguientes permisos que son exclusivos de este rol:
   - Este rol puede crear VPC y subredes públicas.
   - Este rol puede modificar las asignaciones de etiquetas para las subredes de destino.
   - Este rol puede administrar sus propios permisos.
2. En AWS Organizations, se aplica el SCP a la cuenta o unidad organizativa de AWS de destino. Para ver un ejemplo de política, consulte Información adicional en este patrón.
3. Un usuario o una herramienta de la canalización de CI/CD pueden asumir el rol de `AutomationAdminRole` de solicitar la etiqueta `SubnetType` a las subredes de destino.
4. Al asumir otros roles de IAM, los directores de IAM autorizados de su organización pueden administrar las puertas de enlace NAT en las subredes de destino y otros recursos de red permitidos en la cuenta de AWS, como las tablas de enrutamiento. Utilice políticas de IAM para conceder esos permisos. Para obtener más información, consulte Administración de identidad y acceso para Amazon VPC.

Automatizar y escalar

Para ayudar a proteger las subredes públicas, se deben aplicar las etiquetas de AWS correspondientes. Tras aplicar el SCP, las puertas de enlace NAT son el único tipo de recurso de Amazon EC2 que los usuarios autorizados pueden crear en las subredes que tienen la etiqueta `SubnetType:IFA`. (`IFA` se refiere a los activos con acceso a Internet). El SCP impide la creación de otros recursos de Amazon EC2, como instancias e interfaces de red elásticas. Le recomendamos que utilice una canalización de CI/CD que asuma la `AutomationAdminRole` función de crear recursos de VPC para que estas etiquetas se apliquen correctamente a las subredes públicas.

Herramientas

Servicios de AWS

- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Organizations es un servicio de administración de cuentas que le permite agrupar varias cuentas de AWS en una organización que usted crea y administra de manera centralizada. En AWS Organizations, puede implementar políticas de control de servicios (SCP), que son un tipo de política que puede utilizar para administrar permisos en su organización.

- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esta red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Epics

Aplicación del SCP

Tarea	Descripción	Habilidades requeridas
Cree un rol de administrador de pruebas.	Cree un rol de IAM denominado `TestAdminRole` en la cuenta destino de AWS. Adjunte la política de IAM gestionada por AdministratorAccessAWS a la nueva función. Para obtener instrucciones, consulte Crear un rol para delegar permisos a un usuario de IAM en la documentación de IAM.	Administrador de AWS
Cree el rol de administrador de automatización.	1. Cree un rol de IAM denominado `AutomationAdminRole` en la cuenta destino de AWS. 2. Adjunte la política de IAM gestionada por AdministratorAccessAWS a la nueva función. El siguiente es un ejemplo de política de confianza que puede usar para probar el rol de la cuenta de `000000000000` .	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Principa l": { "AWS": ["arn:aws:iam::0000 00000000:root"] }, "Action": "sts:AssumeRole", "Conditio n": {} }] }	

Tarea	Descripción	Habilidades requeridas
Cree y adjunte el SCP.	1. Con el código de ejemplo que se proporciona en la sección de información adicional, cree una política de control de seguridad. Para obtener instrucciones, consulte Creación de un SCP en la documentación de AWS Organizations. 2. Adjunte el SCP a la cuenta o unidad organizativa de AWS de destino. Para obtener instrucciones, consulte Adjuntar y separar políticas de control de servicios en la documenta ción de AWS Organizations.	Administrador de AWS

Pruebe el SCP

Tarea	Descripción	Habilidades requeridas
Cree una VPC o subred.	1. Asuma el rol `TestAdmin Role` en la cuenta de AWS de destino. 2. Intente crear una VPC o una nueva subred pública en una VPC existente. Para obtener instrucciones, consulte Creación de una VPC, subredes y otros recursos de la VPC en la documentación de Amazon	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	VPC. No debería poder crear estos recursos. 3. Asuma el rol `AutomationAdminRole` y vuelva a intentar el paso anterior. Ahora debería poder crear los recursos de red.	

Tarea	Descripción	Habilidades requeridas
Administrar etiquetas.	1. Asuma el rol `TestAdminRole` en la cuenta de AWS de destino. 2. Añada una etiqueta `SubnetType:IFA` a una subred pública disponible. Debería poder añadir esta etiqueta. Para obtener instrucciones sobre cómo añadir etiquetas a través de la Interfaz de la línea de comandos de AWS (AWS CLI), consulte create-tags en la Referencia de los comandos de la CLI de AWS. 3. Sin cambiar sus credenciales, intente modificar la etiqueta `SubnetType:IFA` asignada a esta subred. No debería poder modificar esta etiqueta. 4. Asuma el rol `AutomationAdminRole` y vuelva a intentar los pasos anteriores. Este rol debería poder añadir y modificar esta etiqueta.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Implemente recursos en las subredes de destino.	1. Asumir el rol `TestAdmin Role` . 2. Para una subred pública que tenga la etiqueta `SubnetType:IFA` , intente crear una instancia de EC2. Para obtener instrucciones, consulte Lanzamiento de una instancia en la documenta ción de Amazon EC2. En esta subred, no debería poder crear, modificar ni eliminar ningún recurso de Amazon EC2, excepto las puertas de enlace NAT. 3. Cree una puerta de enlace NAT en la misma subred. Para obtener instrucciones, consulte Creación de una puerta de enlace NAT en la documentación de Amazon VPC. Debería poder crear, modificar o eliminar puertas de enlace NAT en esta subred.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Administre el AutomationAdminRole rol.	1. Asumir el rol `TestAdminRole` . 2. Intente modificar el rol `AutomationAdminRole` . Para obtener instrucciones, consulte Modificación de un rol en la documentación de IAM. No debería poder modificar este rol. 3. Asuma el rol `AutomationAdminRole` y vuelva a intentar el paso anterior. Ahora debería poder modificar el rol.	Administrador de AWS

Limpieza

Tarea	Descripción	Habilidades requeridas
Limpie los recursos desplegados.	1. Separe el SCP de la cuenta o unidad organizativa de AWS. Para obtener instrucciones, consulte Separar un SCP en la documentación de AWS Organizations. 2. Elimine la SCP. Para obtener instrucciones, consulte Eliminar un SCP (documentación de AWS Organizations). 3. Elimine el rol `AutomationAdminRole` y el rol	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	`TestAdminRole` . Para obtener instrucciones, consulte Eliminar funciones en la documentación de IAM. 4. Elimine todos los recursos de red, como las VPC y las subredes, que haya creado para esta solución.	

Recursos relacionados

Documentación de AWS

- Adjuntar y desconectar SCP
- Creación, actualización y eliminación de SCP
- Implemente controles de acceso basados en atributos de detección para subredes públicas mediante AWS Config
- Controles de detección
- Referencia de autorizaciones de servicio
- Etiquetado de recursos de AWS
- ¿Qué es ABAC para AWS?

Referencias adicionales de AWS

- Proteger las etiquetas de recursos utilizadas para la autorización mediante una política de control de servicios en AWS Organizations (entrada del blog de AWS)

Información adicional

La siguiente política de control de servicios es un ejemplo que puede utilizar para probar este enfoque en su organización.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyVPCActions",
      "Effect": "Deny",
      "Action": [
        "ec2:CreateVPC",
        "ec2:CreateRoute",
        "ec2:CreateSubnet",
        "ec2:CreateInternetGateway",
        "ec2:DeleteVPC",
        "ec2:DeleteRoute",
        "ec2:DeleteSubnet",
        "ec2:DeleteInternetGateway"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:*"
      ],
      "Condition": {
        "StringNotLike": {
          "aws:PrincipalARN": ["arn:aws:iam::*:role/AutomationAdminRole"]
        }
      }
    },
    {
      "Sid": "AllowNATGWOnIFASubnet",
      "Effect": "Deny",
      "NotAction": [
        "ec2:CreateNatGateway",
        "ec2:DeleteNatGateway"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition": {
        "ForAnyValue:StringEqualsIfExists": {
          "aws:ResourceTag/SubnetType": "IFA"
        },
        "StringNotLike": {
          "aws:PrincipalARN": ["arn:aws:iam::*:role/AutomationAdminRole"]
        }
      }
```

```
    },
    {
      "Sid": "DenyChangesToAdminRole",
      "Effect": "Deny",
      "NotAction": [
        "iam:GetContextKeysForPrincipalPolicy",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfilesForRole",
        "iam:ListRolePolicies",
        "iam:ListRoleTags"
      ],
      "Resource": [
        "arn:aws:iam::*:role/AutomationAdminRole"
      ],
      "Condition": {
        "StringNotLike": {
          "aws:PrincipalARN": ["arn:aws:iam::*:role/AutomationAdminRole"]
        }
      }
    },
    {
      "Sid": "allowbydefault",
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*"
    }
  ]
}
```

Implementar la solución Security Automations para AWS WAF mediante Terraform

Creado por el Dr. Rahul Sharad Gaikwad (AWS) y Tamilselvan (AWS)

Repositorio de códigos: - samples aws-waf-automation-terraform	Entorno: PoC o piloto	Tecnologías: seguridad, identidad, cumplimiento; infraestructura; entrega de contenido; DevOps
Carga de trabajo: todas las demás cargas de trabajo	Servicios de AWS: AWS WAF	

Resumen

AWS WAF es un firewall de aplicaciones web que ayuda a proteger las aplicaciones de los ataques más comunes mediante reglas personalizables, que se definen e implementan en listas de control de acceso (ACL) web. Configurar las reglas de AWS WAF puede resultar difícil, especialmente para las organizaciones que no cuentan con equipos de seguridad especializados. Para simplificar este proceso, Amazon Web Services (AWS) ofrece la solución Automatizaciones de seguridad para AWS WAF, que implementa automáticamente una única ACL web con un conjunto de reglas de AWS WAF que filtra los ataques basados en la web. Durante la implementación de Terraform, puede especificar qué características de protección desea incluir. Tras implementar esta solución, AWS WAF inspecciona las solicitudes web a las CloudFront distribuciones de Amazon o a los balanceadores de carga de aplicaciones existentes y bloquea las solicitudes que no cumplan con las reglas.

La solución Security Automations for AWS WAF se puede implementar mediante CloudFormation AWS según las instrucciones de la Guía de implementación de Security Automations for AWS WAF. Este patrón ofrece una opción de implementación alternativa para las organizaciones que utilizan HashiCorp Terraform como su herramienta preferida de infraestructura como código (IaC) para aprovisionar y administrar su infraestructura de nube. Al implementar esta solución, Terraform aplica automáticamente los cambios en la nube e implementa y configura los ajustes y las funciones de protección de AWS WAF.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada con los permisos necesarios. Para obtener más información, consulte Introducción (documentación de AWS CLI).
- Terraform instalado y configurado. Para obtener más información, consulte Instalar Terraform (documentación de Terraform).

Versiones de producto

- Versión 2.4.25 o posterior de la CLI de AWS
- Versión de Terraform 1.1.9 o posterior

Arquitectura

Arquitectura de destino

Este patrón despliega la solución Security Automations para AWS WAF. Para obtener más información sobre la arquitectura de destino, consulte la descripción general de la arquitectura en la Guía de implementación de automatizaciones de seguridad para AWS WAF. Para obtener más información sobre las automatizaciones de AWS Lambda en esta implementación, el analizador de registros de aplicaciones, el analizador de registros de AWS WAF, el analizador de listas de IP y el controlador de acceso, consulte los detalles de los componentes en la Guía de implementación de automatizaciones de seguridad para AWS WAF.

Implementación de Terraform

Cuando ejecuta `terraform apply`, Terraform hace lo siguiente:

1. Terraform crea roles de IAM y funciones de Lambda en función de las entradas del archivo testing.tfvars.
2. Terraform crea reglas de ACL y conjuntos de IP de AWS WAF en función de las entradas del archivo testing.tfvars.

3. Terraform crea los depósitos de Amazon Simple Storage Service (Amazon S3), las reglas de Amazon EventBridge , las tablas de bases de datos de AWS Glue y los grupos de trabajo de Amazon Athena en función de las entradas del archivo testing.tfvars.
4. Terraform implementa la CloudFormation pila de AWS para aprovisionar los recursos personalizados.
5. Terraform crea los recursos de Amazon API Gateway en función de las entradas proporcionadas del archivo testing.tfvars.

Automatizar y escalar

Puede usar este patrón para crear reglas de AWS WAF para varias cuentas y regiones de AWS con el fin de implementar la solución de automatizaciones de seguridad para AWS WAF en todo su entorno de nube de AWS.

Herramientas

Servicios de AWS

- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.
- AWS WAF es un firewall de aplicación web que le ayuda a monitorizar las solicitudes HTTP y HTTPS que se reenvíen a los recursos de su aplicación web protegida.

Otros servicios

- Git es un sistema de control de versiones distribuido y de código abierto.
- HashiCorp Terraform es una aplicación de interfaz de línea de comandos que le ayuda a usar código para aprovisionar y administrar la infraestructura y los recursos de la nube.

Repositorio de código

El código de este patrón está disponible en el repositorio GitHub AWS WAF Automation Using Terraform.

Prácticas recomendadas

- Coloque los archivos estáticos en buckets de S3 separados.
- Evite codificar variables de forma rígida.
- Limite el uso de scripts personalizados.
- Adopte una convención de nomenclatura.

Epics

Configure su equipo de trabajo local

Tarea	Descripción	Habilidades requeridas
Instale Git	Siga las instrucciones de Primeros pasos (sitio web de Git) para instalar Git en su estación de trabajo local.	DevOps ingeniero
Clonar el repositorio.	En la estación de trabajo local, introduzca el siguiente comando para clonar el repositorio de código. Para copiar el comando completo, incluida la URL del repositorio, consulte la sección Información adicional de este patrón. `git clone <repo-URL >.git`	DevOps ingeniero
Actualice las variables.	1. Acceda al directorio clonado ejecutando el siguiente comando. `cd terraform-aws-waf-automation`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	2. En cualquier editor de texto, abra el archivo testing.tfvars. 3. Actualice los valores de las variables en el archivo testing.tfvars. 4. Guarde y cierre el archivo.	

Aprovisionar la arquitectura de destino mediante Terraform

Tarea	Descripción	Habilidades requeridas
Inicialice la configuración de Terraform.	Introduzca el siguiente comando para inicializar el directorio de trabajo que contiene los archivos de configuración de Terraform. `terraform init`	DevOps ingeniero
Obtenga una vista previa del plan Terraform.	Escriba el siguiente comando. Terraform evalúa los archivos de configuración para determinar el estado objetivo de los recursos declarados. A continuación, compara el estado objetivo con el estado actual y crea un plan. `terraform plan -var-file ="testing.tfvars"`	DevOps ingeniero
Verifique el plan.	Revise el plan y confirme que configura la arquitectura	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	requerida en su cuenta de AWS de destino.	
Implemente la solución.	1. Escriba el siguiente comando para aplicar el plan. `terraform apply -var-file="testing.tfvars"` 2. Escriba `yes` para confirmar. Terraform crea, actualiza o destruye la infraestructura para alcanzar el estado objetivo declarado en los archivos de configuración. Para obtener más información sobre la secuencia, consulte el implementación de Terraform en la sección Arquitectura de este patrón.	DevOps ingeniero

Validar y limpiar

Tarea	Descripción	Habilidades requeridas
Verifique los cambios.	1. En la consola de Terraform, compruebe que las salidas coincidan con los resultados esperados. 2. Inicie sesión en la Consola de administración de AWS. 3. Compruebe que los resultados de la consola	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	de Terraform se hayan implementado correctam ente en su cuenta de AWS.	
(Opcional) Limpieza de la infraestructura.	Si desea eliminar todos los cambios de configuración y recursos realizados por esta solución, haga lo siguiente: 1. En la consola de Terraform , introduzca el siguiente comando. `terraform destroy -var-file="testing .tfvars”` 2. Escriba `yes` para confirmar.	DevOps ingeniero

Solución de problemas

Problema	Solución
Error de `WAFV2 IPSet: WAFOptimisticLockException`	Si recibe este error al ejecutar el comando `terraform destroy`, debe eliminar manualmente los conjuntos de IP. Para obtener instrucciones, consulte Eliminación de un conjunto de IP (documentación de AWS WAF).

Recursos relacionados

Referencias de AWS

- Guía de implementación de automatizaciones de seguridad para AWS WAF
- Automatizaciones de seguridad para AWS WAF (biblioteca de soluciones de AWS)

- Preguntas frecuentes sobre las automatizaciones de seguridad para AWS WAF

Referencias de Terraform

- Configuración del backend de Terraform
- Terraform AWS Provider: documentación y uso
- Terraform AWS Provider (GitHub repositorio)

Información adicional

El siguiente comando clona el GitHub repositorio para este patrón.

```
git clone https://github.com/aws-samples/aws-waf-automation-terraform-samples.git
```

Genere dinámicamente una política de IAM con IAM Access Analyzer mediante Step Functions

Creado por Thomas Scott (AWS), Adil El Kanabi (AWS), Koen van Blijderveen (AWS) y Rafal Pawlaszek (AWS)

Repositorio de código: Generador de políticas de roles de Automated IAM Access Analyzer	Entorno: PoC o piloto	Tecnologías: seguridad, identidad, conformidad; sin servidor
Servicios de AWS: Analizador de acceso de AWS IAM; AWS Lambda; AWS Step Functions ; AWS Identity and Access Management		

Resumen

El privilegio mínimo es la práctica recomendada de seguridad que consiste en conceder los permisos mínimos necesarios para realizar una tarea. Implementar el acceso con privilegios mínimos en una cuenta de Amazon Web Services (AWS) que ya está activa puede resultar difícil, ya que no se quiere impedir que los usuarios realicen sus tareas laborales cambiando sus permisos de forma involuntaria. Para poder implementar cambios en la política de IAM de AWS Identity and Access Management, debe entender qué acciones y recursos están llevando a cabo los usuarios de la cuenta.

Este patrón está diseñado para ayudarle a aplicar el principio del acceso con privilegio mínimo, sin bloquear ni ralentizar la productividad del equipo. Describe cómo usar IAM Access Analyzer y AWS Step Functions para generar dinámicamente una política de up-to-date IAM para su función, en función de las acciones que se están realizando actualmente en la cuenta. La nueva política está diseñada para permitir la actividad actual, pero eliminar cualquier privilegio elevado e innecesario. Puede personalizar la política generada definiendo reglas de autorización y denegación, y la solución integra sus reglas personalizadas.

Este patrón incluye opciones para implementar la solución con AWS Cloud Development Kit (AWS CDK) o HashiCorp CDK for Terraform (CDKTF). A continuación, puede asociar la nueva política al rol mediante una canalización de integración y entrega continuas (CI/CD). Si tiene una arquitectura de varias cuentas, puede implementar esta solución en cualquier cuenta en la que desee generar políticas de IAM actualizadas para los roles, lo que aumentará la seguridad de todo su entorno de nube de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa con una CloudTrail ruta habilitada.
- Permisos IAM para lo siguiente:
  - Cree e implemente flujos de trabajo de Step Functions. Para obtener más información, consulte Acciones, recursos y claves de condición de AWS Step Functions (documentación de Step Functions).
  - Cree una funciones de Lambda de AWS. Para obtener más información, consulte Rol de ejecución y permisos de usuario (documentación de Lambda).
  - Crear roles de IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un usuario de IAM (documentación de IAM).
- npm instalado. Para obtener más información, consulte Descargar e instalar Node.js y npm (documentación de npm).
- Si va a implementar esta solución con AWS CDK (opción 1):
  - Kit de herramientas de AWS CDK, instalado y configurado. Para obtener más información, consulte Instalar el CDK de AWS (documentación de AWS CDK).
- Si va a implementar esta solución con CDKTF (opción 2):
  - Ha instalado y configurado CDKTF. Para obtener más información, consulte Instalar el CDK para Terraform (documentación de CDKTF).
  - Terraform, instalado y configurado. Para obtener más información, consulte Introducción (documentación de Terraform).
- Interfaz de la línea de comandos de AWS (AWS CLI), instalada y configurada en su cuenta de AWS. Para obtener más información, consulte Instalar o actualizar la última versión de la CLI de AWS (documentación de la CLI DE AWS).

Limitaciones

- Este patrón no aplica la nueva política de IAM al rol. Al final de esta solución, la nueva política de IAM se almacena en un CodeCommit repositorio. Puede utilizar una canalización de CI/CD para aplicar políticas a los roles de su cuenta.

Arquitectura

Arquitectura de destino

1. Una regla de EventBridge eventos de Amazon programada regularmente inicia un flujo de trabajo de Step Functions. Este programa de regeneración se define como parte de la configuración de esta solución.
2. En el flujo de trabajo de Step Functions, una función Lambda genera los intervalos de fechas que se utilizarán al analizar la actividad de la cuenta en los CloudTrail registros.
3. El siguiente paso del flujo de trabajo llama a la API de IAM Access Analyzer para empezar a generar la política.
4. Con el nombre de recurso de Amazon (ARN) del rol que especificó durante la configuración, IAM Access Analyzer analiza los CloudTrail registros para detectar actividad dentro de la tasa de fechas especificada. En función de la actividad, IAM Access Analyzer genera una política de IAM que solo permite las acciones y los servicios que utilice el rol durante el intervalo de fechas especificado. Cuando se completa este paso, se genera un identificador de trabajo.
5. El siguiente paso del flujo de trabajo comprueba el ID del trabajo cada 30 segundos. Cuando se detecta el identificador de trabajo, este paso lo utiliza para llamar a la API de IAM Access Analyzer y recuperar la nueva política de IAM. IAM Access Analyzer devuelve la política como un archivo JSON.
6. El siguiente paso del flujo de trabajo coloca el archivo **<**IAM role name**>**/policy.json en un bucket de Amazon Simple Storage Service (Amazon S3). Defina este bucket de S3 como parte de la configuración de esta solución.
7. Una notificación de eventos de Amazon S3 inicia una función de Lambda.
8. La función Lambda recupera la política del bucket de S3, integra las reglas personalizadas que defina en los archivos allow.json y deny.json y, a continuación, envía la política actualizada a. CodeCommit Usted define el CodeCommit repositorio, la rama y la ruta de la carpeta como parte de la configuración de esta solución.

Herramientas

Servicios de AWS

- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura de la nube de AWS en código.
- Kit de herramientas de AWS CDK es un kit de desarrollo en la nube de línea de comandos que ayuda a interactuar con la aplicación AWS Cloud Development Kit (AWS CDK).
- AWS le CloudTrail ayuda a auditar la gobernanza, el cumplimiento y el riesgo operativo de su cuenta de AWS.
- AWS CodeCommit es un servicio de control de versiones que le ayuda a almacenar y gestionar repositorios de Git de forma privada, sin necesidad de gestionar su propio sistema de control de código fuente.
- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos. Este patrón utiliza el analizador de acceso de IAM, una función de IAM, para analizar sus CloudTrail registros e identificar las acciones y los servicios que ha utilizado una entidad de IAM (usuario o rol) y, a continuación, generar una política de IAM basada en esa actividad.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Step Functions es un servicio de orquestación sin servidor que le permite combinar funciones de Lambda AWS y otros servicios de AWS para crear aplicaciones esenciales desde el punto de vista empresarial. En este patrón, utiliza las integraciones de servicios del SDK de AWS en Step Functions para llamar a las acciones de la API de servicio desde su flujo de trabajo.

Otras herramientas

- CDK para Terraform (CDKTF) le ayuda a definir la infraestructura como código (IaC) mediante el uso de idiomas de programación comunes, como Python y Typescript.
- Lerna es un sistema de compilación para administrar y publicar varios paquetes JavaScript o TypeScript paquetes desde el mismo repositorio.
- Node.js es un entorno de JavaScript ejecución basado en eventos diseñado para crear aplicaciones de red escalables.
- npm es un registro de software que se ejecuta en un entorno Node.js y se utiliza para compartir o tomar prestados paquetes y administrar la implementación de paquetes privados.

Repositorio de código

El código de este patrón está disponible en el repositorio del generador de políticas de roles de GitHub Automated IAM Access Analyzer.

Epics

Preparación para la implementación

Tarea	Descripción	Habilidades requeridas
Clone el repositorio.	El siguiente comando clona el repositorio Automated IAM Access Analyze Role Policy Generator ()GitHub. `git clone https://github.com/aws-samples/automated-iam-access-analyzer.git`	Desarrollador de aplicaciones
Instale Lerna.	El siguiente comando instala Lerna. `npm i -g lerna`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Configure las dependencias.	Ingrese el siguiente comando para instalar las dependencias del repositorio. `cd automated-iam-access-advisor/` `npm install && npm run bootstrap`	Desarrollador de aplicaciones
Crear el código.	El siguiente comando prueba, compila y prepara los paquetes zip de las funciones de Lambda. `npm run test:code` `npm run build:code` `npm run pack:code`	Desarrollador de aplicaciones
Construya los constructos.	El siguiente comando crea la infraestructura que sintetiza las aplicaciones, tanto para el CDK como para el CDKTF de AWS. `npm run build:infra`	
Configure todos los permisos personalizados.	En la carpeta repo del repositorio clonado, edite los archivos allow.json y deny.json para definir los permisos personalizados para el rol. Si los archivos allow.json y deny.json contienen el mismo permiso, se aplica el permiso de denegación.	Administrador de AWS, desarrollador de aplicaciones

Opción 1: implementar la solución mediante AWS CDK

Tarea	Descripción	Habilidades requeridas
Implemente la pila de CDK de AWS.	El siguiente comando implementa la infraestructura a través de AWS CloudFormation. Defina los siguientes parámetros: • `<NAME_OF_ROLE>` : el ARN del rol de IAM para el que está creando una nueva política. • `<TRAIL_ARN>` — El ARN del registro en el que CloudTrail se almacena la actividad del rol. • `<CRON_EXPRESSION_TO_RUN_SOLUTION>` : la expresión Cron que define el programa de regeneración de la política. El flujo de trabajo de Step Functions se ejecuta según esta programación. • `<TRAIL_LOOKBACK>` : el período, en días, para echar un vistazo a la trayectoria al evaluar los permisos de los roles. `cd infra/cdk` `cdk deploy –-parameters roleArn=<NAME_OF_ROLE> \`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`—-parameters trailArn=<TRAIL_ARN> \ --parameters schedule=<CRON_EXPRESSION_TO_RUN_SOLUTION> \ [ --parameters trailLookBack=<TRAIL_LOOKBACK> ]` Nota: Los corchetes indican los parámetros opcionales.	
(Opcional) Espere a que aparezca la nueva política.	Si el registro no contiene una cantidad razonable de actividad histórica para el rol, espere hasta que esté seguro de que hay suficiente actividad registrada como para que IAM Access Analyzer genere una política precisa. Si el rol ha estado activo en la cuenta durante un período de tiempo suficiente, es posible que este período de espera no sea necesario.	Administrador de AWS
Revise manualmente la política generada.	En tu CodeCommit repositorio, revisa el archivo.json <ROLE_ARN>generado para confirmar que los permisos de autorización y denegación son adecuados para el rol.	Administrador de AWS

Opción 2: implementar la solución mediante CDKTF

Tarea	Descripción	Habilidades requeridas
Sintetice la plantilla Terraform.	El siguiente comando sintetiza la plantilla de Terraform. `lerna exec cdktf synth --scope @aiaa/tfm`	Desarrollador de aplicaciones
Implementar la plantilla Terraform.	El siguiente comando navega hasta el directorio que contiene la infraestructura definida por CDKTF. `cd infra/cdktf` El siguiente comando implementa la infraestructura en la cuenta de AWS de destino. Defina los siguientes parámetros: • `<account_ID>` : el ID de la cuenta de destino. • `<region>`: la región de AWS de destino. • `<selected_role_ARN>` : el ARN del rol de IAM para el que está creando una nueva política. • `<trail_ARN>` — El ARN del registro en el que CloudTrail se almacena la actividad del rol.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	• `<schedule_expression>` : la expresión Cron que define el programa de regeneración de la política. El flujo de trabajo de Step Functions se ejecuta según esta programación. • `<trail_look_back>` : el período, en días, para echar un vistazo a la trayectoria al evaluar los permisos de los roles. `TF_VAR_accountId=<account_ID> \ TF_VAR_region=<region> \ TF_VAR_roleArns=<selected_role_ARN> \ TF_VAR_trailArn=<trail_ARN> \ TF_VAR_schedule=<schedule_expression> \ [ TF_VAR_trailLookBack=<trail_look_back> ] \ cdktf deploy` Nota: Los corchetes indican los parámetros opcionales.	

Tarea	Descripción	Habilidades requeridas
(Opcional) Espere a que aparezca la nueva política.	Si el registro no contiene una cantidad razonable de actividad histórica para el rol, espere hasta que esté seguro de que hay suficiente actividad registrada como para que IAM Access Analyzer genere una política precisa. Si el rol ha estado activo en la cuenta durante un período de tiempo suficiente, es posible que este período de espera no sea necesario.	Administrador de AWS
Revise manualmente la política generada.	En tu CodeCommit repositor io, revisa el archivo.json <ROLE_ARN>generado para confirmar que los permisos de autorización y denegación son adecuados para el rol.	Administrador de AWS

Recursos relacionados

Recursos de AWS

- Puntos de conexión y cuotas de IAM Access Analyzer
- Configuración de la CLI de AWS
- Introducción a AWS CDK
- Aplicar permisos de privilegios mínimos

Otros recursos

- CDK para Terraform (sitio web de Terraform)

Habilite Amazon de GuardDuty forma condicional mediante plantillas de AWS CloudFormation

Creado por Ram Kandaswamy (AWS)

Entorno: producción	Tecnologías: seguridad, identidad, cumplimiento; operaciones DevOps	Servicios de AWS: AWS CloudFormation; Amazon GuardDuty; AWS Lambda; AWS Identity and Access Management

Resumen

Puede activar Amazon GuardDuty en una cuenta de Amazon Web Services (AWS) mediante una CloudFormation plantilla de AWS. De forma predeterminada, si ya GuardDuty está habilitada cuando intentas CloudFormation activarla, se produce un error en la implementación de la pila. Sin embargo, puedes usar las condiciones de tu CloudFormation plantilla para comprobar si ya GuardDuty está habilitada. CloudFormation admite el uso de condiciones que comparen valores estáticos; no admite el uso de la salida de otra propiedad de recurso dentro de la misma plantilla. Para obtener más información, consulte las condiciones en la guía CloudFormation del usuario.

En este patrón, utiliza un recurso CloudFormation personalizado respaldado por una función de AWS Lambda para habilitarlo de forma condicional GuardDuty si aún no está habilitada. Si GuardDuty está habilitada, la pila captura el estado y lo registra en la sección de salida de la pila. Si no GuardDuty está activado, la pila lo habilita.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un rol de AWS Identity and Access Management (IAM) con permisos para crear, actualizar y eliminar pilas CloudFormation

Limitaciones

- Si se GuardDuty ha desactivado manualmente para una cuenta o región de AWS, este patrón no se habilita GuardDuty para esa cuenta o región de destino.

Arquitectura

Pila de tecnología de destino

El patrón utiliza CloudFormation Infrastructure as Code (IaC). Utiliza un recurso CloudFormation personalizado respaldado por una función Lambda para lograr la capacidad de habilitación dinámica de servicios.

Arquitectura de destino

El siguiente diagrama de arquitectura de alto nivel muestra el proceso de habilitación GuardDuty mediante la implementación de una plantilla: CloudFormation

1. Se despliega una CloudFormation plantilla para crear una CloudFormation pila.
2. La pila crea un rol de IAM y una función de Lambda.
3. La función de Lambda asume el rol de IAM.
4. Si aún no GuardDuty está habilitada en la cuenta de AWS de destino, la función Lambda la habilita.

Automatizar y escalar

Puede utilizar la CloudFormation StackSet función de AWS para extender esta solución a varias cuentas y regiones de AWS. Para obtener más información, consulte Trabajar con AWS CloudFormation StackSets en la guía del CloudFormation usuario.

Herramientas

- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.
- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.

- Amazon GuardDuty es un servicio de supervisión continua de la seguridad que analiza y procesa los registros para identificar actividades inesperadas y potencialmente no autorizadas en su entorno de AWS.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.

Epics

Cree la CloudFormation plantilla e implemente la pila

Tarea	Descripción	Habilidades requeridas
Crea la CloudFormation plantilla.	1. Copia el código de la CloudFormation plantilla en la sección de información adicional. 2. Pegue el código en un editor de texto. 3. Guarde el archivo como `sample.yaml` en su terminal de trabajo.	AWS DevOps
Crea la CloudFormation pila.	1. En la CLI de AWS, ingrese el comando siguiente . Esto crea una nueva CloudFormation pila con el `sample.yaml` archivo. Para obtener más informaci ón, consulte Creación de una pila en la guía del CloudFormation usuario.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`` aws cloudformation create-stack \ --stack-name guardduty-cf-stack \ --template-body file://sample.yaml ``` 2. Confirme que el siguiente valor aparezca en la CLI de AWS. Este valor indica que la pila se ha creado correctamente. El tiempo necesario para crear la pila puede variar. ``` "StackStatus": "CREATE_COMPLETE", ```	
Valide que GuardDuty esté habilitado para la cuenta de AWS.	1. Inicie sesión en la consola de administración de AWS y abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/. 2. Compruebe que el GuardDuty servicio esté habilitado.	Administrador de la nube, administrador de AWS

Tarea	Descripción	Habilidades requeridas
Configure cuentas o regiones de AWS adicionales.	Según sea necesario para su caso de uso, utilice la CloudFormation StackSet función de AWS para extender esta solución a varias cuentas de AWS y regiones de AWS. Para obtener más información, consulte Trabajar con AWS CloudFormation StackSets en la guía del CloudFormation usuario.	Administrador de la nube, administrador de AWS

Recursos relacionados

Referencias

- CloudFormation Documentación de AWS
- Referencia del tipo de recurso de AWS Lambda
- CloudFormation tipo de recurso: AWS::IAM::Role
- CloudFormation tipo de recurso: AWS::GuardDuty::Detector
- Cuatro formas de recuperar cualquier propiedad de un servicio de AWS mediante AWS CloudFormation (blog)

Tutoriales y videos

- Simplifique la administración de la infraestructura con AWS CloudFormation (tutorial)
- Utilice Amazon GuardDuty y AWS Security Hub para proteger varias cuentas (AWS re:Invent 2020)
- Prácticas recomendadas para la creación de AWS CloudFormation (AWS re:Invent 2019)
- Detección de amenazas en AWS: introducción a Amazon GuardDuty (AWS Re:inForce 2019)

Información adicional

CloudFormation plantilla

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  rLambdaLogGroup:
    Type: 'AWS::Logs::LogGroup'
    DeletionPolicy: Delete
    Properties:
      RetentionInDays: 7
      LogGroupName: /aws/lambda/resource-checker
  rLambdaCheckerLambdaRole:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: !Sub 'resource-checker-lambda-role-${AWS::Region}'
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: lambda.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: /
      Policies:
        - PolicyName: !Sub 'resource-checker-lambda-policy-${AWS::Region}'
          PolicyDocument:
            Version: 2012-10-17
            Statement:
              - Sid: CreateLogGroup
                Effect: Allow
                Action:
                  - 'logs:CreateLogGroup'
                  - 'logs:CreateLogStream'
                  - 'logs:PutLogEvents'
                  - 'iam:CreateServiceLinkedRole'
                  - 'cloudformation:CreateStack'
                  - 'cloudformation:DeleteStack'
                  - 'cloudformation:Desc*'
                  - 'guardduty:CreateDetector'
                  - 'guardduty:ListDetectors'
                  - 'guardduty:DeleteDetector'
                Resource: '*'
  resourceCheckerLambda:
    Type: 'AWS::Lambda::Function'
    Properties:
      Description: Checks for resource type enabled and possibly name to exist
```

```
      FunctionName: resource-checker
      Handler: index.lambda_handler
      Role: !GetAtt
        - rLambdaCheckerLambdaRole
        - Arn
      Runtime: python3.8
      MemorySize: 128
      Timeout: 180
      Code:
        ZipFile: |
          import boto3
          import os
          import json
          from botocore.exceptions import ClientError
          import cfnresponse


          guardduty=boto3.client('guardduty')
          cfn=boto3.client('cloudformation')


          def lambda_handler(event, context):
              print('Event: ', event)
              if 'RequestType' in event:
                if event['RequestType'] in ["Create","Update"]:
                    enabled=False
                    try:
                      response=guardduty.list_detectors()
                      if "DetectorIds" in response and len(response["DetectorIds"])>0:
                        enabled="AlreadyEnabled"
                      elif "DetectorIds" in response and
len(response["DetectorIds"])==0:
                        cfn_response=cfn.create_stack(
                          StackName='guardduty-cfn-stack',
                          TemplateBody='{ "AWSTemplateFormatVersion": "2010-09-09",
"Description": "A sample template",    "Resources": { "IRWorkshopGuardDutyDetector": {
 "Type": "AWS::GuardDuty::Detector",    "Properties": {   "Enable": true  }   } } }'
                          )
                        enabled="True"
                    except Exception as e:
                        print("Exception: ",e)
                    responseData = {}
                    responseData['status'] = enabled
```

```
                    cfnresponse.send(event, context, cfnresponse.SUCCESS, responseData,
 "CustomResourcePhysicalID" )
                elif event['RequestType'] == "Delete":
                    cfn_response=cfn.delete_stack(
                            StackName='guardduty-cfn-stack')
                    cfnresponse.send(event, context, cfnresponse.SUCCESS, {})
  CheckResourceExist:
    Type: 'Custom::LambdaCustomResource'
    Properties:
      ServiceToken: !GetAtt
        - resourceCheckerLambda
        - Arn
Outputs:
  status:
    Value: !GetAtt
      - CheckResourceExist
      - status
```

Opción de código alternativa para el recurso Lambda

La CloudFormation plantilla proporcionada utiliza código en línea para hacer referencia al recurso de Lambda, a fin de facilitar la consulta y la orientación. Como alternativa, puede colocar el código Lambda en un bucket de Amazon Simple Storage Service (Amazon S3) y hacer referencia a él en la plantilla. CloudFormation El código en línea no admite bibliotecas ni dependencias de paquetes. Para respaldarlas, coloque el código Lambda en un bucket de S3 y haga referencia a él en la plantilla. CloudFormation

Sustituya las siguientes líneas de código:

```
Code:
         ZipFile: |
```

con las siguientes líneas de código:

```
Code:
      S3Bucket: <bucket name>
      S3Key: <python file name>
      S3ObjectVersion: <version>
```

La propiedad `S3ObjectVersion` se puede omitir si no usa control de versiones en su bucket de S3. Para más información, consulte Uso de control de versiones en buckets de S3 en la guía de usuario de Amazon S3.

Habilitar el cifrado transparente de datos en Amazon RDS para SQL Server

Creado por Ranga Cherukuri (AWS)

Entorno: PoC o piloto	Tecnologías: Seguridad, identidad, cumplimiento; Bases de datos	Carga de trabajo: Microsoft
Servicios de AWS: Amazon RDS		

Resumen

Este patrón describe cómo implementar el cifrado transparente de datos (TDE) en Amazon Relational Database Service (Amazon RDS) para SQL Server con el fin de cifrar los datos en reposo.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Instancia de base de datos de Amazon RDS para SQL Server

Versiones de producto

Actualmente, Amazon RDS admite TDE para las siguientes versiones y ediciones de SQL Server:

- SQL Server 2012 Enterprise Edition
- SQL Server 2014 Enterprise Edition
- SQL Server 2016 Enterprise Edition
- SQL Server 2017 Enterprise Edition
- SQL Server 2019: Standard y Enterprise Editions

Para obtener la información más reciente sobre las versiones y ediciones compatibles, consulte Compatibilidad con cifrado de datos transparente en SQL Server en la documentación de Amazon RDS.

Arquitectura

Pila de tecnología

- Amazon RDS para SQL Server

Arquitectura

Herramientas

Herramientas

- Microsoft SQL Server Management Studio (SSMS) es un entorno integrado para administrar infraestructuras de SQL Server. Proporciona una interfaz de usuario y un grupo de herramientas con editores de scripts enriquecidos que interactúan con SQL Server.

Epics

Cree un conjunto de opciones en la consola de Amazon RDS

Tarea	Descripción	Habilidades requeridas
Abra la consola de Amazon RDS.	Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon RDS.	Desarrollador, Administrador de base de datos
Crear un grupo de opciones.	En el panel de navegación, elija Opciñon grupos, Crear grupo. Seleccione sqlserver -ee como motor de base de datos y, a continuación,	Desarrollador, Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	seleccione la versión del motor.	
Agregue la opción TRANSPARENT_DATA_ENCRYPTION.	Edite el conjunto de opciones que ha creado y añada la opción denominada `TRANSPARENT_DATA_ENCRYPTION` .	Desarrollador, Administrador de base de datos

Asociar el grupo de opciones a la instancia de base de datos

Tarea	Descripción	Habilidades requeridas
Elija la instancia de base de datos.	En la consola de Amazon RDS, en el panel de navegación, elija Bases de datos y, a continuación, seleccione la instancia de base de datos que desea asociar con el grupo de opciones.	Desarrollador, Administrador de base de datos
Asocie la instancia de base de datos con el grupo de opciones.	Seleccione Modificar y, a continuación, use la configuración del conjunto de opciones para asociar la instancia de base de datos de SQL Server con el conjunto de opciones que creó anteriormente.	Desarrollador, Administrador de base de datos
Aplique los cambios.	Aplique los cambios inmediatamente o durante la siguiente ventana de mantenimiento, según desee.	Desarrollador, Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
Obtenga el nombre del certificado.	Obtenga el nombre predeterminado del certificado ejecutando la siguiente consulta. `USE [master]` `GO` `SELECT name FROM sys.certificates WHERE name LIKE 'RDSTDECertificate%'` `GO`	Desarrollador, Administrador de base de datos

Cree la clave de cifrado de la base de datos

Tarea	Descripción	Habilidades requeridas
Conéctese a la instancia de base de datos de Amazon RDS para SQL Server mediante SSMS.	Para obtener instrucciones, consulte Uar SSMS en la documentación de Microsoft.	Desarrollador, Administrador de base de datos
Cree la clave de cifrado de la base de datos usando el certificado predeterminado.	Crear una clave de encriptación de la base de datos utilizando el nombre del certificado por defecto que obtuvo anteriormente. Ejecute la siguiente consulta de T-SQL para crear una clave de cifrado de base de datos. Puede especificar el algoritmo AES_256 en lugar de AES_128. `USE [Databasename]` `GO`	Desarrollador, Administrador de base de datos

Tarea	Descripción	Habilidades requeridas
	`CREATE DATABASE ENCRYPTION KEY WITH ALGORITHM = AES_128 ENCRYPTION BY SERVER CERTIFICATE [certificatename] GO`	
Habilite el cifrado en la base de datos.	Ejecute la siguiente consulta T-SQL para habilitar el cifrado de base de datos. `ALTER DATABASE [Database Name] SET ENCRYPTION ON GO`	Desarrollador, Administrador de base de datos
Compruebe el estado del cifrado.	Ejecute la siguiente consulta T-SQL para comprobar el estado del cifrado. `SELECT DB_NAME(database_id) AS DatabaseName, encryption_state, percent_complete FROM sys.dm_database_encryption_keys`	Desarrollador, Administrador de base de datos

Recursos relacionados

- Compatibilidad con el Cifrado de datos transparente en SQL Server (documentación de Amazon RDS)
- Trabajo con conjuntos de opciones (documentación de Amazon RDS)
- Modificar una instancia de base de datos de Amazon RDS (documentación de Amazon RDS)
- Cifrado de datos transparente para SQL Server (documentación de Microsoft)

- Uso de SSMS (documentación de Microsoft)

Asegúrese de que las CloudFormation pilas de AWS se lancen desde buckets S3 autorizados

Entorno: producción	Tecnologías: seguridad, identidad, conformidad	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon SNS; AWS CloudWatch; CloudFormation Amazon; AWS Lambda; Amazon S3		

Resumen

Puede utilizar las CloudFormation plantillas de AWS para configurar los recursos de Amazon Web Services (AWS) mediante programación, de modo que dedique menos tiempo a gestionar esos recursos y más a centrarse en las aplicaciones que se ejecutan en AWS. Este patrón permite comprobar que las CloudFormation pilas de AWS se crean únicamente a partir de plantillas almacenadas en depósitos específicos de Amazon Simple Storage Service (Amazon S3). Esta comprobación resulta útil si tiene un requisito de seguridad o conformidad que requiera el uso de plantillas almacenadas en buckets de S3 que estén en una lista de permitidos.

Este control de seguridad supervisa las llamadas a AWS CloudFormation CreateStacky a la UpdateStackAPI e invoca una función de AWS Lambda que comprueba si la plantilla utilizada en la llamada proviene de un bucket de S3 autorizado. Si la plantilla proviene de un bucket no autorizado, la función de Lambda activa una notificación por correo electrónico de Amazon Simple Notification Service (Amazon SNS) al usuario con la información pertinente.

Requisitos previos y limitaciones

Requisitos previos

- Una dirección de correo electrónico activa en la que desee recibir notificaciones de infracciones
- Un bucket de S3 para subir el código de Lambda proporcionado
- Una lista de los nombres de los buckets de S3 autorizados

Limitaciones

- UpdateStackLas llamadas a la API que utilizan una plantilla existente en un bucket de S3 no autorizado no generan infracciones adicionales, ya que la URL del bucket de S3 no está disponible en el EventBridge evento de Amazon. Te recomendamos que elimines las plantillas existentes de los buckets de S3 no autorizados después de recibir la notificación de CreateStackinfracción original.
- Este control de seguridad no supervisa los siguientes CloudFormation eventos de AWS, ya que gestionan las actualizaciones después de la implementación inicial de la plantilla: CreateChangeSet, CreateStackSet, UpdateStackSet.
- Debe implementar este control de seguridad en todas las regiones de AWS que desee supervisar.

Arquitectura

Pila de tecnología de destino

- AWS Lambda
- Amazon SNS
- EventBridge Regla de Amazon

Arquitectura de destino

Automatizar y escalar

Si utiliza AWS Organizations, puede utilizar AWS CloudFormation StackSets para implementar esta plantilla en varias cuentas que desee supervisar.

Herramientas

- AWS Cloudformation: le ayuda a modelar y configurar los recursos de AWS mediante un infrastructure-as-code modelo.
- Amazon EventBridge: ofrece un flujo de datos en tiempo real desde sus propias aplicaciones, aplicaciones software-as-a-service (SaaS) y servicios de AWS, y dirige esos datos a destinos como AWS Lambda.
- AWS Lambda puede ejecutar código sin aprovisionar ni administrar servidores.

- Amazon SNS: proporciona la entrega de mensajes de los publicadores a los suscriptores. Los suscriptores reciben todos los mensajes publicados de los temas a los que están suscritos y todos los suscriptores de un tema reciben los mismos mensajes.
- Amazon S3 puede almacenar y recuperar cualquier cantidad de datos en cualquier momento y desde cualquier parte de la web.

Epics

Implementar el control de seguridad

Tarea	Descripción	Habilidades requeridas
Cargue el código de Lambda en Amazon S3.	Cargue el archivo .zip que contiene el código de Lambda que se proporciona en la sección «Adjuntos» del bucket de S3. Este bucket debería estar en la misma región de AWS que los recursos que desea evaluar.	Arquitecto de la nube
Implemente la CloudFormation plantilla de AWS.	Abra la CloudFormation consola de AWS en la misma región que su bucket de S3 e implemente la plantilla proporcionada en la sección «Adjuntos». Proporcione valores para los parámetro s; se describen en la sección «Información adicional».	Arquitecto de la nube

Confirmar la suscripción

Tarea	Descripción	Habilidades requeridas
Confirme la suscripción al tema de Amazon SNS.	Cuando la CloudFormation plantilla de AWS se implement a correctamente, envía un correo electrónico de suscripci ón a la dirección de correo electrónico que proporcionó. Debe confirmar la suscripci ón para comenzar a recibir notificaciones.	Arquitecto de la nube

Recursos relacionados

- Implementación de CloudFormation plantillas de AWS
- Amazon EventBridge
- AWS Lambda
- Amazon S3

Información adicional

Al implementar la CloudFormation plantilla de AWS proporcionada con este patrón, se le solicitará la siguiente información:

- Bucket de S3: especifique el bucket en el que cargó el código de Lambda adjunto (archivo.zip). Puede crear un nuevo bucket o utilizar un bucket existente.
- Clave S3: especifique la ubicación del archivo .zip de Lambda en el bucket de S3 (por ejemplo, nombre de archivo.zip o controls/nombre de archivo.zip). No utilice barras diagonales iniciales.
- Correo electrónico de notificación: proporcione una dirección de correo electrónico activa a la que deban enviarse las notificaciones de infracción.
- Nivel de registro Lambda: especifique el nivel y la frecuencia de registro de la función de Lambda. Utilice Info para registrar mensajes informativos detallados sobre el progreso, Error para los

eventos de error que pudieran continuar con la implementación y Advertencia en caso de situaciones potencialmente dañinas.

- Buckets autorizados: proporcione una lista delimitada por comas de los buckets de S3 autorizados.

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Asegúrese de que los equilibradores de carga de AWS usen protocolos de escucha seguros (HTTPS, SSL/TLS)

Creado por Chandini Penmetsa (AWS) y Purushotham G K (AWS)

Entorno: Producción	Tecnologías: seguridad, identidad, cumplimiento	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon SNS; AWS CloudWatch; CloudFormation Amazon; AWS Lambda; Elastic Load Balancing (ELB)		

Resumen

En la nube de Amazon Web Services (AWS), el Equilibrador de carga elástico distribuye automáticamente el tráfico entrante de las aplicaciones entre varios destinos, como instancias de Amazon Elastic Compute Cloud (Amazon EC2), contenedores, direcciones IP y funciones de Lambda de AWS. Los equilibradores de carga emplean oyentes para definir los puertos y protocolos que usa el equilibrador de carga para aceptar el tráfico de los usuarios. Los equilibradores de carga de aplicación toman las decisiones de enrutamiento en la capa de aplicación y emplean protocolos HTTP/HTTPS. Los equilibradores de carga de red toman las decisiones de enrutamiento en la capa de transporte y emplean protocolo de control de transmisión (TCP), seguridad de la capa de transporte (TLS), protocolo de datagramas de usuario (UDP) o protocolos TCP_UDP. Los equilibradores de carga clásicos toman las decisiones de enrutamiento en la capa de transporte, mediante protocolos TCP o Secure Sockets Layer (SSL), o bien en la capa de aplicación, mediante HTTP/HTTPS.

Es posible que su organización tenga como requisito de seguridad o conformidad que los equilibradores de carga acepten el tráfico de los usuarios únicamente mediante protocolos seguros, como HTTPS o SSL/TLS.

Este patrón proporciona un control de seguridad que usa una EventBridge regla de Amazon para monitorear las llamadas a la `CreateListener` `ModifyListener` API para los balanceadores de carga de aplicaciones y los balanceadores de carga de red, `CreateLoadBalancerListeners`

y las llamadas a la `CreateLoadBalancer` API para los balanceadores de carga clásicos. Si usa HTTP, TCP/UDP o TCP_UDP para el protocolo de escucha del equilibrador de carga, el control invoca una función de Lambda. La función de Lambda publica un mensaje en un tema de Amazon Simple Notification Service (Amazon SNS) para enviar una notificación con los detalles del equilibrador de carga.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- La dirección de correo electrónico en la que desee recibir la notificación de infracción
- Un bucket de Amazon Simple Storage Service (Amazon S3) para almacenar el archivo .zip del código Lambda.

Limitaciones

- Este control de seguridad no comprueba los equilibradores de carga existentes a menos que se actualicen los oyentes del equilibrador de carga.
- Este control de seguridad es regional, por lo que debe implementarse en las regiones de AWS que se desee supervisar.

Arquitectura

Pila de tecnología de destino

- Función de Lambda
- Tema de Amazon SNS
- EventBridge regla

Arquitectura de destino

Automatizar y escalar

- Si utiliza AWS Organizations, puede utilizar AWS Cloudformation StackSets para implementar esta plantilla en varias cuentas que desee que supervise.

Herramientas

- AWS CloudFormation: AWS CloudFormation es un servicio que le ayuda a modelar y configurar los recursos de AWS mediante el uso de la infraestructura como código.
- Amazon EventBridge: Amazon EventBridge ofrece un flujo de datos en tiempo real desde sus propias aplicaciones, aplicaciones de software como servicio (SaaS) y servicios de AWS, y dirige esos datos a objetivos como las funciones Lambda.
- AWS Lambda: Lambda admite ejecutar código sin aprovisionar ni administrar servidores.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos altamente escalable que se puede utilizar para una amplia gama de soluciones de almacenamiento, incluidos sitios web, aplicaciones móviles, copias de seguridad y lagos de datos.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) coordina y gestiona la entrega o el envío de mensajes entre publicadores y clientes, incluyendo los servidores web y las direcciones de correo electrónico. Los suscriptores reciben todos los mensajes publicados de los temas a los que están suscritos y todos los suscriptores de un tema reciben los mismos mensajes.

Prácticas recomendadas

Asegúrese de que el tema de SNS utilizado no sea de acceso público. Para obtener más información, consulte la documentación de AWS.

Epics

Cargue el código de Lambda

Tarea	Descripción	Habilidades requeridas
Elimine el bucket de S3.	En la consola de Amazon S3, seleccione o cree un bucket de S3 con un nombre único que no contenga barras diagonales en el inicio. Un nombre de bucket S3 es globalmente único y todas las cuentas de AWS comparten	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	el espacio de nombres. Su bucket S3 tiene que estar en la misma Región que el equilibrador de carga que se está evaluando.	
Cargue el código Lambda en el bucket de S3.	Cargue el archivo .zip de código Lambda que se proporciona en la sección «Adjuntos» en el bucket de S3 definido.	Arquitecto de la nube
Implemente la CloudFormation plantilla de AWS.	En la CloudFormation consola de AWS, en la misma región de AWS que el bucket de S3, implemente la plantilla que se proporciona en la sección «Adjuntos». En la epic siguiente, proporcione los valores de los parámetros.	Arquitecto de la nube

CloudFormation parámetros

Tarea	Descripción	Habilidades requeridas
Ponga nombre al bucket de S3.	Escriba el nombre del bucket de S3 que ha creado en la primera epic.	Arquitecto de la nube
Proporcione el prefijo de Amazon S3.	Proporcione la ubicación del archivo .zip de código Lambda en su bucket de S3, sin barras diagonales iniciales (por ejemplo, `<directory>/<file-name>.zip`).	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Proporcione el ARN de tema de SNS.	Si desea usar un tema de SNS existente para notificaciones de infracción, proporcione el nombre de recurso de Amazon (ARN) del tema de SNS. Para crear un tema de SNS nuevo, mantenga el valor como `None` (el valor predeterminado).	Arquitecto de la nube
Proporcione una dirección de correo electrónico.	Proporcione una dirección de correo electrónico activa en la que desea recibir las notificaciones de Amazon SNS.	Arquitecto de la nube
Defina el nivel de registro.	Defina el nivel y la frecuencia de registro de la función de Lambda. `Info` designa mensajes informativos detallados sobre el progreso de la aplicación. `Error` designa los eventos de error que aún podrían permitir que la aplicación siguiera ejecutándose. `Warning` designa situaciones potencialmente dañinas.	Arquitecto de la nube

Implemente la CloudFormation plantilla

Tarea	Descripción	Habilidades requeridas
Descargue la plantilla de .	Descarga la CloudFormation plantilla que se proporciona en la sección de adjuntos.	Arquitecto de la nube
Cree la pila.	En la misma región que el bucket de S3, vaya a la consola de CloudForm ation servicio e implement e la plantilla descargada. Consulte la épica anterior para obtener más detalles sobre los parámetros.	Arquitecto de la nube
Verifique los recursos.	Una vez que la pila se haya creado por completo, acceda a la pestaña Recursos y verifique los recursos. La plantilla creará los siguientes recursos: • EventBridge regla • Función de Lambda • Rol de ejecución de Lambda • Invocar permiso de Lambda	Arquitecto de la nube

Confirmar la suscripción

Tarea	Descripción	Habilidades requeridas
Confirmar la suscripción.	Cuando la plantilla se implementa correctamente, si se ha creado un nuevo tema	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	de SNS, se envía un mensaje de correo electrónico de suscripción a la dirección de correo electrónico proporcio nada en los parámetros. Debe confirmar esta suscripción de correo electrónico para recibir las notificaciones de infraccio nes.	

Solución de problemas

Problema	Solución
Error al crear la pila. Se produjo un error durante GetObject. Código de error S3: PermanentRedirect. Mensaje de error S3: el bucket está en esta región: xx-xxxx-1. Utilice esta región para volver a intentar la solicitud.	Asegúrese de que la región del bucket de S3 y la región en la que se está implementando la pila sean las mismas.
Error al crear la pila. El parámetro de tiempo de ejecución de python3.6 ya no es compatible con la creación o actualización de funciones de Lambda de AWS.	Actualice la plantilla descargada en la línea 186 de la versión 3.6 a la 3.9 de Python.

Recursos relacionados

- Creación de una pila en la CloudFormation consola de AWS
- AWS Lambda
- ¿Qué es un equilibrador de carga clásico?
- ¿Qué es un equilibrador de carga de aplicación?
- ¿Qué es un equilibrador de carga de red?
- Prácticas recomendadas para trabajar con funciones de Lambda de AWS

- Prácticas CloudFormation recomendadas de AWS

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Asegúrese de que el cifrado de los datos en reposo de Amazon EMR esté habilitado en el momento del lanzamiento

Creado por Priyanka Chaudhary (AWS)

Entorno: Producción	Tecnologías: seguridad, identidad; conformidad; análisis	Carga de trabajo: código abierto
Servicios de AWS: Amazon EMR; Amazon SNS; AWS KMS; CloudFormation AWS Lambda; Amazon S3		

Resumen

Este patrón proporciona un control de seguridad para supervisar el cifrado de los clústeres de Amazon EMR en Amazon Web Services (AWS).

El cifrado de datos ayuda a impedir que los usuarios no autorizados lean los datos en un clúster y sistemas de almacenamiento de datos asociados. Esto incluye los datos guardados en medios persistentes, conocidos como datos en reposo y datos que pueden ser interceptados cuando recorren la red, conocidos como datos en tránsito. Los datos en reposo de Amazon Simple Storage Service (Amazon S3) se pueden cifrar de dos maneras.

- Cifrado en el servidor con claves administradas por Amazon S3 (SSE-S3)
- Cifrado en el lado del servidor con claves de AWS Key Management Service (AWS KMS) configuradas con políticas adecuadas para Amazon EMR.

Este control de seguridad supervisa las llamadas a la API e inicia un evento de Amazon CloudWatch Events el RunJobFlow. El desencadenador invoca AWS Lambda, que ejecuta un script de Python. La función recupera la ID del clúster de EMR de la entrada JSON del evento y determina si hay una infracción de seguridad realizando las siguientes comprobaciones.

1. Comprueba si un clúster de EMR está asociado a una configuración de seguridad específica de Amazon EMR.

2. Si el clúster de EMR tiene asociada una configuración de seguridad específica de Amazon EMR, compruebe si la opción Encryption-at-Rest (Cifrado en reposo) está activada.
3. Si el cifrado en reposo no está activado, envíe una notificación de Amazon Simple Notification Service (Amazon SNS) que incluya el nombre del clúster de EMR, los detalles de la infracción, la región de AWS, la cuenta de AWS y el nombre de recurso de Amazon (ARN) de Lambda del que procede esta notificación.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un bucket de S3 para el archivo .zip de código Lambda
- La dirección de correo electrónico en la que desee recibir la notificación de infracción
- El registro de Amazon EMR está desactivado para poder recuperar todos los registros de la API

Limitaciones

- Este control de detección es regional, por lo que debe implementarse en las regiones de AWS que desee supervisar.

Versiones de producto

- Amazon EMR versión 4.8.0 y superiores

Arquitectura

Pila de tecnología de destino

- Amazon EMR
- Evento Amazon CloudWatch Events
- Función de Lambda
- Amazon SNS

Arquitectura de destino

Automatizar y escalar

- Si utiliza AWS Organizations, puede utilizar AWS Cloudformation StackSets para implementar esta plantilla en varias cuentas que desee supervisar.

Herramientas

Herramientas

- AWS CloudFormation: AWS CloudFormation es un servicio que le ayuda a modelar y configurar los recursos de AWS utilizando la infraestructura como código.
- Amazon CloudWatch Events: Amazon CloudWatch Events ofrece una transmisión casi en tiempo real de los eventos del sistema que describen los cambios en los recursos de AWS.
- Amazon EMR: Amazon EMR es una plataforma de clúster administrada que simplifica la ejecución de marcos de trabajo de macrodatos.
- AWS Lambda: AWS Lambda permite ejecutar código sin aprovisionar ni administrar servidores.
- Amazon S3: Amazon S3 es un servicio de almacenamiento de objetos altamente escalable que puede utilizarse para una amplia gama de soluciones de almacenamiento, incluidos sitios web, aplicaciones móviles, copias de seguridad y lagos de datos.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) coordina y gestiona la entrega o el envío de mensajes entre publicadores y clientes, incluyendo los servidores web y las direcciones de correo electrónico. Los suscriptores reciben todos los mensajes publicados de los temas a los que están suscritos y todos los suscriptores de un tema reciben los mismos mensajes.

Código

- Los archivos EMR EncryptionAtRest .zip y EMR EncryptionAtRest .yml de este proyecto están disponibles como archivos adjuntos.

Epics

Definir el bucket de S3

Tarea	Descripción	Habilidades requeridas
Elimine el bucket de S3.	En la consola de Amazon S3, seleccione o cree un bucket de S3 con un nombre único que no contenga barras diagonales en el inicio. Un nombre de bucket S3 es globalmente único y todas las cuentas de AWS comparten el espacio de nombres. Su bucket de S3 debe estar en la misma región de AWS que el clúster de Amazon EMR que se evalúa.	Arquitecto de la nube

Cargue el código Lambda en el bucket de S3

Tarea	Descripción	Habilidades requeridas
Cargue el código Lambda en el bucket de S3.	Cargue el archivo .zip de código Lambda que se proporciona en la sección «Adjuntos» en el bucket de S3 definido.	Arquitecto de la nube

Implemente la CloudFormation plantilla de AWS

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation plantilla de AWS.	En la CloudFormation consola de AWS, en la misma	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	región que su bucket de S3, implemente la CloudForm ation plantilla de AWS que se proporciona como adjunto a este patrón. En la epic siguiente, proporcione los valores de los parámetros. Para obtener más informaci ón sobre la implementación de CloudFormation plantillas de AWS, consulte la sección «Recursos relacionados».	

Complete los parámetros de la CloudFormation plantilla de AWS

Tarea	Descripción	Habilidades requeridas
Ponga nombre al bucket de S3.	Escriba el nombre del bucket de S3 que ha creado en la primera epic.	Arquitecto de la nube
Proporcione la clave de Amazon S3.	Proporcione la ubicación del archivo .zip del código Lambda en su bucket de S3, sin barras diagonales iniciales (por ejemplo, <directory>/<file-name>.zip).	Arquitecto de la nube
Proporcione una dirección de correo electrónico.	Proporcione una dirección de correo electrónico activa en la que desea recibir las notificac iones de Amazon SNS.	Arquitecto de la nube
Defina el nivel de registro.	Defina el nivel y la frecuenci a de registro de la función	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	de Lambda. «Info» designa mensajes informativos detallados sobre el progreso de la aplicación. «Error» designa eventos de error que todavía permiten que la aplicación siga ejecutándose. «Warning» designa situacion es potencialmente peligrosas.	

Confirmar la suscripción

Tarea	Descripción	Habilidades requeridas
Confirmar la suscripción.	Cuando la plantilla se implementa correctamente, se envía un mensaje de correo electrónico de suscripción a la dirección de correo electróni co proporcionada. Debe confirmar esta suscripción de correo electrónico para recibir las notificaciones de infraccio nes.	Arquitecto de la nube

Recursos relacionados

- Creación de una pila en la CloudFormation consola de AWS
- AWS Lambda
- Opciones de cifrado de Amazon EMR

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Asegúrese de que el perfil de IAM esté asociado a una instancia de EC2

Documento creado por Mansi Suratwala (AWS)

Entorno: Producción	Tecnologías: infraestructura; seguridad, identidad y conformidad	Servicios de AWS: Amazon EC2; AWS Identity and Access Management; Amazon CloudWatch; AWS Lambda; Amazon SNS

Resumen

Este patrón proporciona una plantilla de control de CloudFormation seguridad de AWS que configura una notificación automática cuando se produce una infracción del perfil de AWS Identity and Access Management (IAM) en una instancia de Amazon Elastic Compute Cloud (Amazon EC2).

Una perfil de instancia es un contenedor de un rol de IAM, que puede utilizar para transferir información del rol a una instancia EC2 cuando la instancia se inicia.

Amazon CloudWatch Events inicia esta comprobación cuando AWS CloudTrail registra las llamadas a la API de Amazon EC2 en función de `RunInstances` las acciones `AssociateIamInstanceProfile` y. `ReplaceIamInstanceProfileAssociation` El activador llama a una función de AWS Lambda, que utiliza un evento de Amazon CloudWatch Events para comprobar si hay un perfil de IAM.

Si no existe un perfil de IAM, la función de Lambda inicia el envío de una notificación por correo electrónico de Amazon Simple Notification Service (Amazon SNS) que incluye la ID de cuenta de Amazon Web Services (AWS) y la región de AWS.

Si existe un perfil de IAM, la función de Lambda comprueba si hay entradas comodín en los documentos de la política. Si existen entradas con caracteres comodín, se inicia una notificación de infracción de Amazon SNS para ayudarle a implementar una seguridad mejorada. La notificación contiene el nombre del perfil de IAM, el evento, la ID de la instancia de EC2, el nombre de la política gestionada, la infracción, la ID de cuenta y la región.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta activa
- Un bucket de Amazon Simple Storage Service (Amazon S3) para el archivo .zip del código Lambda.

Limitaciones

- La CloudFormation plantilla de AWS debe implementarse únicamente para las `RunInstances` `ReplaceIamInstanceProfileAssociation` acciones y. `AssociateIamInstanceProfile`
- El control de seguridad no supervisa la separación de los perfiles de IAM.
- El control de seguridad no comprueba la modificación de las políticas de IAM asociadas al perfil de IAM de la instancia de EC2.
- El control de seguridad no tiene en cuenta los permisos a nivel de recurso no compatibles que requieren el uso de `"Resource":*`.

Arquitectura

Pila de tecnología de destino

- Amazon EC2
- AWS CloudTrail
- Amazon CloudWatch
- AWS Lambda
- Amazon S3
- Amazon SNS

Arquitectura de destino

Automatizar y escalar

Puede utilizar la CloudFormation plantilla de AWS varias veces para distintas regiones y cuentas de AWS. Sólo tiene que lanzar la plantilla una vez para cada cuenta o Región.

Herramientas

Herramientas

- Amazon EC2: Amazon EC2 proporciona capacidad informática escalable (servidores virtuales) en la nube de AWS.
- AWS CloudTrail: AWS le CloudTrail ayuda a habilitar la gobernanza, el cumplimiento y la auditoría operativa y de riesgos de su cuenta de AWS. Las acciones realizadas por un usuario, un rol o un servicio de AWS se registran como eventos en CloudTrail.
- Amazon CloudWatch Events: Amazon CloudWatch Events ofrece una transmisión casi en tiempo real de los eventos del sistema que describen los cambios en los recursos de AWS.
- AWS Lambda: AWS Lambda es un servicio informático que puede usar para ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo.
- Amazon S3: Amazon S3 proporciona un almacenamiento de objetos altamente escalable que se puede utilizar para una amplia gama de soluciones de almacenamiento, incluidos sitios web, aplicaciones móviles, copias de seguridad y lagos de datos.
- Amazon SNS: Amazon SNS permite a las aplicaciones y dispositivos enviar y recibir notificaciones desde la nube.

Código

- El archivo .zip del proyecto está disponible como adjunto.

Epics

Definir el bucket de S3

Tarea	Descripción	Habilidades requeridas
Elimine el bucket de S3.	Para alojar el archivo .zip de código Lambda, seleccion e o cree un bucket de S3	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	con un nombre único que no contenga barras diagonale s al inicio. Un nombre de bucket S3 es globalmente único y todas las cuentas de AWS comparten el espacio de nombres. Su bucket S3 tiene que estar en la misma Región que la instancia EC2 que se está evaluando.	

Cargue el código Lambda en el bucket de S3

Tarea	Descripción	Habilidades requeridas
Cargue el código Lambda en el bucket de S3.	Cargue el archivo .zip de código Lambda que se proporciona en la sección Adjuntos del bucket de S3. El bucket S3 debe estar en la misma Región que la instancia EC2 que se está evaluando.	Arquitecto de la nube

Implemente la CloudFormation plantilla de AWS

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation plantilla de AWS.	Implemente la CloudForm ation plantilla de AWS que se proporciona como adjunto a este patrón. En la epic siguiente, proporcione los valores de los parámetros.	Arquitecto de la nube

Complete los parámetros de la CloudFormation plantilla de AWS

Tarea	Descripción	Habilidades requeridas
Ponga nombre al bucket de S3.	Escriba el nombre del bucket de S3 que ha creado en la primera epic.	Arquitecto de la nube
Proporcione la clave S3.	Proporcione la ubicación del archivo .zip de código Lambda en su bucket de S3 sin barras diagonales iniciales (por ejemplo, `<directory>/<file-name>.zip`).	Arquitecto de la nube
Proporcione una dirección de correo electrónico.	Proporcione una dirección de correo electrónico activa en la que desea recibir las notificaciones de Amazon SNS.	Arquitecto de la nube
Defina el nivel de registro.	Defina el nivel y la frecuencia de registro de la función de Lambda. `Info` designa mensajes informativos detallados sobre el progreso de la aplicación. `Error` designa los eventos de error que aún podrían permitir que la aplicación siguiera ejecutándose. `Warning` designa situaciones potencialmente dañinas.	Arquitecto de la nube

Confirmar la suscripción

Tarea	Descripción	Habilidades requeridas
Confirmar la suscripción.	Cuando la plantilla se implementa correctamente, se envía un mensaje de correo electrónico de suscripción a la dirección de correo electróni co proporcionada. Debe confirmar esta suscripción de correo electrónico para recibir las notificaciones de infraccio nes.	Arquitecto de la nube

Recursos relacionados

- Crear un bucket de S3
- Cargar los archivos en un bucket de S3
- Uso de perfiles de instancia
- Crear una regla de CloudWatch eventos que se active en una llamada a la API de AWS mediante AWS CloudTrail

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Asegúrese de que el clúster de Amazon Redshift esté cifrado en el momento de su creación

Documento creado por Mansi Suratwala (AWS)

Entorno: producción	Tecnologías: análisis; lago de datos; seguridad, identidad y cumplimiento	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon Redshift; Amazon SNS; AWS; Amazon; CloudWatch Amazon; CloudTrail AWS Lambda; Amazon S3		

Resumen

Este patrón proporciona una CloudFormation plantilla de AWS que le proporciona una notificación automática cuando se crea un nuevo clúster de Amazon Redshift sin cifrado.

La CloudFormation plantilla de AWS crea un evento de Amazon CloudWatch Events y una función de AWS Lambda. El evento detecta cualquier clúster de Amazon Redshift que se esté creando o restaurando a partir de una instantánea a través de AWS. CloudTrail Si el clúster se crea sin el cifrado del AWS Key Management Service (AWS KMS) o del modelo de seguridad de hardware en la nube (HSM) en la cuenta de AWS, CloudWatch inicia una función Lambda que le envía una notificación del Amazon Simple Notification Service (Amazon SNS) informándole de la infracción.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una nube privada virtual (VPC) con un grupo de subredes de clúster y un grupo de seguridad asociado.

Limitaciones

- La CloudFormation plantilla de AWS solo se puede implementar para las `RestoreFromClusterSnapshot` acciones `CreateCluster` y.

Arquitectura

Pila de tecnología de destino

- Amazon Redshift
- AWS CloudTrail
- Amazon CloudWatch
- AWS Lambda
- Amazon Simple Storage Service (Amazon S3)
- Amazon SNS

Arquitectura de destino

Automatizar y escalar

Puede utilizar la CloudFormation plantilla de AWS varias veces para distintas regiones y cuentas de AWS. Debe ejecutarla solo una vez en cada región o cuenta.

Herramientas

Herramientas

- Amazon Redshift: Amazon Redshift es un servicio de almacenamiento de datos totalmente administrado de varios petabytes en la nube. Amazon Redshift está integrado en el lago de datos, lo que permite usar los datos para adquirir nueva información para su empresa y sus clientes.
- AWS CloudTrail: AWS CloudTrail es un servicio de AWS que le ayuda a implementar la gobernanza, el cumplimiento y la auditoría operativa y de riesgos de su cuenta de AWS. Las acciones realizadas por un usuario, un rol o un servicio de AWS se registran como eventos en CloudTrail.
- Amazon CloudWatch Events: Amazon CloudWatch Events ofrece una transmisión casi en tiempo real de los eventos del sistema que describen los cambios en los recursos de AWS.

- AWS Lambda: AWS Lambda permite ejecutar código sin aprovisionar ni administrar servidores. AWS Lambda ejecuta el código solo cuando es necesario y amplia la capacidad de manera automática, pasando de pocas solicitudes al día a miles por segundo.
- Amazon S3: Amazon S3 es un servicio de almacenamiento de objetos altamente escalable que se puede utilizar para una amplia gama de soluciones de almacenamiento, incluidos sitios web, aplicaciones móviles, copias de seguridad y lagos de datos.
- Amazon SNS: Amazon SNS es un servicio web que coordina y gestiona la entrega o el envío de mensajes entre publicadores y clientes, incluidos servidores web y direcciones de correo electrónico.

Código

- El archivo .zip del proyecto está disponible como adjunto.

Epics

Definir el bucket de S3

Tarea	Descripción	Habilidades requeridas
Definir el bucket de S3.	En la consola de Amazon S3, elija o cree un bucket de S3. Este bucket de S3 alojará el archivo .zip de código Lambda. El bucket de Amazon S3 debe estar en la misma región que el clúster de Amazon Redshift que se está evaluando. El nombre de bucket de S3 no puede contener barras a la izquierda.	Arquitecto de la nube

Cargue el código Lambda en el bucket de S3

Tarea	Descripción	Habilidades requeridas
Cargue el código Lambda en el bucket de S3.	Cargue el código Lambda que se proporciona en la sección Adjuntos del bucket de S3. El bucket de S3 debe estar en la misma región que el clúster de Amazon Redshift que se está evaluando.	Arquitecto de la nube

Implemente la CloudFormation plantilla de AWS

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation plantilla de AWS.	Implemente la CloudFormation plantilla de AWS que se proporciona como adjunto a este patrón. En la epic siguiente, proporcione los valores de los parámetros.	Arquitecto de la nube

Complete los parámetros de la CloudFormation plantilla de AWS

Tarea	Descripción	Habilidades requeridas
Ponga nombre al bucket de S3.	Escriba el nombre del bucket de S3 que ha creado en la primera epic.	Arquitecto de la nube
Proporcione la clave S3.	Proporcione la ubicación del archivo .zip de código Lambda en su bucket de S3 sin barras diagonales iniciales (por	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	ejemplo, `<directory>/<file-name>.zip`).	
Proporcione una dirección de correo electrónico.	Proporcione una dirección de correo electrónico activa en la que desea recibir las notificaciones de Amazon SNS.	Arquitecto de la nube
Defina el nivel de registro.	Defina el nivel y la frecuencia de registro de la función de Lambda. `Info` designa mensajes informativos detallados sobre el progreso de la aplicación. `Error` designa los eventos de error que aún podrían permitir que la aplicación siguiera ejecutándose. `Warning` designa situaciones potencialmente dañinas.	Arquitecto de la nube

Confirmar la suscripción

Tarea	Descripción	Habilidades requeridas
Confirmar la suscripción.	Cuando la plantilla se implementa correctamente, se envía un correo electrónico de suscripción a la dirección de correo electrónico proporcionada. Debe confirmar esta suscripción de correo electrónico para recibir las notificaciones de infracciones.	Arquitecto de la nube

Recursos relacionados

- Crear un bucket de S3
- Carga de los archivos en un bucket de S3
- Crear una regla de CloudWatch eventos que se active en una llamada a la API de AWS mediante AWS CloudTrail
- Crear un clúster de Amazon Redshift)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Exporte un informe de las identidades del centro de identidad de IAM de AWS y sus asignaciones mediante PowerShell

Creado por Jorge Pava (AWS), Chad Miles (AWS), Frank Allotta (AWS) y Manideep Reddy Gillela (AWS)

Entorno: producción	Tecnologías: seguridad, identidad, cumplimiento; administración y gobierno	Carga de trabajo: Microsoft
Servicios de AWS: IAM Identity Center; herramientas de AWS para PowerShell		

Resumen

Cuando utiliza AWS IAM Identity Center (sucesor de AWS Single Sign-On) para gestionar de forma centralizada el acceso de inicio de sesión único (SSO) a todas sus cuentas y aplicaciones en la nube de Amazon Web Services (AWS), informar y auditar esas asignaciones a través de la consola de administración de AWS puede resultar tedioso y llevar mucho tiempo. Esto es especialmente cierto si está informando sobre los permisos de un usuario o grupo en docenas o cientos de cuentas de AWS.

Para muchos, la herramienta ideal para ver esta información sería en una aplicación de hoja de cálculo, como Microsoft Excel. Esto puede ayudarle a filtrar, buscar y visualizar los datos de toda su organización, gestionados por AWS Organizations.

Este patrón describe cómo utilizar las herramientas de AWS PowerShell para generar un informe de las configuraciones de identidad de SSO en el Centro de identidades de IAM. El informe tiene el formato de un archivo CSV e incluye el nombre de la identidad (entidad principal), el tipo de identidad (usuario o grupo), las cuentas a las que la identidad puede acceder y los conjuntos de permisos. Tras generar este informe, puede abrirlo en la aplicación que prefiera para buscar, filtrar y auditar los datos según sea necesario. En la siguiente imagen se muestran datos de muestra en una aplicación de hoja de cálculo.

Importante: dado que este informe contiene información confidencial, le recomendamos encarecid amente que la almacene de forma segura y que la comparta solo de forma need-to-know puntual.

Requisitos previos y limitaciones

Requisitos previos

- IAM Identity Center y AWS Organizations, configurados y habilitados.
- PowerShell, instalado y configurado. Para obtener más información, consulte Instalación PowerShell (documentación de Microsoft).
- Herramientas de AWS para PowerShell, instaladas y configuradas. Por motivos de rendimiento, le recomendamos encarecidamente que instale la versión modularizada de las herramientas de AWS para PowerShell, llamada. `AWS.Tools` Cada servicio de AWS es compatible con su pequeño módulo propio. En el PowerShell shell, introduzca los siguientes comandos para instalar los módulos necesarios para este patrón:`AWS.Tools.Installer`, `OrganizationsSSOAdmin`, y. `IdentityStore`

```
Install-Module AWS.Tools.Installer
Install-AWSToolsModule -Name Organizations, SSOAdmin, IdentityStore
```

  Para obtener más información, consulte Instalar AWS.Tools en Windows o Instalar AWS.Tools en Linux o macOS (AWS Tools para obtener documentación). PowerShell Si recibe un error al instalar los módulos, consulte la sección de Solución de problemas de este patrón.
- Interfaz de la línea de comandos de AWS (AWS CLI) o AWS SDK se deben configurar previamente con credenciales de trabajo mediante una de las siguientes acciones:
  - Utilice `aws configure` de CLI de AWS. Para obtener más información, consulte Configuración rápida (documentación de la CLI de AWS).
  - Configure la CLI de AWS o el AWS Cloud Development Kit (AWS CDK) para obtener acceso temporal a través de un rol de AWS Identity and Access Management (IAM). Para obtener más información, consulte Obtener credenciales de rol de IAM para acceder a la CLI (documentación del IAM Identity Center).
- Un perfil con nombre para la AWS CLI que ha guardado las credenciales de una entidad principal de IAM que:

- Tiene acceso a la cuenta de administración de AWS Organizations o a la cuenta de administrador delegado para IAM Identity Center
- Tiene aplicadas las políticas administradas de AWS `AWSSSOReadOnly` y `AWSSSODirectoryReadOnly`

Para obtener más información, consulte Uso de perfiles con nombre (documentación de CLI de AWS) y políticas administradas de AWS (documentación de IAM).

Limitaciones

- Las cuentas de AWS de destino deben administrarse como una organización en AWS Organizations.

Versiones de producto

- Para todos los sistemas operativos, se recomienda utilizar la PowerShell versión 7.0 o posterior.

Arquitectura

Arquitectura de destino

1. El usuario ejecuta el script en una línea de PowerShell comandos.
2. El script asume el perfil indicado para la CLI de AWS. Esto le da acceso al Centro de identidades de IAM.
3. El script recupera las configuraciones de identidad del SSO del IAM Identity Center.
4. El script genera un archivo CSV en el mismo directorio de la estación de trabajo en las instalaciones donde se guarda el script.

Herramientas

Servicios de AWS

- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que permite interactuar con los servicios de AWS mediante comandos en el intérprete de comandos de línea de comandos.

- AWS IAM Identity Center le ayuda a gestionar de forma centralizada el acceso de inicio de sesión único (SSO) a todas sus cuentas y aplicaciones en la nube de AWS.
- Las herramientas de AWS PowerShell son un conjunto de PowerShell módulos que le ayudan a programar operaciones en sus recursos de AWS desde la línea de PowerShell comandos.

Otras herramientas

- PowerShelles un programa de administración de automatización y configuración de Microsoft que se ejecuta en Windows, Linux y macOS.

Epics

Genere el informe

Tarea	Descripción	Habilidades requeridas
Preparación del script.	1. Copie el PowerShell script en la sección de informaci ón adicional de este patrón. 2. En la sección `Param`, en su entorno de AWS, defina los valores de las siguientes variables: • `OutputFile` : el nombre de archivo del informe. • `ProfileName` : el perfil con nombre de la AWS CLI que desea utilizar para generar el informe. • `Region`: la Región de AWS en la que se implementa IAM Identity Center. Para obtener una lista completa de las	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	regiones, consulte Puntos de conexión regionales. 3. Guarde el script con el nombre de archivo `SSO-Report.ps1` .	
Ejecute el script.	Se recomienda ejecutar el script personalizado en el PowerShell shell con el siguiente comando. `.\SSO-Report.ps1` Si lo desea, también puede ejecutar el script desde otro intérprete de comandos introduciendo el siguiente comando. `pwsh .\SSO-Report.ps1` El script genera un archivo CSV en el mismo directorio que el archivo de script.	Administrador de la nube
Analice los datos de los informes.	El archivo CSV de salida tiene los encabezados AccountNamePermissionSet, Principal y Tipo. Abra este archivo en la aplicación de hojas de cálculo que prefiera. Puede crear una tabla de datos para filtrar y ordenar la salida.	Administrador de la nube

Solución de problemas

Problema	Solución
Error de `The term 'Get-<parameter>' is not recognized as the name of a cmdlet, function, script file, or operable program.`	Las herramientas de AWS PowerShell o sus módulos no están instalados. En el PowerShell shell, introduzca los siguientes comandos para instalar las herramientas de AWS PowerShel l y los módulos necesarios para este patrón: `AWS.Tools.Installer` `Organizat ions` ,`SSOAdmin`, y`IdentityStore` . `Install-Module AWS.Tools.Installer` `Install-AWSToolsModule -Name` ` Organizations, SSOAdmin, IdentityS` `tore`
Error de `No credentials specified or obtained from persisted/shell defaults`	En la sección Preparar el script, en la sección Epics, confirme que ha introducido correctam ente las variables `ProfileName` y `Region`. Asegúrese de que la configuración y las credenciales del perfil indicado tengan permisos suficientes para administrar el IAM Identity Center.
Error `Authenticode Issuer …` al instalar los módulos de AWS.Tools	Agregue el parámetro `-SkipPubl isherCheck` al final del comando `Install-AWSToolsModule` .
Error de `Get-ORGAccountList : Assembly AWSSDK.SSO could not be found or loaded.`	Este error puede producirse cuando se especifican perfiles de CLI de AWS con nombre, la CLI de AWS se configura para autenticar a los usuarios con el Centro de identidad de IAM y la CLI de AWS se configura para recuperar automáticamente los tokens de autenticación actualizados. Para corregir este error, haga lo siguiente:

Problema	Solución
	1. Introduzca el siguiente comando para confirmar que los módulos `SSO` y `SSOOIDC` están instalados. `Install-AWSToolsModule SSO, SSOOIDC` 2. Inserte las siguientes líneas en el script situado debajo del bloque `param()`. `Import-Module AWS.Tools.SSO` `Import-Module AWS.Tools.SSOOIDC`

Recursos relacionados

- ¿Dónde se almacenan las opciones de configuración? (documentación de la CLI de AWS)
- Configurar la CLI de AWS para usar AWS IAM Identity Center (documentación de la CLI de AWS)
- Uso de perfiles con nombre (documentación de la CLI de AWS)

Información adicional

En el siguiente script, determine si necesita actualizar los valores de los siguientes parámetros:

- Si utiliza un perfil con nombre en la AWS CLI para acceder a la cuenta en la que está configurado el Centro de identidades de IAM, actualice el valor `$ProfileName`.
- Si el Centro de identidades de IAM se implementa en una región de AWS diferente a la región predeterminada para la configuración de AWS CLI o SDK de AWS, actualice el valor `$Region` para usar la región en la que está implementado el Centro de identidades de IAM.
- Si no se da ninguna de estas situaciones, no será necesario actualizar el script.

```
param (
    # The name of the output CSV file
    [String] $OutputFile  = "SSO-Assignments.csv",
```

```
    # The AWS CLI named profile
    [String] $ProfileName = "",
    # The AWS Region in which IAM Identity Center is configured
    [String] $Region      = ""
)
$Start = Get-Date; $OrgParams = @{}
If ($Region){ $OrgParams.Region = $Region}
if ($ProfileName){$OrgParams.ProfileName = $ProfileName}
$SSOParams   = $OrgParams.Clone(); $IdsParams = $OrgParams.Clone()
$AccountList = Get-ORGAccountList @OrgParams | Select-Object Id, Name
$SSOinstance = Get-SSOADMNInstanceList @OrgParams
$SSOParams['InstanceArn']       = $SSOinstance.InstanceArn
$IdsParams['IdentityStoreId']   = $SSOinstance.IdentityStoreId
$PSsets       = @{}; $Principals   = @{}
$Assignments  = @(); $AccountCount = 1; Write-Host ""
foreach ($Account in $AccountList) {
    $Duration = New-Timespan -Start $Start -End (Get-Date) | ForEach-Object
 {[Timespan]::New($_.Days, $_.Hours, $_.Minutes, $_.Seconds)}
    Write-Host "`r$Duration - Account $AccountCount of $($AccountList.Count)
 (Assignments:$($Assignments.Count))        " -NoNewline
    $AccountCount++
    foreach ($PS in Get-SSOADMNPermissionSetsProvisionedToAccountList -AccountId
 $Account.Id @SSOParams) {
        if (-not $PSsets[$PS]) {$PSsets[$PS] = (Get-SSOADMNPermissionSet @SSOParams -
PermissionSetArn $PS).Name;$APICalls++}
        $AssignmentsResponse = Get-SSOADMNAccountAssignmentList @SSOParams -
PermissionSetArn $PS -AccountId $Account.Id
        if ($AssignmentsResponse.NextToken) {$AccountAssignments =
 $AssignmentsResponse.AccountAssignments}
        else {$AccountAssignments = $AssignmentsResponse}
        While ($AssignmentsResponse.NextToken) {
            $AssignmentsResponse = Get-SSOADMNAccountAssignmentList @SSOParams -
PermissionSetArn $PS -AccountId $Account.Id -NextToken $AssignmentsResponse.NextToken
            $AccountAssignments += $AssignmentsResponse.AccountAssignments}
        foreach ($Assignment in $AccountAssignments) {
            if (-not $Principals[$Assignment.PrincipalId]) {
                $AssignmentType = $Assignment.PrincipalType.Value
                $Expression     = "Get-IDS"+$AssignmentType+" @IdsParams -"+
$AssignmentType+"Id "+$Assignment.PrincipalId
                $Principal      = Invoke-Expression $Expression
                if ($Assignment.PrincipalType.Value -eq "GROUP")
 { $Principals[$Assignment.PrincipalId] = $Principal.DisplayName }
                else { $Principals[$Assignment.PrincipalId] = $Principal.UserName }
            }
```

```
            $Assignments += [PSCustomObject]@{
                AccountName     = $Account.Name
                PermissionSet   = $PSsets[$PS]
                Principal       = $Principals[$Assignment.PrincipalId]
                Type            = $Assignment.PrincipalType.Value}
        }
    }
}
$Duration = New-Timespan -Start $Start -End (Get-Date) | ForEach-Object
 {[Timespan]::New($_.Days, $_.Hours, $_.Minutes, $_.Seconds)}
Write-Host "`r$($AccountList.Count) accounts done in $Duration. Outputting result to
 $OutputFile"
$Assignments | Sort-Object Account | Export-CSV -Path $OutputFile -Force
```

Supervisar y corregir la eliminación programada de las claves de AWS KMS

Creado por Mikesh Khanal (AWS) y Ramya Pulipaka (AWS)

Entorno: producción	Tecnologías: seguridad, identidad, conformidad; operaciones	Servicios de AWS: Amazon SNS; AWS CloudTrail; Amazon CloudWatch

Resumen

En la nube de Amazon Web Services (AWS), eliminar una clave de AWS Key Management Service (AWS KMS) puede provocar la pérdida de datos. El borrado elimina el material de la clave y todos los metadatos asociados a la clave de AWS KMS, y es irreversible. Una vez eliminada una clave de AWS KMS, ya no podrá descifrar los datos que estaban cifrados bajo esa clave de AWS KMS, por lo que no se podrán recuperar esos datos.

Este patrón configura la supervisión, con notificaciones cuando una aplicación o un usuario programa la eliminación de una clave de AWS KMS. Si recibe una notificación, puede cancelar la eliminación de la clave de AWS KMS y reconsiderar su decisión de eliminarla. El patrón utiliza el manual AWSConfigRemediation de automatización de AWS Systems Manager CancelKeyDeletion para facilitar la cancelación de la eliminación de una clave de AWS KMS.

Nota: La CloudFormation plantilla del patrón debe implementarse en todas las regiones de AWS en las que desee supervisar la eliminación de las claves de AWS KMS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Comprender los siguientes servicios de AWS:
  - Amazon EventBridge
  - AWS KMS
  - Amazon Simple Notification Service (Amazon SNS)
  - AWS Systems Manager

Limitaciones

- Cualquier personalización de la solución requiere conocer las CloudFormation plantillas de AWS y los servicios de AWS utilizados en este patrón.
- Actualmente, esta solución utiliza el bus de eventos predeterminado y se puede personalizar de acuerdo con los requisitos. Para obtener más información sobre el bus de eventos personalizado, consulte la documentación de AWS.

Arquitectura

Pila de tecnología de destino

- Amazon EventBridge
- AWS KMS
- Amazon SNS
- AWS Systems Manager
- Automatización mediante lo siguiente:
  - Interfaz de la línea de comandos de AWS (AWS CLI) o AWS SDK
  - CloudFormation Pila de AWS

Arquitectura de destino

1. La eliminación de una clave de AWS KMS está programada.
2. El evento de eliminación programada se evalúa mediante una regla. EventBridge
3. La EventBridge regla aborda el tema de Amazon SNS.
4. La EventBridge regla inicia la automatización y los manuales de ejecución de Systems Manager.
5. Los manuales de procedimientos cancelan la eliminación.

Automatizar y escalar

La CloudFormation pila despliega todos los recursos y servicios necesarios para que esta solución funcione. El patrón se puede ejecutar de forma independiente en una sola cuenta o se puede

ejecutar mediante AWS CloudFormation StackSets para varias cuentas independientes o una organización.

```
aws cloudformation create-stack --stack-name  <stack-name>\
    --template-body file://<Full-Path-of-file> \
    --parameters ParameterKey=,ParameterValue= \
    --capabilities CAPABILITY_NAMED_IAM
```

Herramientas

Herramientas

- AWS CloudFormation: AWS CloudFormation es un servicio que le ayuda a modelar y configurar sus recursos de Amazon Web Services para que pueda dedicar menos tiempo a gestionar esos recursos y más a centrarse en las aplicaciones que se ejecutan en AWS. Puede usar una CloudFormation plantilla para crear pilas en una cuenta de AWS en una región de AWS. La plantilla describe todos los recursos de AWS que desea y los CloudFormation aprovisiona y configura por usted.
- AWS CLI: la Interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de líneas de comandos.
- Amazon EventBridge: Amazon EventBridge es un servicio de bus de eventos sin servidor que conecta sus aplicaciones con datos de diversas fuentes. EventBridge ofrece un flujo de datos en tiempo real desde sus propias aplicaciones y servicios de AWS, y dirige esos datos a objetivos como AWS Lambda. EventBridge simplifica el proceso de creación de arquitecturas basadas en eventos.
- AWS KMS – AWS Key Management Service (AWS KMS) es un servicio administrado para crear y controlar las claves de AWS KMS, las claves de cifrado que se utilizan para cifrar sus datos.
- SDK de AWS – Las herramientas de AWS incluyen SDK para que pueda desarrollar y administrar aplicaciones en AWS en el lenguaje de programación que prefiera.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) es un servicio administrado con el que se ofrece la entrega de mensajes de los publicadores a los suscriptores (también conocido como productores y consumidores). Los publicadores se comunican de forma asíncrona con los suscriptores mediante el envío mensajes a un tema, que es un punto de acceso lógico y un canal de comunicación.
- AWS Systems Manager: AWS Systems Manager es un servicio que puede utilizar para ver y controlar su infraestructura en AWS. Mediante la consola de Systems Manager, puede automatizar

las tareas operativas en sus recursos de AWS. Systems Manager lo ayuda a mantener la seguridad y la conformidad mediante el análisis de sus instancias administradas y el informe sobre las infracciones de las políticas que detecte o la toma de medidas correctivas con respecto a estas.

Código

- Se adjunta la `alerting_ct_logs.yaml` CloudFormation plantilla del proyecto.

Epics

Preparación de la cuenta de AWS

Tarea	Descripción	Habilidades requeridas
Instalar y configurar la CLI de AWS.	Instale la CLI de AWS versión 2. A continuación, configure los ajustes de las credencia les de seguridad para una identidad, el formato de salida predeterminado y la región de AWS predeterminada que la CLI de AWS utiliza para interactuar con AWS. La identidad debe tener los permisos necesarios para realizar las tareas.	Desarrollador, ingeniero de seguridad

Implemente la CloudFormation plantilla de AWS

Tarea	Descripción	Habilidades requeridas
Descarga la CloudFormation plantilla.	Descargue el archivo adjunto a una ruta local en su computadora y extraiga	Desarrollador, ingeniero de seguridad

Tarea	Descripción	Habilidades requeridas
	el archivo `alerting_ct_logs.yaml` de plantilla .	
Implemente la plantilla.	En la ventana de terminal en la que se ha configurado el perfil de la cuenta de AWS, ejecute el siguiente comando. `aws cloudformation create-stack --stack-name <stack_name> \ --capabilities <Value> \ --template-body file://<Full_Path> \ --parameters ParameterKey=DestinationEmailAddress,ParameterValue=<Value> \ ParameterKey=SNSTopicName,ParameterValue=<Value> \ ParameterKey=EnableRemediation ,ParameterValue=<Value> \ ParameterKey=AutomationAssumeRole, ParameterValue=<Value>` En el siguiente paso, introduzca los valores de los parámetros de la plantilla.	Desarrollador, ingeniero de seguridad

Tarea	Descripción	Habilidades requeridas
Complete los parámetros de la plantilla.	Introduzca valores requeridos para los parámetros. • `DestinationEmailAddress` – La dirección de correo electrónico para recibir una alerta cuando esté programada la eliminación de una clave de AWS KMS. • `SNSTopicName` – El nombre del tema de Amazon SNS. • `EnableRemediation` – Cancelación de la eliminación programada de claves mediante un manual de procedimientos de Systems Manager. Los valores permitidos son `true` y `false`. • `AutomationAssumeRole` : el nombre de recurso de Amazon (ARN) del rol que permite a System Manager Automation realizar las acciones en su nombre. Para obtener más información, consulte la sección Permisos de IAM necesarios en la AWSConfigRemediation CancelKeyDeletion documentación.	Desarrollador, ingeniero de seguridad

Tarea	Descripción	Habilidades requeridas
	• `Capabilities` — Para CloudFormation que AWS cree la pila, debe reconocer explícitamente que la plantilla de pila contiene determinadas capacidades.	

Confirmar la suscripción

Tarea	Descripción	Habilidades requeridas
Confirmar la suscripción.	Verifique la bandeja de entrada de correo electrónico y elija Confirmar la suscripción en el mensaje de correo electrónico que reciba de Amazon SNS. Se abrirá una ventana del navegador web que mostrará una confirmación de suscripción y su ID de suscripción.	Desarrollador, ingeniero de seguridad

Recursos relacionados

Referencias

- Creación de una regla para un servicio de AWS
- Crear una CloudWatch alarma de Amazon para detectar el uso de una clave de AWS KMS pendiente de eliminación

Tutoriales y videos

- Cómo empezar con Amazon EventBridge
- Profundice en Amazon EventBridge (charlas técnicas en línea de AWS)

Taller de AWS

- ¿Trabajando con EventBridge reglas

Información adicional

En el siguiente código se proporcionan ejemplos para ampliar la solución a fin de supervisar y notificarlo sobre cualquier cambio en cualquier servicio de AWS. Los ejemplos incluyen patrones predefinidos y patrones personalizados. Para obtener más información, consulte Eventos y patrones de eventos en EventBridge.

```
EventPattern:
        source:
        - aws.kms
        detail-type:
        - AWS API Call via CloudTrail
        detail:
          eventSource:
          - kms.amazonaws.com
          eventName:
          - ScheduleKeyDeletion
```

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Identifique los buckets públicos de S3 en AWS Organizations mediante Security Hub

Creado por Mourad Cherfaoui (AWS), Arun Chandapillai (AWS) y Parag Nagwekar (AWS)

Entorno: producción	Tecnologías: seguridad, identidad, conformidad; almacenamiento y copias de seguridad	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon EventBridge; AWS Security Hub; Amazon SNS		

Resumen

Este patrón le muestra cómo crear un mecanismo para identificar buckets públicos de Amazon Simple Storage Service (Amazon S3) en sus cuentas de AWS Organizations. El mecanismo funciona mediante el uso de controles del estándar AWS Foundational Security Best Practices (FSBP) incluido en AWS Security Hub para supervisar los buckets S3. Puedes usar Amazon EventBridge para procesar las conclusiones de Security Hub y, después, publicarlas en un tema del Amazon Simple Notification Service (Amazon SNS). Las partes interesadas de su organización pueden suscribirse al tema y recibir notificaciones inmediatas por correo electrónico sobre los hallazgos.

De forma predeterminada, los nuevos buckets 63 y sus objetos no permiten el acceso público. Puede utilizar este patrón en situaciones en las que deba modificar las configuraciones predeterminadas de Amazon S3 en función de los requisitos de su organización. Por ejemplo, este podría ser un escenario en el que tenga un bucket S3 que aloje un sitio web de acceso público o archivos que todos los usuarios de Internet puedan leer desde su bucket S3.

Security Hub suele implementarse como un servicio central para consolidar todos los hallazgos de seguridad, incluidos los relacionados con los estándares de seguridad y los requisitos de cumplimiento. Hay otros servicios de AWS que puede utilizar para detectar buckets S3 públicos, pero este patrón utiliza una implementación de Security Hub existente con una configuración mínima.

Requisitos previos y limitaciones

Requisitos previos

- Una configuración de varias cuentas de AWS con una cuenta de Administrador dedicada de Security Hub
- Security Hub y AWS Config, habilitados en la región de AWS que desee monitorear (Nota: debe habilitar la agregación entre regiones en Security Hub si quiere monitorear varias regiones desde una sola región de agregación).
- Permisos de usuario para acceder y actualizar la cuenta de administrador de Security Hub, acceso de lectura a todos los buckets S3 de la organización y permisos para desactivar el acceso público (si es necesario)

Arquitectura

Pila de tecnología

- AWS Security Hub
- Amazon EventBridge
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)

Arquitectura de destino

El siguiente diagrama muestra una arquitectura para usar Security Hub para identificar los buckets S3 públicos.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Security Hub supervisa la configuración de los buckets S3 en todas las cuentas de AWS Organizations (incluida la cuenta de administrador) mediante los controles S3.2 y S3.3 del estándar de seguridad FSBP y detecta un resultado si un bucket está configurado como público.
2. La cuenta de administrador de Security Hub accede a los resultados (incluidos los de S3.2 y S3.3) desde todas las cuentas de los miembros.

3. Security Hub envía automáticamente todos los hallazgos nuevos y todas las actualizaciones de los hallazgos existentes EventBridge como Security Hub Findings - Imported events. Esto incluye eventos para conocer los resultados de las cuentas del administrador y de los miembros.
4. Una EventBridge regla filtra los resultados de las versiones S3.2 y S3.3 que tienen un `ComplianceStatus` de`FAILED`, un estado de flujo de trabajo de `NEW` y un `RecordState` de. `ACTIVE`
5. Las reglas utilizan los patrones de eventos para identificar los eventos y enviarlos a un tema de SNS una vez que coinciden.
6. Un tema de SNS envía los eventos a sus suscriptores (por ejemplo, por correo electrónico).
7. Los analistas de seguridad designados para recibir las notificaciones por correo electrónico revisan el bucket S3 en cuestión.
8. Si el bucket está aprobado para el acceso público, el analista de seguridad establece el estado del flujo de trabajo del resultado correspondiente en Security Hub como `SUPPRESSED`. De lo contrario, el analista establece el estado como `NOTIFIED`. Esto elimina las notificaciones futuras para el bucket S3 y reduce el ruido de las notificaciones.
9. Si el estado del flujo de trabajo está establecido como `NOTIFIED`, el analista de seguridad analiza los resultados con el propietario del bucket para determinar si el acceso público está justificado y si cumple con los requisitos de privacidad y protección de datos. Como resultado de la investigación, se elimina el acceso público al bucket o se aprueba el acceso público. En este último caso, el analista de seguridad establece el estado del flujo de trabajo como `SUPPRESSED`.

Nota: El diagrama de arquitectura se aplica a las implementaciones de agregación de una sola región y entre regiones. En las cuentas A, B y C del diagrama, Security Hub puede pertenecer a la misma región que la cuenta de administrador o pertenecer a regiones diferentes si está habilitada la agregación entre regiones.

Herramientas

Herramientas de AWS

- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. EventBridge ofrece un flujo de datos en tiempo real desde sus propias aplicaciones, aplicaciones de software como servicio (SaaS) y servicios de AWS. EventBridge enruta esos datos a destinos como temas de SNS y funciones de AWS Lambda si los datos coinciden con las reglas definidas por el usuario.

- Amazon Simple Notification Service (Amazon SNS) permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico. Los suscriptores reciben todos los mensajes publicados en los temas a los que están suscritos y todos los suscriptores de un tema reciben los mismos mensajes.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Security Hub proporciona una visión completa de su estado de seguridad en AWS. El Centro de seguridad le permite comprobar su entorno de AWS con los estándares y las prácticas recomendadas del sector de la seguridad. El Centro de seguridad recopila datos de seguridad de todas las cuentas de AWS, de los servicios y de los productos de terceros compatibles y posteriormente, le ayuda a analizar las tendencias de seguridad y a identificar los problemas de seguridad de mayor prioridad.

Epics

Configurar cuentas Security Hub

Tarea	Descripción	Habilidades requeridas
Habilite Security Hub en las cuentas de AWS Organizat ions.	Para habilitar Security Hub en las cuentas de la organización en las que desee supervisar los buckets S3, consulte las directrices de Designación de una cuenta de administrador de Security Hub (consola) y Administración de cuentas de miembros que pertenecen a una organización en la Guía del usuario de AWS Security Hub.	Administrador de AWS
(Opcional) Habilite la agregación entre regiones.	Si desea monitorear los buckets S3 en varias regiones desde una sola región,	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	configure la agregación entre regiones.	
Active los controles S3.2 y S3.3 para el estándar de seguridad FSBP.	Debe habilitar los controles S3.2 y S3.3 para el estándar de seguridad FSBP. 1. Para habilitar los controles de S3.2, siga las instrucciones de [S3.2] Los buckets S3 deberían prohibir el acceso de lectura público en la Guía del usuario de AWS Security Hub. 2. Para habilitar los controles de S3.3, siga las instrucciones de [3] Los buckets S3 deberían prohibir el acceso de escritura público en la Guía del usuario de AWS Security Hub.	Administrador de AWS

Configuración del entorno

Tarea	Descripción	Habilidades requeridas
Configure el tema de SNS y la suscripción por correo electrónico.	1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon SNS. 2. En el panel de navegación, seleccione Topics (Temas) y, a continuación, Create topic (Crear tema).	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	3. En Tipo, seleccione Estándar. 4. En Nombre, especifique un nombre para el tema (por ejemplo, public-s3-buckets). 5. Seleccione Create new topic (Crear nuevo tema). 6. En la pestaña Suscripciones, seleccione Crear suscripción. 7. En Protocol, seleccione Email. 8. En Endpoint (Punto de conexión), ingrese una dirección de correo electrónico para recibir las notificaciones. Puede utilizar la dirección de correo electrónico de un administrador de AWS, un profesional de TI o un profesional de Infosec. 9. Seleccione Crear una suscripción. Para crear suscripciones de correo electrónico adicionales, repita los pasos 6 a 8 según sea necesario.	

Tarea	Descripción	Habilidades requeridas
Configure la regla. EventBridge	1. Abra la consola de EventBridge . 2. En la sección Comenzar, selecciona EventBridge Regla y, a continuación, selecciona Crear regla. 3. En la página Definir detalles de la regla, en Nombre, especifique un nombre para la regla (por ejemplo, public-s3-buckets). Seleccione Next (Siguiente). 4. En la sección Event pattern (Patrón de eventos), seleccione Event pattern form (Formulario de patrón de eventos). 5. Copie el siguiente código, péguelo en el editor de códigos de Patrones de eventos y, a continuación, selecciona Siguiente. `{ "source": ["aws.securityhub"], "detail-type": ["Security Hub Findings - Imported"], "detail": { "findings": { "Compliance": { "Status": ["FAILED"]`	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	<pre>}, "RecordState": ["ACTIVE"], "Workflow": { "Status": ["NEW"] }, "ProductFields": { "ControlId": ["S3.2", "S3.3"] } } } }</pre> A continuación, proceda del modo siguiente: 1. En la página Seleccionar destinos, en Seleccione un destino, seleccione Tema de SNS como destino y, a continuación, seleccione el tema que creó anteriormente. 2. Elija Siguiente, vuelva a elegir Siguiente y, a continuación, elija Crear regla.	

Solución de problemas

Problema	Solución
Tengo un bucket S3 con acceso público activado, pero no recibo notificaciones por correo electrónico al respecto.	Esto podría deberse a que el bucket se creó en otra región y la agregación entre regiones no está habilitada en la cuenta de administr ador de Security Hub. Para resolver este problema, habilite la agregación entre regiones o implemente la solución de este patrón en la región en la que reside actualmente su bucket S3.

Recursos relacionados

- ¿Qué es el Centro de seguridad de AWS? (documentación de Centro de seguridad)
- Estándar de prácticas recomendadas de seguridad fundamentales (FSBP) de AWS (documentación de Security Hub)
- Scripts de activación de múltiples cuentas de AWS Security Hub (Laboratorios de AWS)
- Prácticas recomendadas de seguridad para Amazon S3 (documentación de Amazon S3)

Información adicional

Flujo de trabajo para monitorear buckets públicos S3

El siguiente flujo de trabajo ilustra cómo puede supervisar los buckets S3 públicos de su organización. El flujo de trabajo supone que ha completado los pasos descritos en Configurar el tema SNS y la suscripción de correo electrónico en la historia de este patrón.

1. Recibirá una notificación por correo electrónico cuando un bucket S3 esté configurado con acceso público.
   - Si el bucket está aprobado para el acceso público, defina el estado del flujo de trabajo del resultado correspondiente a `SUPPRESSED` en la cuenta de administrador de Security Hub. Esto evita que Security Hub emita más notificaciones para este bucket y puede eliminar las alertas duplicadas.

- Si el bucket no está aprobado para el acceso público, defina el estado del flujo de trabajo del resultado en la cuenta de administrador de Security Hub a `NOTIFIED`. Esto evita que Security Hub emita más notificaciones para este bucket desde Security Hub y puede eliminar el ruido.

2. Si el bucket puede contener datos confidenciales, desactive el acceso público inmediatamente hasta que se complete la revisión. Si desactiva el acceso público, Security Hub cambiará el estado del flujo de trabajo a `RESOLVED`. A continuación, se detienen las notificaciones por correo electrónico del bucket.
3. Busque al usuario que configuró el bucket como público (por ejemplo, mediante AWS CloudTrail) e inicie una revisión. Como resultado de la revisión, se elimina el acceso público al bucket o se aprueba el acceso público. Si se aprueba el acceso público, defina el estado del flujo de trabajo del resultado correspondiente a `SUPPRESSED`.

Gestione los conjuntos de permisos del AWS IAM Identity Center como código mediante AWS CodePipeline

Creado por Andre Cavalcante (AWS) y Claison Amorim (AWS)

Repositorio de código: - pipeline aws-iam-identity-center	Entorno: producción	Tecnologías: seguridad, identidad, cumplimiento; DevOps
Servicios de AWS: AWS CodeBuild; AWS CodeCommit CodePipeline; AWS IAM Identity Center		

Resumen

AWS IAM Identity Center (sucesor de AWS Single Sign-On) le ayuda a administrar de forma centralizada el acceso de inicio de sesión único (SSO) a todas las cuentas y aplicaciones de AWS. Puede crear y administrar identidades de usuario en IAM Identity Center, o puede conectar una fuente de identidades existente, como un dominio de Microsoft Active Directory o un proveedor de identidades (IdP) externo. IAM Identity Center ofrece una experiencia de administración unificada para definir, personalizar y asignar un acceso detallado a su entorno de AWS mediante conjuntos de permisos. Los conjuntos de permisos se aplican a los usuarios y grupos federados de su almacén de identidades de AWS IAM Identity Center o de su IdP externo.

Este patrón le ayuda a administrar los conjuntos de permisos del IAM Identity Center como código en su entorno de cuentas múltiples que se administra como una organización en AWS Organizations. Con este patrón, puede lograr lo siguiente:

- Crear, eliminar y actualizar conjuntos de permisos
- Cree, actualice o elimine asignaciones de conjuntos de permisos de destino a cuentas de AWS, unidades organizativas (OU) o la raíz de la organización.

Para gestionar los permisos y las asignaciones del IAM Identity Center como código, esta solución implementa una canalización de integración y entrega continuas (CI/CD) que utiliza AWS, AWS

y CodeCommit AWS. CodeBuild CodePipeline Usted administra los conjuntos de permisos y las asignaciones en plantillas JSON que almacena en el repositorio. CodeCommit Cuando EventBridge las reglas de Amazon detectan un cambio en el repositorio o detectan modificaciones en las cuentas de la unidad organizativa de destino, se inicia una función de AWS Lambda. La función de Lambda inicia la canalización de CI/CD que actualiza los conjuntos de permisos y las asignaciones en IAM Identity Center.

Requisitos previos y limitaciones

Requisitos previos

- Un entorno de varias cuentas gestionado como una organización en AWS Organizations. A fin de obtener más información, consulte Creación de una organización.
- IAM Identity Center, habilitado y configurado con una fuente de identidad. Para obtener más información, consulte Introducción en la documentación de IAM Identity Center.
- Una cuenta de miembro que está registrada como administrador delegado del IAM Identity Center. Para obtener instrucciones, consulte Registrar una cuenta de miembro en la documentación del IAM Identity Center.
- Permisos para implementar CloudFormation pilas de AWS en la cuenta de administrador delegado del IAM Identity Center y en la cuenta de administración de la organización. Para obtener más información, consulte Controlar el acceso en la documentación. CloudFormation
- Un bucket de Amazon Simple Storage Service (Amazon S3) en el administrador delegado del Identity Center para cargar el código del artefacto. Para ver instrucciones, consulte Crear un bucket.
- El ID de la cuenta de gestión de la organización. Para obtener instrucciones, consulte Encontrar el ID de su cuenta de AWS.

Limitaciones

- Este patrón no se puede usar para administrar o asignar conjuntos de permisos para entornos de una sola cuenta o para cuentas que no se administran como una organización en AWS Organizations.
- Los nombres de los conjuntos de permisos, los ID de asignación y los tipos e ID de entidad principal del IAM Identity Center no se pueden modificar después de la implementación.
- Este patrón le ayuda a crear y administrar permisos personalizados. No puede usar este patrón para administrar o asignar permisos predefinidos.

- Este patrón no se puede usar para administrar un conjunto de permisos para la cuenta de administración de la organización.

Arquitectura

Pila de tecnología

- AWS CodeBuild
- AWS CodeCommit
- AWS CodePipeline
- Amazon EventBridge
- AWS Identity Center
- AWS Lambda
- AWS Organizations

Arquitectura de destino

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un usuario realiza uno de los siguientes cambios:
   a. Realiza uno o más cambios en el repositorio CodeCommit
   b. Modifica las cuentas de la unidad organizativa (OU) de AWS Organizations
2. Si el usuario ha realizado un cambio en el CodeCommit repositorio, la `CodeChange` EventBridge regla detecta el cambio e inicia una función Lambda en la cuenta de administrador delegado de IAM Identity Center. La regla no reacciona a los cambios en determinados archivos del repositorio, como el archivo `README.md`.

   Si el usuario modificó las cuentas de la unidad organizativa, la `MoveAccount` EventBridge regla detecta el cambio e inicia una función Lambda en la cuenta de administración de la organización.
3. La función Lambda iniciada inicia la canalización de CI/CD. CodePipeline
4. CodePipeline inicia el proyecto. `CodebuildTemplateValidation` CodeBuild

5. El `CodebuildTemplateValidation` CodeBuild proyecto utiliza un script de Python en el CodeCommit repositorio para validar las plantillas del conjunto de permisos. CodeBuild valida lo siguiente:
   - Los nombres de conjunto de permisos son únicos.
   - Los ID de la declaración de asignación (`Sid`) son únicos.
   - Las definiciones de política figuran en el parámetro `CustomPolicy` y son válidas. (Esta validación utiliza AWS Identity and Access Management Access Analyzer)
   - Los nombres de recurso de Amazon (ARN) de las políticas administradas son válidos.
6. El `CodebuildPermissionSet` CodeBuild proyecto utiliza AWS SDK for Python (Boto3) para eliminar, crear o actualizar los conjuntos de permisos en el Centro de identidades de IAM. Solo se ven afectados los conjuntos de permisos con la etiqueta `SSOPipeline:true`. Todos los conjuntos de permisos que se administran a través de esta canalización tienen esta etiqueta.
7. El `CodebuildAssignments` CodeBuild proyecto utiliza Terraform para eliminar, crear o actualizar las asignaciones en el Centro de Identidad de IAM. Los archivos de estado del backend de Terraform se almacenan en un bucket de S3 en la misma cuenta.
8. CodeBuild asume una función de `lookup` IAM en la cuenta de administración de la organización. Llama a las API de las organizaciones y de identitystore para enumerar los recursos necesarios para conceder o revocar permisos.
9. CodeBuild actualiza los conjuntos de permisos y las asignaciones en el Centro de identidades de IAM.

Automatizar y escalar

Como todas las cuentas nuevas en un entorno de varias cuentas se trasladan a una unidad organizativa específica de AWS Organizations, esta solución se ejecuta automáticamente y concede los conjuntos de permisos necesarios a todas las cuentas que especifique en las plantillas de asignación. No se necesitan automatizaciones ni acciones de escalado adicionales.

En entornos de gran tamaño, la cantidad de solicitudes de API al IAM Identity Center puede provocar que esta solución se ejecute más lentamente. Terraform y Boto3 gestionan automáticamente la limitación para minimizar cualquier degradación del rendimiento.

Herramientas

Servicios de AWS

- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- AWS CodeBuild es un servicio de compilación totalmente gestionado que le ayuda a compilar código fuente, ejecutar pruebas unitarias y producir artefactos listos para su implementación.
- AWS CodeCommit es un servicio de control de versiones que le ayuda a almacenar y gestionar repositorios de Git de forma privada, sin necesidad de gestionar su propio sistema de control de código fuente.
- AWS le CodePipeline ayuda a modelar y configurar rápidamente las diferentes etapas de una versión de software y a automatizar los pasos necesarios para publicar cambios de software de forma continua.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, las funciones de Lambda de AWS, los puntos de conexión de invocación HTTP que utilizan destinos de API o los buses de eventos de otras cuentas de AWS.
- AWS IAM Identity Center le ayuda a gestionar de forma centralizada el acceso de inicio de sesión único (SSO) a todas sus cuentas y aplicaciones en la nube de AWS.
- AWS Organizations es un servicio de administración de cuentas que le permite agrupar varias cuentas de AWS en una organización que usted crea y administra de manera centralizada.
- AWS SDK para Python (Boto3) es un kit de desarrollo de software que permite integrar su aplicación, biblioteca o script de Python con los servicios de AWS.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Repositorio de código

El código de este patrón está disponible en el repositorio aws-iam-identity-center-pipeline. La carpeta de plantillas del repositorio incluye plantillas de muestra tanto para los conjuntos de permisos como para las asignaciones. También incluye CloudFormation plantillas de AWS para implementar la canalización de CI/CD y los recursos de AWS en las cuentas de destino.

Prácticas recomendadas

- Antes de empezar a modificar el conjunto de permisos y las plantillas de asignación, le recomendamos que planifique los conjuntos de permisos para su organización. Tenga en cuenta cuáles deben ser los permisos, a qué cuentas o unidades organizativas debe aplicarse el conjunto

de permisos y qué entidades principales (usuarios o grupos) del IAM Identity Center deberían verse afectados por el conjunto de permisos. Los nombres de los conjuntos de permisos, los ID de asociación y los tipos de entidad principal del IAM Identity Center no se pueden modificar tras la implementación.

- Cumpla con el principio de privilegio mínimo y conceda los permisos mínimos necesarios para llevar a cabo una tarea. Para obtener más información, consulte Otorgar privilegio mínimo y Prácticas recomendadas de seguridad en la documentación de IAM.

Epics

Planificar conjuntos de permisos y asignaciones

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	En un shell de bash, ingrese el siguiente comando: Esto clona el repositorio aws-iam-identity-center-pipeline desde. GitHub `git clone https://github.com/aws-samples/aws-iam-identity-center-pipeline.git`	DevOps ingeniero
Defina los conjuntos de permisos.	1. En el repositorio clonado, vaya a la carpeta `templates/permissionsets` y, a continuación, abra una de las plantillas disponibles. 2. En el parámetro `Name`, especifique un nombre para el conjunto de permisos. Este valor debe ser único y no se puede cambiar después de la implementación.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	3. En el parámetro `Description` , describa brevemente el conjunto de permisos, como por ejemplo su caso de uso. 4. En el parámetro `SessionDuration` , especifique el tiempo durante el que un usuario puede iniciar sesión en una cuenta de AWS. Utilice el formato de duración ISO-8601 (Wikipedia), por ejemplo, como `PT4H` durante 4 horas. Si no se define ningún valor, el valor predeterminado en IAM Identity Center es de 1 hora. 5. Personalice las políticas del conjunto de permisos. Todos los parámetros siguientes son opcionales y se pueden modificar después de la implementación. Debe usar al menos uno de los parámetros para definir las políticas del conjunto de permisos: • En el `ManagedPolicies` parámetro , introduzca los ARN de cualquier política	

Tarea	Descripción	Habilidades requeridas
	administrada de AWS que desee asignar. • En el parámetro `CustomerManagedPolicies`, introduzca los nombres de cualquier política administrada por el cliente que desee asignar. No utilice el ARN. • En el parámetro `PermissionBoundary`, haga lo siguiente para asignar un límite de permiso: • Si utiliza una política administrada de AWS como límite de permisos, en `PolicyType` introduzca `AWS`, y en `Policy` introduzca el ARN de la política. • Si utiliza una política administrada por el cliente como límite de permisos, en `PolicyType`, introduzca `Customer`, y en `Policy`, introduzca el nombre de la política. No utilice el ARN.	

Tarea	Descripción	Habilidades requeridas
	• En el parámetro `CustomPolicy` , defina cualquier política personalizada con formato JSON que desee asignar. Para obtener más información acerca de la estructura de la política de JSON, consulte Información general de las políticas de JSON. 6. Guarde y cierre la plantilla del conjunto de permisos. Le recomendamos que guarde el archivo con un nombre que coincida con el nombre del conjunto de permisos. 7. Repita este proceso para crear tantos conjuntos de permisos como necesite su organización y elimine las plantillas de muestra que no sean necesarias.	

Tarea	Descripción	Habilidades requeridas
Defina las asignaciones.	1. En el repositorio clonado, vaya a la carpeta `templates/assignments` y, a continuación, abra `iam-identitycenter-assigments.json`. En este archivo se describe cómo desea asignar los conjuntos de permisos a las cuentas o unidades organizativas de AWS. 2. En el parámetro `SID` introduzca un identificador para la asignación. Este valor debe ser único y no se puede modificar después de la implementación. 3. En el parámetro `Target`, defina las cuentas u organizaciones a las que desea aplicar el conjunto de permisos. Los valores válidos son los ID de cuenta, los ID de OU, los nombres de OU o `root`. `root` asigna el conjunto de permisos a todas las cuentas miembro de la organización, excluyendo la cuenta de administración. Introduzca los valores entre comillas dobles y separe los valores múltiples	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	con comas. Para obtener instrucciones sobre cómo encontrar los identific adores, consulte Visualiza ción de los detalles de una cuenta o Visualización de los detalles de una unidad organizativa. 4. En el parámetro `PrincipalType` , introduzca el tipo de entidad principal del IAM Identity Center que se verá afectada por el conjunto de permisos. Los valores válidos son `USER` o `GROUP`. Este valor no se puede modificar después de la implementación. 5. En el parámetro `PrincipalID` , introduzc a el nombre del usuario o grupo del almacén de identidades del IAM Identity Center al que afectará el conjunto de permisos. Este valor no se puede modificar después de la implement ación. 6. En el parámetro `PermissionSetName` introduzca el nombre del conjunto de permisos que desea asignar.	

Tarea	Descripción	Habilidades requeridas
	7. Repita los pasos del 2 al 6 para crear tantas asignaciones como necesite en este archivo. Normalmente, hay una asignación para cada conjunto de permisos. Elimine cualquier asignación de muestra que no sea necesaria. 8. Guarde y cierre el archivo `iam-identitycenter-assigments.json` .	

Implementación de los conjuntos de permisos y las asignaciones

Tarea	Descripción	Habilidades requeridas
Cargue los archivos en un bucket de S3.	1. Comprima el repositorio clonado en un archivo .zip. 2. Inicie sesión en la cuenta de administrador delegado del IAM Identity Center. 3. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3. 4. En el panel de navegación situado a la izquierda, elija Buckets. 5. Seleccione el bucket que desea utilizar para implementar esta solución.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	6. Cargue el archivo .zip en el bucket de destino de S3. Para obtener instrucciones, consulte Carga de objetos.	
Implemente los recursos en la cuenta de administrador delegado del IAM Identity Center.	1. En la cuenta de administrador delegado del IAM Identity Center, abra la CloudFormation consola en https://console.aws.amazon.com/cloudformation/. 2. Implemente la plantilla `iam-identitycenter-pipeline.yaml` . Asigne a la pila un nombre claro y descriptivo y actualice los parámetros según las instrucciones. Para obtener instrucciones, consulte Crear una pila en la CloudFormation documentación.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Implemente recursos en la cuenta de administración de AWS Organizations.	1. Inicie sesión en la cuenta administrativa de la organización. 2. Abra la CloudFormation consola en https://console.aws.amazon.com/cloudformation/. 3. En la barra de navegación, elija el nombre de la región de AWS que aparece. A continuación, elija la región `us-east-1` . Esta región es necesaria para que la `MoveAccount` EventBridge regla pueda detectar los CloudTrail eventos de AWS asociados a los cambios en la organización. 4. Implemente la plantilla `iam-identitycenter-organization` . Asigne a la pila un nombre claro y descriptivo y actualice los parámetros según las instrucciones. Para obtener instrucciones, consulte Crear una pila en la CloudFormation documentación.	DevOps ingeniero

Actualización de los conjuntos de permisos y las asignaciones

Tarea	Descripción	Habilidades requeridas
Actualice los conjuntos de permisos y las asignaciones.	Cuando la EventBridge regla de `MoveAccount` Amazon detecta modificaciones en las cuentas de la organizac ión, la canalización de CI/CD se inicia automáticamente y actualiza los conjuntos de permisos. Por ejemplo, si añade una cuenta a una unidad organizativa especific ada en el archivo JSON de asignaciones, a continuac ión la canalización de CI/ CD aplicará el conjunto de permisos a la nueva cuenta. Si desea modificar los conjuntos de permisos y las asignaciones implementados, actualice los archivos JSON y, a continuación, consérvelos en el CodeCommit repositor io de la cuenta de administr ador delegado del IAM Identity Center. Para obtener instrucciones, consulte Crear una confirmación en la CodeCommit documentación. Tenga en cuenta lo siguiente cuando utilice la canalizac ión de CI/CD para gestionar conjuntos de permisos y	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	asociaciones implementados anteriormente: • Si cambia el nombre de un conjunto de permisos, la canalización de CI/CD elimina el conjunto de permisos original y crea uno nuevo. • Esta canalización administra solo los conjuntos de permisos que tienen la etiqueta `SSOPipeline:true` . • Puede tener varios conjuntos de permisos y plantillas de asignación en la misma carpeta del repositorio. • Si elimina una plantilla, la canalización eliminará la asignación o el conjunto de permisos. • Si elimina un bloque JSON de una asignación completa, la canalización eliminará la asignación del IAM Identity Center. • No puede eliminar un conjunto de permisos asignado a una cuenta de AWS. En primer lugar, debe anular la asignación del conjunto de permisos.	

Solución de problemas

Problema	Solución
Errores de acceso denegado	Confirme que tiene los permisos necesarios para implementar las CloudFormation plantillas y los recursos definidos en ellas. Para obtener más información, consulte Controlar el acceso en la CloudFormation documentación.
Errores de canalización en la fase de validación	Este error se muestra si hay algún error en el conjunto de permisos o en las plantillas de asignación. 1. En CodeBuild, consulte los detalles de la compilación. 2. En el registro de compilación, busque el error de validación que proporciona más información sobre la causa del error de compilación. 3. Actualice el conjunto de permisos o las plantillas de asignación y, a continuación, consérvelos en el repositorio. 4. La canalización de CI/CD reinicia el proyecto. CodeBuild Supervise el estado para confirmar que se ha resuelto el error de validación.

Recursos relacionados

- Conjuntos de permisos (documentación del IAM Identity Center)

Administrar credenciales mediante AWS Secrets Manager

Documento creado por Durga Prasad Cheepuri (AWS)

Creado por: AWS	Entorno: PoC o piloto	Tecnologías: bases de datos, seguridad, identidad, cumplimiento
Servicios de AWS: AWS Secrets Manager		

Resumen

Este patrón le guía en el uso de AWS Secrets Manager para obtener de forma dinámica las credenciales de bases de datos de una aplicación Java Spring.

En el pasado, cuando creaba una aplicación personalizada que recuperaba información desde una base de datos, normalmente tenía que incrustar las credenciales (el secreto) para obtener acceso a la base de datos directamente en la aplicación. Cuando llegaba el momento de cambiar las credenciales, había que invertir tiempo en actualizar la aplicación para utilizar las nuevas credenciales y, a continuación, distribuir la aplicación actualizada. Si tenía varias aplicaciones que compartían credenciales y se olvidaba de actualizar una de ellas, la aplicación dejaba de funcionar. Debido a este riesgo, muchos usuarios decidían no rotar sus credenciales periódicamente, lo que finalmente sustituye un riesgo por otro.

Secrets Manager le permite reemplazar las credenciales codificadas en el código (incluidas contraseñas), con una llamada a la API para recuperar el secreto mediante programación. Esto ayuda a garantizar la integridad del secreto si alguien examina el código, dado que el secreto sencillamente no está allí. Además, puede configurar Secrets Manager para rotar el secreto automáticamente de acuerdo con una programación especificada. Esto le permite reemplazar secretos a largo plazo con secretos a corto plazo, lo que contribuye a reducir significativamente el riesgo. Para obtener más información, consulte la documentación de AWS Secrets Manager.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS con acceso a Secrets Manager
- Una aplicación de Java Spring

Arquitectura

Pila de tecnología de origen

- Una aplicación Java Spring con código que acceda a una base de datos, con credenciales de base de datos administradas desde el archivo application.properties.

Pila de tecnología de destino

- Una aplicación Java Spring con código que acceda a una base de datos, con credenciales de base de datos administradas en Secrets Manager. El archivo application.properties contiene los secretos de Secrets Manager.

Integración de Secrets Manager en una aplicación

Herramientas

- Secrets Manager: AWS Secrets Manager es un servicio de AWS que facilita la administración de los secretos. Los secretos pueden ser credenciales de base de datos, contraseñas, claves de API de terceros e incluso texto arbitrario. Puede almacenar y controlar el acceso a estos secretos de forma centralizada a través de la consola de Secrets Manager, la interfaz de la línea de comandos (CLI) de Secrets Manager y la API y los SDK de Secrets Manager.

Epics

Almacenar el secreto en Secrets Manager

Tarea	Descripción	Habilidades requeridas
Almacene las credenciales como un secreto en Secrets Manager.	Almacene las credenciales de Amazon Relational Database Service (Amazon RDS) u	Sys Admin

Tarea	Descripción	Habilidades requeridas
	otras credenciales de base de datos como un secreto en Secrets Manager; para ello, siga los pasos que se indican en Creating a secret (Crear un secreto) en la documentación de Secrets Manager.	
Establezca permisos para que la aplicación Spring acceda a Secrets Manager.	Establezca los permisos adecuados en función de cómo la aplicación Java Spring utilice Secrets Manager. Para controlar el acceso al secreto, cree una política basada en la información proporcionada en la documentación de Secrets Manager, en las secciones Using identity-based policies (IAM Policies) and ABAC for Secrets Manager (Usar políticas basadas en identidad [políticas de IAM] y ABAC para Secrets Manager) y Using resource-based policies for Secrets Manager (Usar políticas basadas en recursos para Secrets Manager). Siga los pasos de la sección Retrieving the secret value (Recuperar el valor del secreto) de la documentación de Secrets Manager.	Sys Admin

Actualizar la aplicación Spring

Tarea	Descripción	Habilidades requeridas
Agregue dependencias JAR para usar Secrets Manager.	Para obtener más detalles, consulte la sección Informaci ón adicional.	Desarrollador de Java
Agregue los detalles del secreto a la aplicación Spring.	Actualice el archivo applicati on.properties con el nombre del secreto, los puntos de conexión y la región de AWS. Para obtener ejemplos, consulte la sección Informaci ón adicional.	Desarrollador de Java
Actualice el código de recuperación de credenciales de base de datos en Java.	En la aplicación, actualice el código Java que obtiene las credenciales de base de datos para obtener esos detalles de Secrets Manager. Para ver un código de ejemplo, consulte la sección Información adicional.	Desarrollador de Java

Recursos relacionados

- Documentación de AWS Secrets Manager
- Using identity-based policies (IAM Policies) and ABAC for Secrets Manager (Usar políticas basadas en identidad [políticas de IAM] y ABAC para Secrets Manager)
- Using resource-based policies for Secrets Manager (Usar políticas basadas en recursos para Secrets Manager)
- Código de muestra

Información adicional

Adding JAR dependencies for using Secrets Manager (Agregar dependencias JAR para usar Secrets Manager)

Maven:

```
<groupId>com.amazonaws</groupId>
    <artifactId>aws-java-sdk-secretsmanager</artifactId>
    <version>1.11. 355 </version>
```

Gradle:

```
compile group: 'com.amazonaws', name: 'aws-java-sdk-secretsmanager', version:
 '1.11.355'
```

Updating the application.properties file with the details of the secret (Actualizar el archivo application.properties con los detalles del secreto)

```
spring.aws.secretsmanager.secretName=postgres-local
spring.aws.secretsmanager.endpoint=secretsmanager.us-east-1.amazonaws.com
spring.aws.secretsmanager.region=us-east-1
```

Updating the DB credentials retrieval code in Java (Actualizar el código de recuperación de credenciales de base de datos en Java.)

```
String  secretName  =  env.getProperty("spring.aws.secretsmanager.secretName");
String  endpoints  =  env.getProperty("spring.aws.secretsmanager.endpoint");
String  AWS Region  =  env.getProperty("spring.aws.secretsmanager.region");
AwsClientBuilder.EndpointConfiguration  config  =  new
  AwsClientBuilder.EndpointConfiguration(endpoints, AWS Region);
AWSSecretsManagerClientBuilder  clientBuilder  =
  AWSSecretsManagerClientBuilder.standard();
clientBuilder.setEndpointConfiguration(config);
AWSSecretsManager  client  =  clientBuilder.build();

ObjectMapper  objectMapper  =  new  ObjectMapper();

JsonNode  secretsJson  =  null;
```

```
ByteBuffer  binarySecretData;

GetSecretValueRequest  getSecretValueRequest  =  new
  GetSecretValueRequest().withSecretId(secretName);

GetSecretValueResult  getSecretValueResponse  =  null;

try  {
     getSecretValueResponse  =  client.getSecretValue(getSecretValueRequest);
    }

catch  (ResourceNotFoundException  e)  {
     log.error("The requested secret "  +  secretName  +  " was not found");
    }

catch  (InvalidRequestException  e)  {
     log.error("The request was invalid due to: "  +  e.getMessage());
     }

catch  (InvalidParameterException  e)  {
     log.error("The request had invalid params: "  +  e.getMessage());
     }
if  (getSecretValueResponse  ==  null)  {
     return  null;
     }  // Decrypted secret using the associated KMS key // Depending on whether the
 secret was a string or binary, one of these fields will be populated


String secret = getSecretValueResponse.getSecretString();

if (secret != null) {
     try {
                 secretsJson  =  objectMapper.readTree(secret);
           }

     catch  (IOException  e)  {
                 log.error("Exception while retrieving secret values: "  +
  e.getMessage());
           }
}

else  {
     log.error("The Secret String returned is null");
```

```
    return null;

    }
    String  host  =  secretsJson.get("host").textValue();
    String  port  =  secretsJson.get("port").textValue();
    String  dbname  =  secretsJson.get("dbname").textValue();
    String  username  =  secretsJson.get("username").textValue();
    String  password  =  secretsJson.get("password").textValue();
}
```

Supervisar los clústeres de Amazon EMR para comprobar el cifrado en tránsito en el momento del lanzamiento

Entorno: producción	Tecnologías: Análisis; macrodatos; nativo en la nube; seguridad, identidad, conformidad	Carga de trabajo: código abierto
Servicios de AWS: Amazon EMR; Amazon SNS; AWS; CloudTrail Amazon CloudWatch		

Resumen

Este patrón proporciona un control de seguridad que supervisa los clústeres de Amazon EMR en el momento del lanzamiento y envía una alerta si no se ha habilitado el cifrado en tránsito.

Amazon EMR es un servicio web que le facilita la ejecución de los marcos de trabajo de macrodatos, tales como Apache Hadoop, para procesar y analizar datos. Amazon EMR le permite procesar grandes cantidades de datos de forma rentable al ejecutar el mapeo y reducir los pasos en paralelo.

El cifrado de datos evita que usuarios no autorizados accedan o lean los datos en reposo o los datos en tránsito. Los datos en reposo se refieren a los datos que se almacenan en medios como un sistema de archivos local en cada nodo, el Sistema de archivos distribuido de Hadoop (HDFS) o el Sistema de archivos EMR (EMRFS) a través de Amazon Simple Storage Service (Amazon S3). Los datos en tránsito se refieren a los datos que viajan por la red y están en movimiento entre un trabajo y otro. El cifrado en tránsito admite características de cifrado de código abierto para Apache Spark, Apache TEZ, Apache Hadoop, Apache HBase y Presto. Para habilitar el cifrado, debe crear una configuración de seguridad desde la interfaz de la línea de comandos de AWS (AWS CLI), la consola o los SDK de AWS y especificando la configuración de cifrado de datos. Puede proporcionar los artefactos de cifrado para el cifrado en tránsito de estas dos maneras:

- Cargando un archivo comprimido de certificados en Amazon S3.
- Haciendo referencia a una clase Java personalizada que proporciona artefactos de cifrado.

El control de seguridad que se incluye en este patrón monitorea las llamadas a la API y genera un evento de Amazon CloudWatch Events en la acción RunJobFlow. El evento llama a una función de Lambda de AWS que ejecuta un script de Python. La función obtiene el ID del clúster de EMR de la entrada JSON del evento y realiza las siguientes comprobaciones para determinar si hay una infracción de seguridad:

- Comprueba si el clúster de EMR tiene una configuración de seguridad específica de Amazon EMR.
- Si el clúster tiene una configuración de seguridad, comprueba si el cifrado en tránsito está habilitado.
- Si el clúster no tiene una configuración de seguridad, envía una alerta a la dirección de correo electrónico que usted proporcione mediante Amazon Simple Notification Service (Amazon SNS). La notificación especifica el nombre del clúster de EMR, los detalles de la infracción, la información de la región y la cuenta de AWS y el ARN (nombre de recurso de Amazon) de AWS Lambda del que proviene la notificación.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Un bucket de S3 para cargar el código de Lambda que se proporciona con este patrón.
- Una dirección de correo electrónico en la que desee recibir las notificaciones de infracciones.
- El registro de Amazon EMR está habilitado para acceder a todos los registros de la API.

Limitaciones

- Este control de detección es regional y debe implementarse en cada región de AWS que desee supervisar.

Versiones de producto

- Amazon EMR versión 4.8.1 o posterior.

Arquitectura

Arquitectura de flujo de trabajo

Automatizar y escalar

- Si utiliza AWS Organizations, puede utilizar AWS Cloudformation StackSets para implementar la plantilla en varias cuentas que desee supervisar.

Herramientas

Servicios de AWS

- Amazon EMR: Amazon EMR es una plataforma de clúster administrada que simplifica la ejecución de los marcos de trabajo de macrodatos, tales como Apache Hadoop y Apache Spark en AWS para procesar y analizar grandes cantidades de datos. Mediante el uso de estos marcos de trabajo y proyectos de código abierto relacionados, puede procesar datos para fines de análisis y cargas de trabajo de inteligencia empresarial. Además, puede utilizar Amazon EMR para transformar y trasladar grandes cantidades de datos hacia y desde otros almacenes de datos y bases de datos de AWS, tales como Amazon S3 y Amazon DynamoDB.
- AWS Cloudformation: AWS le CloudFormation ayuda a modelar y configurar sus recursos de AWS, a aprovisionarlos de forma rápida y coherente y a gestionarlos durante todo su ciclo de vida. Facilita poder usar una plantilla para describir los recursos y sus dependencias, y lanzarlos y configurarlos juntos como una pila, en lugar de administrarlos de forma individual. Puede administrar y aprovisionar pilas en varias cuentas y regiones de AWS.
- AWS Cloudwatch Events: Amazon CloudWatch Events ofrece una transmisión casi en tiempo real de eventos del sistema que describen los cambios en los recursos de AWS. CloudWatch Events se da cuenta de los cambios operativos a medida que se producen y toma las medidas correctivas necesarias, mediante el envío de mensajes en respuesta al entorno, la activación de funciones, la realización de cambios y la recopilación de información sobre el estado.
- AWS Lambda: AWS Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo. Solo pagará por el tiempo de computación que consuma, no se aplican cargos cuando el código no se está ejecutando.
- AWS SNS – Amazon Simple Notification Service (Amazon SNS) coordina y administra el envío de mensajes entre los publicadores y los clientes, incluyendo los servidores web y las direcciones de correo electrónico. Los suscriptores reciben todos los mensajes publicados de los temas a los que están suscritos y todos los suscriptores de un tema reciben los mismos mensajes.

Código

Este patrón incluye un adjunto con dos archivos:

- `EMRInTransitEncryption.zip` es un archivo comprimido que incluye el control de seguridad (código de Lambda).
- `EMRInTransitEncryption.yml`es una CloudFormation plantilla que despliega el control de seguridad.

Consulte la sección Epics para obtener información sobre cómo usar estos archivos.

Epics

Implementar el control de seguridad

Tarea	Descripción	Habilidades requeridas
Cargue el código en un bucket de S3.	Cree un bucket de S3 nuevo o utilice un bucket de S3 ya existente para cargar el archivo adjunto `EMRInTransitEncryption.zip` (código de Lambda). Este depósito debe estar en la misma región de AWS que la CloudFormation plantilla y los recursos que desea evaluar.	Arquitecto de la nube
Implemente la CloudFormation plantilla.	Abra la consola de Cloudformation en la misma región de AWS que el bucket de S3 e implemente el archivo `EMRInTransitEncryption.yml` que se incluye en el archivo adjunto. En la siguiente Epic, proporcione los valores de los parámetros.	Arquitecto de la nube,

Complete los parámetros de la CloudFormation plantilla

Tarea	Descripción	Habilidades requeridas
Proporcione el nombre del bucket de S3.	Escriba el nombre del bucket de S3 que ha creado o seleccionado en la primera Epic. Este bucket de S3 contiene el archivo.zip del código Lambda y debe estar en la misma región de AWS que CloudFormation la plantilla y el recurso que se van a evaluar.	Arquitecto de la nube
Proporcione la clave de S3.	Especifique la ubicación del archivo .zip de código de Lambda en su bucket de S3, sin barras diagonales iniciales (por ejemplo, `EMRInTransitEncryption.zip` o `controls/EMRInTransitEncryption.zip`).	Arquitecto de la nube
Proporcione una dirección de correo electrónico.	Especifique una dirección de correo electrónico activa en la que desee recibir notificaciones de infracciones.	Arquitecto de la nube
Especifique un nivel de registro.	Especifique el nivel de registro y la verbosidad de los registros de Lambda. `Info` designa mensajes informativos detallados sobre el progreso de la aplicación y solo debe usarse para la depuración. `Error` designa	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	los eventos de error que aún podrían permitir que la aplicación siguiera ejecutándose. `Warning` designa situaciones potencialmente dañinas.	

Confirmar la suscripción

Tarea	Descripción	Habilidades requeridas
Confirme la suscripción de correo electrónico.	Cuando la CloudFormation plantilla se implementa correctamente, envía un mensaje de correo electrónico de suscripción a la dirección de correo electrónico que proporcionó. Debe confirmar esta suscripción de correo electrónico para recibir notificaciones.	Arquitecto de la nube

Recursos relacionados

- Creación de una pila en la CloudFormation consola de AWS (CloudFormation documentación de AWS)
- Opciones de cifrado (documentación de Amazon EMR)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Supervise ElastiCache los clústeres de Amazon para comprobar el cifrado en reposo

Entorno: producción	Tecnologías: seguridad, identidad, conformidad; bases de datos; infraestructura; nativo en la nube	Carga de trabajo: código abierto
Servicios de AWS: Amazon SNS; Amazon; Amazon CloudWatch ElastiCache		

Resumen

Amazon ElastiCache es un servicio de Amazon Web Services (AWS) que proporciona una solución de almacenamiento en caché rentable, escalable y de alto rendimiento para distribuir un almacén de datos en memoria o un entorno de caché en la nube. Recupera datos de almacenes de datos en memoria de alto rendimiento y baja latencia. Esta funcionalidad lo convierte en una opción popular para casos de uso en tiempo real, como el almacenamiento en caché, los almacenes de sesiones, los juegos, los servicios geoespaciales, los análisis en tiempo real y las colas. ElastiCache ofrece los almacenes de datos de Redis y Memcached, los cuales ofrecen tiempos de respuesta inferiores a un milisegundo.

El cifrado de datos ayuda a evitar que usuarios no autorizados lean datos confidenciales disponibles en sus clústeres Redis y sus sistemas de almacenamiento en caché asociados. Esto incluye los datos guardados en medios persistentes, conocidos como datos en reposo y datos que pueden ser interceptados cuando recorren la red entre los clientes y los servidores de caché, conocidos como datos en tránsito.

Puede habilitar el cifrado en reposo ElastiCache para Redis al crear un grupo de replicación configurando el parámetro en true. AtRestEncryptionEnabled Cuando este parámetro está habilitado, cifra el disco durante las operaciones de sincronización, copia de seguridad e intercambio, y cifra las copias de seguridad almacenadas en Amazon Simple Storage Service (Amazon S3). No puede habilitar el cifrado en reposo en un grupo de reproducción existente. Cuando cree un grupo de replicación, puede activar la encriptación en reposo de estas dos formas:

- Al seleccionar la opción Predeterminado, que utiliza el cifrado administrado por el servicio en reposo.
- Mediante una clave administrada por el cliente y proporcionando el ID de clave o nombre de recurso de Amazon (ARN) de AWS Key Management Service (AWS KMS).

Este patrón proporciona un control de seguridad que supervisa las llamadas a la API y genera un evento de Amazon CloudWatch Events en la operación del CreateReplicationgrupo. Este evento llama a una función de Lambda de AWS que ejecuta un script de Python. La función obtiene el ID del grupo de replicación de la entrada JSON del evento y realiza las siguientes comprobaciones para determinar si hay alguna infracción de seguridad:

- Comprueba si la AtRestEncryptionEnabledclave existe.
- Si AtRestEncryptionEnabledexiste, comprueba el valor para ver si es verdadero.
- Si el AtRestEncryptionEnabledvalor se establece en false, establece una variable que rastrea las infracciones y envía un mensaje de infracción a la dirección de correo electrónico que usted proporcione, mediante una notificación de Amazon Simple Notification Service (Amazon SNS).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Un bucket de S3 para cargar el código de Lambda proporcionado.
- Una dirección de correo electrónico en la que desee recibir las notificaciones de infracciones.
- ElastiCache registro activado, para acceder a todos los registros de la API.

Limitaciones

- Este control de detección es regional y debe implementarse en cada región de AWS que desee supervisar.
- El control es compatible con los grupos de replicación que se ejecutan en una nube privada virtual (VPC).
- El control admite grupos de replicación que ejecutan los siguientes tipos de nodos:
  - R5, R4, R3

- M5, M4, M3
- T3, T2

Versiones de producto

- ElastiCache para Redis versión 3.2.6 o posterior

Arquitectura

Arquitectura de flujo de trabajo

Automatizar y escalar

- Si utiliza AWS Organizations, puede utilizar AWS Cloudformation StackSets para implementar esta plantilla en varias cuentas que desee supervisar.

Herramientas

Servicios de AWS

- Amazon ElastiCache: Amazon ElastiCache facilita la configuración, la administración y el escalado de los entornos de caché en memoria distribuidos en la nube de AWS. Proporciona una caché en memoria rentable, redimensionable y de alto rendimiento, a la vez que elimina la complejidad asociada a la implementación y la administración de un entorno de caché distribuida. ElastiCache funciona con los motores Redis y Memcached.
- AWS CloudFormation: AWS le CloudFormation ayuda a modelar y configurar sus recursos de AWS, a aprovisionarlos de forma rápida y coherente y a gestionarlos durante todo su ciclo de vida. Facilita poder usar una plantilla para describir los recursos y sus dependencias, y lanzarlos y configurarlos juntos como una pila, en lugar de administrarlos de forma individual. Puede administrar y aprovisionar pilas en varias cuentas y regiones de AWS.
- AWS Cloudwatch Events: Amazon CloudWatch Events ofrece una transmisión casi en tiempo real de eventos del sistema que describen los cambios en los recursos de AWS. CloudWatch Events se da cuenta de los cambios operativos a medida que se producen y toma las medidas correctivas necesarias, mediante el envío de mensajes en respuesta al entorno, la activación de funciones, la realización de cambios y la recopilación de información sobre el estado.

- AWS Lambda: AWS Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo. Solo pagará por el tiempo de computación que consuma, no se aplican cargos cuando el código no se está ejecutando.
- Amazon SNS – Amazon Simple Notification Service (Amazon SNS) coordina y gestiona el envío de mensajes entre publicadores y clientes, incluyendo servidores web y direcciones de correo electrónico. Los suscriptores reciben todos los mensajes publicados de los temas a los que están suscritos y todos los suscriptores de un tema reciben los mismos mensajes.

Código

Este patrón incluye un adjunto con dos archivos:

- `ElasticCache-EncryptionAtRest.zip` es un archivo comprimido que incluye el control de seguridad (código de Lambda).
- `elasticache_encryption_at_rest.yml`es una CloudFormation plantilla que despliega el control de seguridad.

Consulte la sección Epics para obtener información sobre cómo usar estos archivos.

Epics

Implementar el control de seguridad

Tarea	Descripción	Habilidades requeridas
Cargue el código en un bucket de S3.	Cree un bucket de S3 nuevo o utilice un bucket de S3 ya existente para cargar el archivo adjunto `ElastiCache-EncryptionAtRest.zip` (código de Lambda). Este bucket debe estar en la misma región de AWS que los recursos que desea evaluar.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation plantilla.	Abra la consola de Cloudformation en la misma región de AWS que el bucket de S3 e implemente el archivo `elasticache_encryption_at_rest.yml` que se incluye en el archivo adjunto. En la siguiente Epic, proporcione los valores de los parámetros.	Arquitecto de la nube

Complete los parámetros de la CloudFormation plantilla

Tarea	Descripción	Habilidades requeridas
Proporcione el nombre del bucket de S3.	Escriba el nombre del bucket de S3 que ha creado o seleccionado en la primera Epic. Este bucket de S3 contiene el archivo.zip del código Lambda y debe estar en la misma región de AWS que CloudFormation la plantilla y el recurso que se van a evaluar.	Arquitecto de la nube
Proporcione la clave de S3.	Proporcione la ubicación del archivo .zip del código de Lambda en su bucket de S3, sin barras diagonales iniciales (por ejemplo, `ElasticCache-EncryptionAtRest.zip` o `controls/`	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	`ElasticCache-EncryptionAtRest.zip`).	
Proporcione una dirección de correo electrónico.	Proporcione una dirección de correo electrónico activa en la que desee recibir notificaciones de infracciones.	Arquitecto de la nube
Especifique un nivel de registro.	Especifique el nivel de registro y el detalle. `Info` designa mensajes informativos detallados sobre el progreso de la aplicación y solo debe usarse para la depuración. `Error` designa los eventos de error que aún podrían permitir que la aplicación siguiera ejecutándose. `Warning` designa situaciones potencialmente dañinas.	Arquitecto de la nube

Confirmar la suscripción

Tarea	Descripción	Habilidades requeridas
Confirme la suscripción de correo electrónico.	Cuando la CloudFormation plantilla se implementa correctamente, envía un mensaje de correo electrónico de suscripción a la dirección de correo electrónico que proporcionó. Debe confirmar esta suscripción de correo	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	electrónico para recibir notificaciones.	

Recursos relacionados

- Creación de una pila en la CloudFormation consola de AWS (CloudFormation documentación de AWS)
- Cifrado en reposo ElastiCache para Redis (documentación de Amazon ElastiCache)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Supervisar los pares de claves de instancias EC2 mediante AWS Config

Entorno: producción	Tecnologías: seguridad, identidad, conformidad	Servicios de AWS: Amazon SNS; AWS Config; AWS Lambda

Resumen

Al lanzar una instancia de Amazon Elastic Compute Cloud (Amazon EC2) en la nube de Amazon Web Services (AWS), se recomienda crear un par de claves o utilizar uno existente para conectarse a la instancia. El par de claves, que consta de una clave pública almacenada en la instancia y una clave privada que se proporciona al usuario, permite el acceso seguro a través de Secure Shell (SSH) a la instancia y evita el uso de contraseñas. Sin embargo, a veces los usuarios pueden lanzar instancias de forma inadvertida sin asociarles un par de claves. Como los pares de claves solo se pueden asignar durante el lanzamiento de la instancia, es importante identificar y marcar rápidamente como no conformes aquellas instancias lanzadas sin pares de claves. Esto resulta especialmente útil cuando se trabaja en cuentas o entornos que exigen el uso de pares de claves para acceder a las instancias.

Este patrón describe cómo crear una regla personalizada en AWS Config para supervisar los pares de claves de instancias de EC2. Cuando las instancias se identifican como no conformes, se envía una alerta mediante las notificaciones del Amazon Simple Notification Service (Amazon SNS) iniciadas a través de un evento de Amazon. EventBridge

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- AWS Config habilitado para la región de AWS que va a supervisar y configurado para registrar todos los recursos de AWS

Limitaciones

- Esta solución es específica de cada región. Todos los recursos deben crearse en la misma región de AWS.

Arquitectura

Pila de tecnología de destino

- AWS Config
- Amazon EventBridge
- AWS Lambda
- Amazon SNS

Arquitectura de destino

1. AWS Config inicia la regla.
2. La regla invoca la función de Lambda para evaluar la conformidad de las instancias EC2.
3. La función de Lambda envía el estado de conformidad actualizado a AWS Config.
4. AWS Config envía un evento a EventBridge.
5. EventBridge publica notificaciones de cambios de conformidad en un tema de SNS.
6. Amazon SNS envía una alerta por correo electrónico.

Automatizar y escalar

La solución puede supervisar cualquier número de instancias de EC2 en una región.

Herramientas

Herramientas

- AWS Config: AWS Config es un servicio que permite evaluar y auditar las configuraciones de los recursos de AWS. AWS Config supervisa de forma continua y registra las configuraciones de los recursos de AWS y permite automatizar la evaluación de las configuraciones registradas con las configuraciones deseadas.

- Amazon EventBridge: Amazon EventBridge es un servicio de bus de eventos sin servidor para conectar sus aplicaciones con datos de diversas fuentes.
- AWS Lambda: AWS Lambda es un servicio de computación sin servidor que permite ejecutar código sin aprovisionar ni administrar servidores, crear una lógica de escalado de clústeres adaptada a las cargas de trabajo, mantener las integraciones de eventos o gestionar los tiempos de ejecución.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) es un servicio de mensajería totalmente gestionado para la comunicación (A2A) y (application-to-application A2P). application-to-person

Código

Se incluye en los documentos adjuntos el código de la función de Lambda.

Epics

Crear una función de Lambda para evaluar la conformidad de Amazon EC2

Tarea	Descripción	Habilidades requeridas
Cree un rol de AWS Identity and Access Management (IAM) para Lambda.	En la consola de administración de AWS, seleccione IAM y, a continuación, cree el rol, utilizando Lambda como entidad de confianza y añadiendo los permisos `AmazonEventBridgeFullAccess` y `AWSConfigRulesExecutionRole` permisos. Para obtener más información, consulte la documentación de AWS.	DevOps
Crear e implementar la función de Lambda.	1. En la consola Lambda, cree una función con Author from scratch con Python 3.6 como motor de ejecución	DevOps

Tarea	Descripción	Habilidades requeridas
	y el rol de IAM creado anteriormente. Anote el nombre de recurso de Amazon (ARN). 2. En la pestaña Code, seleccione `lambda_function.py` y pegue el código adjunto a este patrón. 3. Para guardar los cambios, seleccione Deploy (Implementar).	

Crear una regla de AWS Config personalizada

Tarea	Descripción	Habilidades requeridas
Agregue una regla de AWS Config personalizada.	En la consola de AWS Config, agregue una regla personalizada con la configuración siguiente: • ARN: El ARN de la función de Lambda creada anteriormente • Tipo de disparador: cambios de configuración • Alcance de los cambios: recursos • Tipo de recurso: instancia de Amazon EC2	DevOps

Tarea	Descripción	Habilidades requeridas
	Para obtener más información, consulte la documentación de AWS.	

Configurar las notificaciones por correo electrónico cuando se detecte un evento de cambio de conformidad

Tarea	Descripción	Habilidades requeridas
Para crear un tema de SNS y una suscripción.	En la consola de Amazon SNS, cree un tema con el tipo Standard (Estándar) y, a continuación, cree una suscripción con Email como protocolo. Cuando reciba el mensaje de confirmación por correo electrónico, seleccione el enlace para confirmar la suscripción. Para obtener más información, consulte la documentación de AWS.	DevOps
Cree una EventBridge regla para iniciar las notificaciones de Amazon SNS.	En la EventBridge consola, cree una regla con los siguientes ajustes: • Nombre del servicio: AWS Config • Tipo de evento: Config Rules Compliance Change	DevOps

Tarea	Descripción	Habilidades requeridas
	(cambio de conformidad de las reglas de configuración) • Tipo de mensaje: tipos de mensajes específicos, ComplianceChangeNotification • Nombre de regla específico: el nombre de la regla de AWS Config creada anteriormente • Destino: tema de SNS, el tema que creó anteriormente Para obtener más información, consulte la documentación de AWS.	

Verificar la regla y las notificaciones

Tarea	Descripción	Habilidades requeridas
Cree instancias de EC2.	Cree dos instancias de EC2 de cualquier tipo, asócieles un par de claves y cree una instancia EC2 sin un par de claves.	DevOps
Verifique la regla.	1. En la consola de AWS Config, en la página Rules (Reglas), seleccione la regla.	DevOps

Tarea	Descripción	Habilidades requeridas
	2. Para ver las instancias de EC2 conformes y no conformes, cambie Resources in scope (Recursos del ámbito de aplicación) a All (Todos). Compruebe que dos instancias estén listadas como conformes y que una instancia esté listada como no conforme. 3. Espere a recibir una notificación por correo electrónico de Amazon SNS relativa al estado de conformidad de las instancias de EC2.	

Recursos relacionados

- Creación de un rol para delegar permisos a un servicio de AWS
- Creating a custom rule in AWS Config (Crear una regla personalizada en AWS Config)
- Creating an Amazon SNS topic (Crear un tema de Amazon SNS)
- Subscribing to an Amazon SNS topic (Suscribirse a un tema de Amazon SNS)
- Crear una regla en Amazon EventBridge

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Supervise ElastiCache los clústeres para grupos de seguridad

Documento creado por Susanne Kangnoh (AWS) y Archit Mathur (AWS)

Entorno: producción	Tecnologías: seguridad, identidad, cumplimiento; bases de datos; infraestructura; nativo en la nube	Servicios de AWS: Amazon SNS; AWS; CloudTrail Amazon; Amazon CloudWatch ElastiCache

Resumen

Amazon ElastiCache es un servicio de Amazon Web Services (AWS) que proporciona una solución de almacenamiento en caché rentable, escalable y de alto rendimiento para distribuir un almacén de datos en memoria o un entorno de caché en la nube. Recupera datos de almacenes de datos en memoria de alto rendimiento y baja latencia. Esta funcionalidad lo convierte en una opción popular para casos de uso en tiempo real, como el almacenamiento en caché, los almacenes de sesiones, los juegos, los servicios geoespaciales, los análisis en tiempo real y las colas. ElastiCache ofrece los almacenes de datos de Redis y Memcached, los cuales ofrecen tiempos de respuesta inferiores a un milisegundo.

Un grupo de seguridad actúa como un firewall virtual para sus ElastiCache instancias al controlar el tráfico entrante y saliente. Los grupos de seguridad actúan en el nivel de la instancia, no en el de la subred. Para cada grupo de seguridad, es necesario añadir un conjunto de reglas que controla el tráfico entrante a las instancias, así como un conjunto de reglas distinto que controla el tráfico saliente. Puede especificar reglas de permiso, pero no reglas de denegación.

Este patrón proporciona un control de seguridad que supervisa las llamadas a la API y genera un evento de Amazon CloudWatch Events en las ModifyReplicationGroupoperaciones CreateReplicationGroupCreateCacheClusterModifyCacheCluster,, y. El evento llama a una función de AWS Lambda, que ejecuta un script de Python. La función obtiene el ID del grupo de replicación de la entrada JSON del evento y realiza las siguientes comprobaciones para determinar si hay alguna infracción de seguridad:

- Comprueba si el grupo de seguridad del clúster coincide con el grupo de seguridad que está configurado en la función de Lambda.

- Si el grupo de seguridad del clúster no coincide, la función envía un mensaje de infracción a la dirección de correo electrónico proporcionada, mediante una notificación de Amazon Simple Notification Service (Amazon SNS).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Un bucket de S3 para cargar el código Lambda.
- Una dirección de correo electrónico activa en la que recibir las notificaciones de infracciones.
- ElastiCache registro activado, para acceder a todos los registros de la API.

Limitaciones

- Este control de detección es regional, por lo que debe implementarse en cada región de AWS que se supervise.
- El control es compatible con los grupos de replicación que se ejecutan en una nube privada virtual (VPC).

Arquitectura

Arquitectura de flujo de trabajo

Automatizar y escalar

- Si utiliza AWS Organizations, puede utilizar AWS Cloudformation StackSets para implementar esta plantilla en varias cuentas que desee supervisar.

Herramientas

Servicios de AWS

- Amazon ElastiCache facilita la configuración, la administración y el escalado de los entornos de caché en memoria distribuidos en la nube de AWS. Proporciona una caché en memoria

rentable, redimensionable y de alto rendimiento, a la vez que elimina la complejidad asociada a la implementación y la administración de un entorno de caché distribuida. ElastiCache funciona con los motores Redis y Memcached.

- AWS le CloudFormation ayuda a modelar y configurar sus recursos de AWS, a aprovisionarlos de forma rápida y coherente y a gestionarlos durante todo su ciclo de vida. Facilita poder usar una plantilla para describir los recursos y sus dependencias, y lanzarlos y configurarlos juntos como una pila, en lugar de administrarlos de forma individual. Puede administrar y aprovisionar pilas en varias cuentas y regiones de AWS.
- AWS Cloudwatch Events ofrece una transmisión casi en tiempo real de los eventos del sistema que describen los cambios en los recursos de AWS. CloudWatch Events se percata de los cambios operativos a medida que se producen y toma las medidas correctivas necesarias, mediante el envío de mensajes en respuesta al entorno, la activación de funciones, la introducción de cambios y la recopilación de información sobre el estado.
- AWS Lambda es un servicio informático que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta el código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo. Solo pagará por el tiempo de computación que consuma, no se aplican cargos cuando el código no se está ejecutando.
- Amazon Simple Notification Service (Amazon SNS) coordina y gestiona el envío de mensajes entre publicadores y clientes, incluidos servidores web y direcciones de correo electrónico. Los suscriptores reciben todos los mensajes publicados de los temas a los que están suscritos y todos los suscriptores de un tema reciben los mismos mensajes.

Código

Este patrón incluye un adjunto con dos archivos:

- `ElastiCacheAllowedSecurityGroup.zip` es un archivo comprimido que incluye el control de seguridad (código Lambda).
- `ElastiCacheAllowedSecurityGroup.yml`es una CloudFormation plantilla que despliega el control de seguridad.

Consulte la sección Epics para obtener información sobre cómo usar estos archivos.

Epics

Implementar el control de seguridad

Tarea	Descripción	Habilidades requeridas
Cargue el código en un bucket de S3.	Cree un bucket de S3 nuevo o utilice un bucket de S3 ya existente para cargar el archivo adjunto `ElastiCacheAllowedSecurityGroup.zip` (código Lambda). Este bucket debe estar en la misma región de AWS que los recursos que desea evaluar.	Arquitecto de la nube
Implemente la CloudFormation plantilla.	Abra la consola de Cloudformation en la misma región de AWS que el bucket de S3 e implemente el archivo `ElastiCacheAllowedSecurityControl.yml` que se incluye en el archivo adjunto. En la siguiente Epic, proporcione los valores de los parámetros.	Arquitecto de la nube

Complete los parámetros de la CloudFormation plantilla

Tarea	Descripción	Habilidades requeridas
Proporcione el nombre del bucket de S3.	Escriba el nombre del bucket de S3 que ha creado o seleccionado en la primera Epic. Este bucket de S3 contiene el archivo.zip del código Lambda y debe	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	estar en la misma región de AWS que CloudFormation la plantilla y el recurso que se van a evaluar.	
Proporcione la clave de S3.	Proporcione la ubicación del archivo .zip de código Lambda del bucket de S3, sin barras diagonales iniciales (por ejemplo, `ElasticCacheAllowedSecurityGroup.zip` o `controls/ElasticCacheAllowedSecurityGroup.zip`).	Arquitecto de la nube
Proporcione una dirección de correo electrónico.	La dirección de correo electrónico en la que desee recibir la notificaciones de infracciones.	Arquitecto de la nube
Especifique un nivel de registro.	Especifique el nivel de registro y el detalle. `Info` designa mensajes informativos detallados sobre el progreso de la aplicación y solo debe usarse para la depuración. `Error` designa los eventos de error que aún podrían permitir que la aplicación siguiera ejecutándose. `Warning` designa situaciones potencialmente dañinas.	Arquitecto de la nube

Confirmar la suscripción

Tarea	Descripción	Habilidades requeridas
Confirme la suscripción de correo electrónico.	Cuando la CloudFormation plantilla se implementa correctamente, envía un mensaje de correo electrónico de suscripción a la dirección de correo electrónico que proporcionó. Debe confirmar esta suscripción de correo electrónico para comenzar a recibir notificaciones.	Arquitecto de la nube

Recursos relacionados

- Creación de una pila en la CloudFormation consola de AWS (CloudFormation documentación de AWS)
- Amazon VPC y ElastiCache seguridad (documentación de Amazon ElastiCache for Redis)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Supervisar la actividad del usuario raíz de IAM

Creado por Mostefa Brougui (AWS)

Repositorio de código: aws-iam-root-user-activity-monitor	Entorno: PoC o piloto	Tecnologías: seguridad, identidad, conformidad; administración y gobernanza
Carga de trabajo: todas las demás cargas de trabajo	Servicios de AWS: Amazon EventBridge; AWS Lambda; Amazon SNS; AWS Identity and Access Management	

Resumen

Cada cuenta de Amazon Web Services (AWS) tiene un usuario raíz. Como práctica de seguridad recomendada para AWS Identity and Access Management (IAM), se aconseja utilizar el usuario raíz para realizar las tareas que solo este puede llevar a cabo. Para ver la lista completa, consulte Tareas que requieren credenciales de usuario raíz en Guía de referencia de administración de la cuenta de AWS. Como el usuario raíz tiene acceso absoluto a todos los recursos e información de facturación de AWS, recomendamos que no se utilice esta cuenta y que se supervise para detectar cualquier actividad, ya que podría indicar que las credenciales del usuario raíz se han visto comprometidas.

Con este patrón, se configura una arquitectura basada en eventos que supervisa al usuario raíz de IAM. Este patrón configura una hub-and-spoke solución que monitorea varias cuentas de AWS, las cuentas radiales, y centraliza la administración y los informes en una sola cuenta, la cuenta hub.

Cuando se utilizan las credenciales del usuario raíz de IAM, Amazon CloudWatch y AWS CloudTrail registran la actividad en el registro y en el registro, respectivamente. En la cuenta radial, una EventBridge regla de Amazon envía el evento al bus de eventos central de la cuenta hub. En la cuenta hub, una EventBridge regla envía el evento a una función de AWS Lambda. La función utiliza un tema de Amazon Simple Notification Service (Amazon SNS) que notifica la actividad del usuario raíz.

En este patrón, se utiliza una CloudFormation plantilla de AWS para implementar los servicios de supervisión y gestión de eventos en las cuentas radiales. Utiliza una plantilla de HashiCorp Terraform para implementar los servicios de notificación y gestión de eventos en la cuenta central.

Requisitos previos y limitaciones

Requisitos previos

1. Permisos para implementar recursos de AWS en el entorno de AWS.
2. Permisos para implementar conjuntos de pilas CloudFormation . Para obtener más información, consulte Requisitos previos para las operaciones de conjuntos de pilas (CloudFormation documentación).
3. Terraform instalado y listo para su uso. Para obtener más información, consulte Introducción - AWS (documentación de Terraform).
4. Un registro de seguimiento existente en cada cuenta spoke. Para obtener más información, consulte Introducción a AWS CloudTrail (CloudTrail documentación).
5. La ruta está configurada para enviar eventos a CloudWatch Logs. Para obtener más información, consulte Enviar eventos a CloudWatch los registros (CloudTrail documentación).
6. AWS Organizations debe administrar las cuentas hub y spoke.

Arquitectura

En el diagrama siguiente se muestran los componentes básicos de la implementación.

1. Cuando se utilizan las credenciales del usuario raíz de IAM, CloudWatch CloudTrail registre la actividad en el registro y en el registro, respectivamente.
2. En la cuenta radial, una EventBridge regla envía el evento al bus de eventos central de la cuenta central.
3. En la cuenta hub, una EventBridge regla envía el evento a una función Lambda.
4. La función de Lambda utiliza un tema de Amazon SNS que notifica la actividad del usuario raíz.

Herramientas

Servicios de AWS

- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.

- AWS le CloudTrail ayuda a auditar la gobernanza, el cumplimiento y el riesgo operativo de su cuenta de AWS.
- Amazon CloudWatch Logs le ayuda a centralizar los registros de todos sus sistemas, aplicaciones y servicios de AWS para que pueda supervisarlos y archivarlos de forma segura.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, las funciones de Lambda de AWS, los puntos de conexión de invocación HTTP que utilizan destinos de API o los buses de eventos de otras cuentas de AWS.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.

Otras herramientas y servicios

- Terraform es una aplicación de CLI para aprovisionar y administrar la infraestructura y los recursos de la nube mediante el uso de código, en forma de archivos de configuración.

Repositorio de código

El código fuente y las plantillas de este patrón están disponibles en un GitHub repositorio. Este patrón proporciona dos plantillas:

- Una plantilla de Terraform que contiene los recursos que se despliegan en la cuenta hub
- Una CloudFormation plantilla que se implementa como una instancia de conjunto de pilas en las cuentas de Spoke

El repositorio tiene la estructura siguiente.

```
.
|__README.md
```

```
|__spoke-stackset.yaml
|__hub.tf
|__root-activity-monitor-module
    |__main.tf  # contains Terraform code to deploy resources in the Hub account
    |__iam      # contains IAM policies JSON files
        |__ lambda-assume-policy.json          # contains trust policy of the IAM role
used by the Lambda function
        |__ lambda-policy.json                 # contains the IAM policy attached to
the IAM role used by the Lambda function
    |__outputs  # contains Lambda function zip code
```

La sección Epics proporciona step-by-step instrucciones para implementar las plantillas.

Epics

Implementar recursos en la cuenta hub

Tarea	Descripción	Habilidades requeridas
Clone el repositorio de código de muestra.	1. Abra el repositorio AWS IAM Root User Activity Monitor. 2. En la pestaña Code (Código), situada encima de la lista de archivos, seleccione Code y, a continuación, copie la URL HTTPS. 3. En una interfaz de la línea de comandos, cambie el directorio de trabajo a la ubicación en la que desee almacenar los archivos de muestra. 4. Escriba el siguiente comando: `git clone <repoURL>`	AWS general

Tarea	Descripción	Habilidades requeridas
Actualice la plantilla de Terraform.	1. Recupere el ID de su organización. Para obtener instrucciones, consulte Viewing the details of an organization from the management account (Ver detalles de una organización desde la cuenta de administración) (documentación de AWS Organizations). 2. En el repositorio clonado, abra `hub.tf`. 3. Actualice lo siguiente con los valores adecuados para su entorno: • `OrganizationId` : Agregue el ID de su organización. • `SNSTopicName` : Agregue el nombre del tema de Amazon SNS. • `SNSSubscriptions` : Agregue el correo electrónico al que deben enviarse las notificaciones de Amazon SNS. • `Region`: Agregue el código de región de AWS en el que va a implementar los recursos. Por ejemplo, `eu-west-1` .	AWS general

Tarea	Descripción	Habilidades requeridas
	• `Tags`: Agregue sus etiquetas. Para obtener más información, consulte Etiquetado de recursos de AWS (Referencia general de AWS). 4. Guarde y cierre el archivo `hub.tf`.	
Implemente los recursos en la cuenta hub de AWS.	1. En la interfaz de la línea de comandos de Terraform, vaya hasta la carpeta raíz del repositorio clonado e ingrese el comando siguiente. `terraform init && terraform plan` 2. Revise la salida y confirme que desea crear los recursos descritos. 3. Escriba el siguiente comando. `terraform apply` 4. Cuando se le solicite, especifique `yes` para confirmar la implement ación.	AWS general

Implementar recursos en sus cuentas spoke

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation plantilla.	1. Inicie sesión en la consola de administración de AWS y abra la consola de CloudFormation . 2. En el panel de navegación, seleccione StackSets. 3. En la parte superior de la StackSetspágina, seleccion a Crear StackSet. 4. En Permisos, selecciona Permisos gestionados por el servicio. CloudFormation configura automáticamente los permisos necesarios para realizar la implement ación en las cuentas de destino administradas por AWS Organizations. 5. En Requisito previo - Preparación de la plantilla , seleccione Template is ready (La plantilla está lista). 6. En Especificar plantilla , seleccione Cargar un archivo de plantilla. 7. Seleccione Choose file (Elegir archivo) y, a continuación, en el repositor io clonado, seleccione	AWS general

Tarea	Descripción	Habilidades requeridas
	`spoke-stackset.yaml` . 8. Seleccione Siguiente. 9. En la página Especificar StackSet detalles, introduzca un nombre para el conjunto de pilas. 10. En Parameters, especifique el ID de cuenta de la cuenta hub y, a continuación, seleccione Next (Siguiente). 11. En la página Configurar StackSet opciones, en Etiquetas, añada sus etiquetas. 12. En Execution configuration (Configuración de ejecución), seleccione Inactive y, a continuación, selecciona Next (Siguiente). 13. En la página Cómo establecer opciones de implementación, especifique las unidades organizativas y las regiones en las que desea implementar el conjunto de pilas y, a continuación, seleccione Siguiente. 14. En la página de revisión, seleccione Acepto que AWS CloudFormation podría crear recursos de	

Tarea	Descripción	Habilidades requeridas
	IAM y, a continuación, elija Enviar. CloudFormation comienza a implementar su conjunto de pilas. Para obtener más informaci ón e instrucciones, consulte Crear un conjunto de pilas (CloudFormation documenta ción).	

(Opcional) Probar las notificaciones

Tarea	Descripción	Habilidades requeridas
Utilice las credenciales de usuario raíz.	1. Inicie sesión en una cuenta spoke o en la cuenta hub con las credenciales de usuario raíz. 2. Confirme que la cuenta de correo electrónico que especificó reciba la notificac ión de Amazon SNS.	AWS general

Recursos relacionados

- Prácticas recomendadas de seguridad (documentación de IAM)
- Trabajar con StackSets (CloudFormation documentación)
- Introducción (documentación de Terraform)

Información adicional

Amazon GuardDuty es un servicio de supervisión continua de la seguridad que analiza y procesa los registros para identificar actividades inesperadas y potencialmente no autorizadas en su entorno de AWS. Como alternativa a esta solución, si la tiene habilitada GuardDuty, puede avisarle cuando se hayan utilizado las credenciales del usuario raíz. El GuardDuty resultado es`Policy:IAMUser/RootCredentialUsage`, y la gravedad predeterminada es baja. Para obtener más información, consulta Cómo gestionar GuardDuty los hallazgos de Amazon.

Enviar una notificación cuando se cree un usuario de IAM

Documento creado por Mansi Suratwala (AWS) y Sergiy Shevchenko (AWS)

Entorno: producción	Tecnologías: Seguridad, identidad, cumplimiento; Infraestructura	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon SNS; AWS Identity and Access Management; AWS Lambda; Amazon CloudWatch		

Resumen

En Amazon Web Services (AWS), puede utilizar este patrón para implementar una CloudFormation plantilla de AWS que le permita recibir notificaciones automáticamente cuando se creen usuarios de AWS Identity and Access Management (IAM).

Con IAM, puede administrar el acceso a los servicios y recursos de AWS de forma segura. Puede crear y administrar usuarios y grupos de AWS, y utilizar permisos para permitir y denegar a dichos usuarios y grupos el acceso a los recursos de AWS.

La CloudFormation plantilla crea un evento de Amazon CloudWatch Events y una función de AWS Lambda. El evento usa AWS CloudTrail para monitorear cualquier usuario de IAM que se esté creando en la cuenta de AWS. Si se crea un usuario, el evento CloudWatch Events inicia una función Lambda, que le envía una notificación de Amazon Simple Notification Service (Amazon SNS) informándole del nuevo evento de creación del usuario.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Creación e implementación de una CloudTrail ruta de AWS

Limitaciones

- La CloudFormation plantilla de AWS debe implementarse `CreateUser` únicamente para.

Arquitectura

Pila de tecnología de destino

- IAM
- AWS CloudTrail
- CloudWatch Eventos de Amazon
- AWS Lambda
- Amazon Simple Storage Service (Amazon S3)
- Amazon SNS

Arquitectura de destino

Automatizar y escalar

Puede utilizar la CloudFormation plantilla de AWS varias veces para distintas regiones y cuentas de AWS. Debe ejecutarla solo una vez en cada región o cuenta. Para automatizar la implementación en varias cuentas, utilice AWS CloudFormation StackSets. La CloudFormation plantilla podrá implementar todos los recursos necesarios en cada cuenta.

Herramientas

Herramientas

- IAM: AWS Identity and Access Management (IAM) es un servicio web que le ayuda a controlar de forma segura el acceso a los recursos de AWS. Utilice IAM para controlar quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos.
- AWS CloudFormation: AWS le CloudFormation ayuda a modelar y configurar sus recursos de Amazon Web Services para que pueda dedicar menos tiempo a gestionar esos recursos y más a centrarse en las aplicaciones que se ejecutan en AWS. Cree una plantilla que describa todos los recursos de AWS que desee y CloudFormation se encarga de aprovisionar y configurar esos recursos por usted.

- AWS CloudTrail: AWS le CloudTrail ayuda a gestionar la gobernanza, el cumplimiento y la auditoría operativa y de riesgos de su cuenta de AWS. Las acciones realizadas por un usuario, un rol o un servicio de AWS se registran como eventos en CloudTrail. Los eventos incluyen las acciones llevadas a cabo en la consola de administración de AWS, la interfaz de línea de comandos de AWS y las API de AWS.
- Amazon CloudWatch Events: Amazon CloudWatch Events ofrece una near-real-time secuencia de eventos del sistema que describen los cambios en los recursos de AWS.
- AWS Lambda es un servicio informático que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet. Puede utilizar Amazon S3 para almacenar y recuperar cualquier cantidad de datos en cualquier momento y desde cualquier parte de la web.
- Amazon SNS – Amazon Simple Notification Service (Amazon SNS) es un servicio gestionado que proporciona la entrega de mensajes mediante Lambda, HTTP, correo electrónico, notificaciones push móviles y mensajes de texto móviles (SMS).

Código

El archivo .zip del proyecto está disponible como adjunto.

Epics

Cree el bucket de S3 para el script de Lambda

Tarea	Descripción	Habilidades requeridas
Definir el bucket de S3.	Abra la consola de Amazon S3 y elija o cree un bucket de S3. Este bucket de S3 alojará el archivo .zip de código Lambda. El nombre del bucket de S3 no puede incluir barras diagonales iniciales.	Arquitecto de la nube

Cargue el código Lambda en el bucket de S3

Tarea	Descripción	Habilidades requeridas
Cargue el código Lambda.	Cargue el archivo .zip de código Lambda proporcio nado en la sección Archivos adjuntos en el bucket S3 que haya definido.	Arquitecto de la nube

Implemente la CloudFormation plantilla

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation plantilla.	En la CloudFormation consola, implementa la CloudFormation `createIAMuser.yaml` plantilla que se proporcio na como adjunto a este patrón. En la siguiente Epic, proporcione los valores de los parámetros.	Arquitecto de la nube

Complete los parámetros de la CloudFormation plantilla

Tarea	Descripción	Habilidades requeridas
Proporcione el nombre del bucket de S3.	Escriba el nombre de bucket de S3 que ha creado o elegido en la primera Epic.	Arquitecto de la nube
Proporcione la clave S3.	Proporcione la ubicación del archivo .zip de código Lambda en su bucket de S3 sin barras diagonales iniciales (por	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	ejemplo, `<directory>/<file-name>.zip`).	
Proporcione una dirección de correo electrónico.	Proporcione una dirección de correo electrónico activa en la que desea recibir las notificaciones de Amazon SNS.	Arquitecto de la nube
Defina el nivel de registro.	Defina el nivel y la frecuencia de registro de la función de Lambda. `Info` designa mensajes informativos detallados sobre el progreso de la aplicación. `Error` designa los eventos de error que aún podrían permitir que la aplicación siguiera ejecutándose. `Warning` designa situaciones potencialmente dañinas.	Arquitecto de la nube

Confirmar la suscripción

Tarea	Descripción	Habilidades requeridas
Confirmar la suscripción.	Cuando la plantilla se implementa correctamente, se envía un mensaje de correo electrónico de suscripción a la dirección de correo electrónico proporcionada. Debe confirmar esta suscripción de correo electrónico para	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	comenzar a recibir notificac iones.	

Recursos relacionados

- Creación de un registro de seguimiento
- Crear un bucket de S3
- Carga de los archivos en un bucket de S3
- Despliegue de una CloudFormation plantilla
- Creación de un usuario de IAM
- Crear una regla de CloudWatch eventos que se active en una llamada a la API de AWS mediante AWS CloudTrail

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Impida el acceso a Internet a nivel de cuenta mediante una política de control de servicios

Creado por Sergiy Shevchenko (AWS), Sean O'Sullivan (AWS) y Victor Mazeo Whitaker (AWS)

Entorno: PoC o piloto	Tecnologías: seguridad, identidad, conformidad; redes	Servicios de AWS: AWS Organizations

Resumen

Con frecuencia, las organizaciones desean limitar el acceso a Internet para los recursos de las cuentas que deben permanecer privados. En estas cuentas, los recursos de las nubes privadas virtuales (VPC) no deberían acceder a Internet de ninguna manera. Muchas organizaciones eligen una arquitectura de inspección centralizada. Para el tráfico este-oeste (de VPC a VPC) en una arquitectura de inspección centralizada, debe asegurarse de que las cuentas radiales y sus recursos no tengan acceso a Internet. Para el tráfico norte-sur (salida de Internet y local), querrá permitir el acceso a Internet únicamente a través de la VPC de inspección.

Este patrón utiliza una política de control de servicios (SCP) para evitar el acceso a Internet. Puedes aplicar este SCP a nivel de cuenta o unidad organizativa (OU). El SCP limita la conectividad a Internet al impedir lo siguiente:

- Crear o adjuntar una puerta de enlace a Internet IPv4 o IPv6 que permita el acceso directo a Internet a la VPC
- Crear o aceptar una conexión de emparejamiento de VPC que pueda permitir el acceso indirecto a Internet a través de otra VPC
- Crear o actualizar una AWS Global Acceleratorconfiguración que pueda permitir el acceso directo de Internet a los recursos de la VPC

Requisitos previos y limitaciones

Requisitos previos

- Uno o varios Cuentas de AWS gestionados como una organización en AWS Organizations.

- Todas las funciones están habilitadas en AWS Organizations.
- Los SCP están habilitados en la organización.
- Permisos para:
  - Acceder a la cuenta de administración de la organización.
  - Crea SCP. Para obtener más información sobre los permisos mínimos, consulte Creación de un SCP.
  - Adjunta el SCP a las cuentas o unidades organizativas (OU) de destino. Para obtener más información sobre los permisos mínimos, consulte Adjuntar y separar políticas de control de servicios.

Limitaciones

- Las SCP no afectan a los usuarios ni a los roles de la cuenta de administración. Afectan solo a las cuentas miembro de su organización.
- Los SCP afectan únicamente a los usuarios y roles AWS Identity and Access Management (de IAM) que son administrados por cuentas que forman parte de la organización. Para más información, consulte Efectos de las SCP en los permisos.

Herramientas

Servicios de AWS

- AWS Organizationses un servicio de administración de cuentas que le ayuda a consolidar múltiples cuentas Cuentas de AWS en una organización que puede crear y administrar de forma centralizada. En este patrón, se utilizan las políticas de control de servicios (SCP) en AWS Organizations.
- Amazon Virtual Private Cloud (Amazon VPC) le ayuda a lanzar AWS recursos en una red virtual que haya definido. Esa red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Prácticas recomendadas

Tras establecer este SCP en su organización, asegúrese de actualizarlo con frecuencia para abordar cualquier novedad Servicios de AWS o función que pueda afectar al acceso a Internet.

Epics

Cree y adjunte el SCP

Tarea	Descripción	Habilidades requeridas
Cree el SCP.	1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión en la cuenta de administración de la organización. 2. En el panel izquierdo, selecciona Políticas. 3. En la página de políticas, elija Políticas de control de servicios. 4. En la página Políticas de control de servicios, seleccione Crear política. 5. En la página Crear una nueva política de control de servicios, introduzca un nombre de política y una descripción de la política opcional. 6. (Opcional) Añada AWS etiquetas a su política. 7. En el editor JSON, elimina la política de marcadores de posición. 8. Pegue la siguiente política de en el editor JSON. `{ "Version": "2012-10-17",`	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	<pre>"Statement": [{ "Action": ["ec2:Atta chInternetGateway", "ec2:Crea teInternetGateway", "ec2:Crea teVpcPeeringConnec tion", "ec2:Acce ptVpcPeeringConnec tion", "ec2:Crea teEgressOnlyIntern etGateway"], "Resource": "*", "Effect": "Deny" }, { "Action": ["globalac celerator:Create*", "globalac celerator:Update*"], "Resource": "*", "Effect": "Deny" }] }</pre> 9. Elija Crear política.	

Tarea	Descripción	Habilidades requeridas
Adjunta el SCP.	1. En la página Políticas de control de servicios, elija la política que creó. 2. En la pestaña Objetivos, seleccione Adjuntar. 3. Seleccione la OU o la cuenta a la que desee adjuntar la política. Puede que tenga que expandir las unidades organizativas para encontrar la unidad organizativa o la cuenta que desee. 4. Elija Asociar política.	Administrador de AWS

Recursos relacionados

- AWS Organizations documentación
- Políticas de control de servicios (SCP)
- Arquitectura de inspección centralizada con AWS Gateway Load Balancer y AWS Transit Gateway (entrada del AWS blog)

Escanea los repositorios de Git en busca de información confidencial y problemas de seguridad mediante git-secrets

Creado por Saurabh Singh (AWS)

Entorno: producción	Tecnologías: seguridad, identidad y conformidad	Carga de trabajo : código abierto

Resumen

Este patrón describe cómo usar la herramienta git-secrets de código abierto de los Laboratorios de AWS para escanear los repositorios de código fuente de Git y encontrar código que pueda incluir información confidencial, como contraseñas de usuario o claves de acceso de AWS, o que presente algún otro problema de seguridad.

`git-secrets` escanea las confirmaciones, los mensajes de confirmación y las fusiones para evitar que se añada información confidencial, como secretos, a tus repositorios de Git. Por ejemplo, si una confirmación, un mensaje de confirmación o cualquier confirmación de un historial de fusiones coincide con uno de tus patrones de expresión regular prohibidos y configurados, la confirmación se rechaza.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un repositorio de Git que requiere un análisis de seguridad
- Un cliente Git (versión 2.37.1 y posteriores) instalado

Arquitectura

Arquitectura de destino

- Git
- `git-secrets`

Herramientas

- git-secrets es una herramienta que evita que se guarde información confidencial en los repositorios de Git.
- Git es un sistema de control de versiones distribuido de código abierto.

Prácticas recomendadas

- Escanee siempre un repositorio de Git incluyendo todas las revisiones:

```
git secrets --scan-history
```

Epics

Conexión con instancias EC2

Tarea	Descripción	Habilidades requeridas
Conéctese a la instancia EC2 mediante SSH.	Conéctese a una instancia de Amazon Elastic Compute Cloud (Amazon EC2) mediante SSH y un archivo de par de claves. Puede omitir este paso si escanea un repositorio en su equipo local.	AWS general

Instale Git

Tarea	Descripción	Habilidades requeridas
Instale Git	Instale Git mediante el comando:	AWS general

Tarea	Descripción	Habilidades requeridas
	`yum install git -y` Si utiliza su máquina local, puede instalar un cliente Git para una versión específica del sistema operativo. Para obtener más información, consulte el sitio web de Git.	

Clone el repositorio fuente e instale git-secrets

Tarea	Descripción	Habilidades requeridas
Clone el repositorio de código fuente de Git.	Para clonar el repositorio de Git que quiera escanear, seleccione el comando Git clone (Clonar Git) en su directorio principal.	AWS general
Clone git-secrets.	Clone el repositorio de Git `git-secrets` . `git clone https://github.com/awslabs/git-secrets.git` Coloque `git-secrets` en algún lugar de su `PATH` para que Git lo recoja cuando usted ejecute `git-secrets` .	AWS general
Instale git-secrets.	Para Unix y sus variantes (Linux/macOS):	AWS general

Tarea	Descripción	Habilidades requeridas
	Usted puede usar el destino `install` del `Makefile` (que se proporciona en el repositorio `git-secrets`) para instalar la herramienta. Usted puede personalizar la ruta de instalación mediante las variables `PREFIX` y `MANPREFIX` . `make install` Para Windows: Ejecute el PowerShell `install.ps1` script proporcionado en el `git-secrets` repositorio. Este script copia los archivos de instalación en un directorio de instalación (`%USERPROFILE%/.git-secrets` de forma predeterminada) y agrega el directorio al usuario actual `PATH`. `PS > ./install.ps1` Para Homebrew (usuarios de macOS): Ejecute: `brew install git-secrets`	

Tarea	Descripción	Habilidades requeridas
	Para obtener más información, consulte la sección Related resources (Recursos relacionados).	

Escanee el repositorio de código de git

Tarea	Descripción	Habilidades requeridas
Vaya al repositorio de origen.	Cambie al directorio del repositorio de Git que desee escanear: `cd my-git-repository`	AWS general
Registre el conjunto de reglas de AWS (enlaces de Git).	Para configurar `git-secrets` el escaneo de su repositorio de Git en cada confirmación, ejecute el comando: `git secrets --register-aws`	AWS general
Escanee el repositorio.	Ejecute el siguiente comando para comenzar a escanear su repositorio: `git secrets --scan`	AWS general
Revise el archivo de salida.	La herramienta genera un archivo de salida si encuentra una vulnerabilidad en su	AWS general

Tarea	Descripción	Habilidades requeridas
	repositorio de Git. Por ejemplo: `example.sh:4:AWS_SECRET_ACCESS_KEY = *********` `[ERROR] Matched one or more prohibited patterns` `Possible mitigations:` `- Mark false positives as allowed using: git config --add secrets.allowed ...` `- Mark false positives as allowed by adding regular expressions to .gitallowed at repository's root directory` `- List your configured patterns: git config --get-all secrets.patterns` `- List your configured allowed patterns: git config --get-all secrets.allowed` `- List your configured allowed patterns in .gitallowed at repository's root directory` `- Use --no-verify if this is a one-time false positive`	

Recursos relacionados

- Git webhooks con servicios de AWS (Guía rápida de AWS)
- herramienta git-secrets
- Migración de un repositorio de Git a AWS (tutorial práctico de AWS)
- Referencia de CodeCommit API de AWS

Enviar alertas desde AWS Network Firewall a un canal de Slack

Creado por Venki Srivatsav (AWS) y Aromal Raj Jayarajan (AWS)

Repositorio de código: NfwSlackIntegration	Entorno: PoC o piloto	Tecnologías: seguridad, identidad, conformidad; redes
Servicios de AWS: AWS Lambda; AWS Network Firewall; Amazon S3		

Resumen

Este patrón describe cómo implementar un firewall mediante el Firewall de red de Amazon Web Services (AWS) con el modelo de implementación distribuida y cómo propagar las alertas generadas por AWS Network Firewall a un canal de Slack configurable.

Los estándares de conformidad, como el Estándar de seguridad de datos del sector de pagos con tarjeta (PCI DSS), requieren que instale y mantenga un firewall para proteger los datos de los clientes. En la nube de AWS, una nube privada virtual (VPC) se considera igual que una red física en el contexto de estos requisitos de conformidad. Puede usar Network Firewall para monitorear el tráfico de red entre las VPC y proteger las cargas de trabajo que se ejecutan en las VPC que se rigen por un estándar de cumplimiento. Network Firewall bloquea el acceso o genera alertas cuando detecta un acceso no autorizado desde otras VPC de la misma cuenta. Sin embargo, Network Firewall admite un número limitado de destinos para enviar las alertas. Estos destinos incluyen depósitos de Amazon Simple Storage Service (Amazon S3), grupos de registros de CloudWatch Amazon y transmisiones de entrega de Amazon Data Firehose. Cualquier otra acción relacionada con estas notificaciones requiere un análisis fuera de línea mediante Amazon Athena o Amazon Kinesis.

Este patrón proporciona un método para propagar las alertas generadas por Network Firewall a un canal de Slack configurable para tomar medidas adicionales casi en tiempo real. También puede ampliar la funcionalidad a otros mecanismos de alerta PagerDuty, como Jira y el correo electrónico. (Esas personalizaciones quedan fuera del alcance de este patrón).

Requisitos previos y limitaciones

Requisitos previos

- Canal de Slack (consulte Primeros pasos en el centro de ayuda de Slack)
- Privilegios necesarios para enviar un mensaje al canal
- La URL del punto de conexión de Slack con un token de API (seleccione su aplicación y elija un webhook entrante para ver su URL; para obtener más información, consulte Cómo crear un webhook entrante en la documentación de la API de Slack)
- Una instancia de prueba de Amazon Elastic Compute Cloud (Amazon EC2) en las subredes de carga de trabajo
- Reglas de prueba en Network Firewall
- Tráfico real o simulado para activar las reglas de prueba
- Un bucket de S3 para almacenar los archivos fuente que se van a implementar

Limitaciones

- Actualmente, esta solución solo admite un rango de enrutamiento entre dominios sin clase (CIDR) como filtro para las IP de origen y destino.

Arquitectura

Pila de tecnología de destino

- Una VPC
- Cuatro subredes (dos para el firewall y dos para las cargas de trabajo)
- Puerta de enlace de Internet
- Cuatro tablas de enrutamiento con reglas
- El bucket de S3 se utiliza como destino de alertas y se configura con una política de bucket y una configuración de eventos para ejecutar una función de Lambda
- Función de Lambda con un rol de ejecución, para enviar notificaciones de Slack
- El secreto de AWS Secrets Manager para almacenar la URL de Slack
- Firewall de red con configuración de alertas
- Canal de Slack

Todos los componentes, excepto el canal de Slack, se aprovisionan mediante las CloudFormation plantillas y la función Lambda que se proporcionan con este patrón (consulta la sección Código).

Arquitectura de destino

Este patrón configura un firewall de red descentralizado con integración con Slack. Esta arquitectura consta de una VPC con dos zonas de disponibilidad. La VPC incluye dos subredes protegidas y dos subredes de firewall con puntos de conexión del firewall de red. Todo el tráfico que entra y sale de las subredes protegidas se puede supervisar mediante la creación de políticas y reglas de firewall. El firewall de la red está configurado para colocar todas las alertas en un bucket de S3. Este bucket de S3 está configurado para llamar a una función de Lambda cuando recibe un evento `put`. La función Lambda obtiene la URL de Slack configurada de Secrets Manager y envía el mensaje de notificación al espacio de trabajo de Slack.

Para obtener más información sobre esta arquitectura, consulte la entrada del blog de AWS sobre modelos de implementación para AWS Network Firewall.

Herramientas

Servicios de AWS

- AWS Network Firewall es un servicio de detección y prevención de intrusiones y de firewall de red con estado y administrado para nubes privadas virtuales (VPC) en la nube de AWS. Puede utilizar el firewall de red para filtrar el tráfico en el perímetro de su VPC y proteger sus cargas de trabajo en AWS.
- AWS Secrets Manager es un servicio de almacenamiento y recuperación de credenciales. Con Secrets Manager puede reemplazar las credenciales codificadas en el código, incluidas las contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación. Este patrón usa Secrets Manager para almacenar la URL de Slack.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos. Puede utilizar Amazon S3 para almacenar y recuperar cualquier cantidad de datos en cualquier momento y desde cualquier parte de la web. Este patrón utiliza Amazon S3 para almacenar las CloudFormation plantillas y el script de Python para la función Lambda. También utiliza un bucket de S3 como el destino de alerta del firewall de red.
- AWS le CloudFormation ayuda a modelar y configurar sus recursos de AWS, a aprovisionarlos de forma rápida y coherente y a gestionarlos durante todo su ciclo de vida. Facilita poder usar una plantilla para describir los recursos y sus dependencias, y lanzarlos y configurarlos juntos como

una pila, en lugar de administrarlos de forma individual. Este patrón utiliza AWS CloudFormation para implementar automáticamente una arquitectura distribuida para Firewall Manager.

Código

El código de este patrón está disponible en el GitHub repositorio Network Firewall Slack Integration. En la carpeta `src` del repositorio, encontrará:

- Conjunto de CloudFormation archivos en formato YAML. Estas plantillas se utilizan para aprovisionar los componentes de este patrón.
- Un archivo fuente de Python (`slack-lambda.py`) para crear la función de Lambda.
- Un paquete de implementación de archivos .zip (`slack-lambda.py.zip`) para cargar el código de la función de Lambda.

Para usar el código de muestra, siga las instrucciones de la siguiente sección.

Epics

Configuración del bucket de S3

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3.	1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/. 2. Elija o cree un bucket de S3 para alojar el código. Un nombre de bucket de S3 es globalmente único y todas las cuentas de AWS comparten el espacio de nombres. El nombre de bucket de S3 no puede incluir barras a la izquierda	Desarrollador de aplicaciones, propietario de la aplicación, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	. Se recomienda utilizar un prefijo para organizar el código de este patrón. Para más información, consulte Crear un bucket en la documentación de Amazon S3.	
Cargue las CloudFormation plantillas y el código Lambda.	1. Descargue los siguiente s archivos del GitHub repositorio para este patrón: • `base.yml` • `igw-ingress-route.yml` • `slack-lambda.py` • `slackLambda.yml` • `decentralized-deployment.yml` • `protected-subnet-route.yml` • `slack-lambda.py.zip` 2. Cargue los archivos en el bucket de S3 que ha creado.	Desarrollador de aplicaciones, propietario de la aplicación, administrador de la nube

Implemente la CloudFormation plantilla

Tarea	Descripción	Habilidades requeridas
Lanza la CloudFormation plantilla.	Abra la CloudFormation consola de AWS en la misma región de AWS que su bucket de S3 e implemente la plantilla `base.yml`. Esta plantilla crea los recursos de AWS y las funciones de Lambda necesarios para que las alertas se transmitan al canal de Slack. Para obtener más informaci ón sobre la implementación de CloudFormation plantillas, consulte Crear una pila en la CloudFormation consola de AWS en la CloudFormation documentación.	Desarrollador de aplicaciones, propietario de la aplicación, administrador de la nube
Complete los parámetros de la plantilla.	Especifique el nombre de la pila y configure los valores de los parámetros. Para obtener una lista de los parámetros, sus descripciones y valores predeterminados, consulte CloudFormation los parámetro s en la sección de información adicional.	Desarrollador de aplicaciones, propietario de la aplicación, administrador de la nube
Cree la pila.	1. Revise los detalles de la pila y actualice los valores en función de los requisitos de su entorno.	Desarrollador de aplicaciones, propietario de la aplicación, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	2. Elija Crear pila para implementar la plantilla.	

Verificación de la solución

Tarea	Descripción	Habilidades requeridas
Probar la implementación.	Utilice la CloudFormation consola de AWS o la interfaz de línea de comandos de AWS (AWS CLI) para comprobar que se han creado los recursos que figuran en la sección Pila de tecnologías de destino. Si la CloudFormation plantilla no se implementa correctamente, compruebe los valores que proporcionó para los `pAvailabilityZone2` parámetros `pAvailabilityZone1` y. Deberían ser adecuados para la región de AWS en la que vaya a implementar la solución. Para obtener una lista de las zonas de disponibilidad de cada región de, consulte Regiones y zonas en la documentación de Amazon EC2.	Desarrollador de aplicaciones, propietario de la aplicación, administrador de la nube
Pruebe la funcionalidad.	1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.	Desarrollador de aplicaciones, propietario de la aplicación, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	2. Cree una instancia EC2 en una de las subredes protegidas. Elija una AMI (HVM) de Amazon Linux 2 para usarla como servidor HTTPS. Para obtener instrucciones, consulte Lanzamiento de una instancia en la documentación de Amazon EC2. 3. Utilice los siguientes datos de usuario para instalar un servidor web en la instancia EC2: `#!/bin/bash` `yum install httpd -y` `systemctl start httpd` `systemctl stop firewalld` `cd /var/www/html` `echo "Hello!! this is a NFW alert test page, 200 OK" > index.html` 4. Cree las siguientes reglas de firewall de red: Regla sin estado: `Source: 0.0.0.0/0` `Destination 10.0.3.65/32 (private IP of the EC2 instance)` `Action: Forward` Regla con estado:	

Tarea	Descripción	Habilidades requeridas
	`Protocol: HTTP` `Source ip/port: Any / Any` `Destination ip/port: Any /Any` 5. Obtenga la IP pública del servidor web que creó en el paso 3. 6. Acceda a la IP pública en un navegador. Debería ver el siguiente mensaje en el navegador: `Hello!! this is a NFW alert test page, 200 OK` También recibirá una notificación en el canal de Slack. Es posible que la notificación se retrase en función del tamaño del mensaje. Para realizar pruebas, considere la posibilidad de proporcionar un filtro CIDR que no sea demasiado estrecho (por ejemplo, un valor CIDR con /32 se consideraría demasiado estrecho y /8 sería demasiado ancho). Para obtener más información, consulte la sección Comportamiento del filtro en Información adicional.	

Recursos relacionados

- Deployment models for AWS Network Firewall (entrada del blog de AWS)
- Políticas de AWS Network Firewall (documentación de AWS)
- Integración de Network Firewall con Slack (GitHub repositorio)
- Crear un espacio de trabajo de Slack (centro de ayuda de Slack)

Información adicional

CloudFormation parámetros

Parámetro	Descripción	Valor predeterminado o de muestra
`pVpcName`	Nombre del VPC que se va a crear.	Inspección
`pVpcCidr`	El rango CIDR que debe crear la VPC.	10.0.0.0/16
`pVpcInstanceTenancy`	Cómo se distribuyen las instancias EC2 en el hardware físico. Las opciones son `default` (arrendamiento compartido) o `dedicated` (arrendamiento único).	predeterminada
`pAvailabilityZone1`	La primera zona de disponibilidad de la infraestructura.	us-east-2a
`pAvailabilityZone2`	La segunda zona de disponibilidad de la infraestructura.	us-east-2b
`pNetworkFirewallSubnet1Cidr`	El rango CIDR de la primera subred del firewall (mínimo /28).	10.0.1.0/24

pNetworkFirewallSubnet2Cidr	El rango CIDR de la segunda subred del firewall (mínimo /28).	10.0.2.0/24
pProtectedSubnet1Cidr	El rango CIDR de la primera subred protegida (carga de trabajo).	10.0.3.0/24
pProtectedSubnet2Cidr	El rango CIDR de la segunda subred protegida (carga de trabajo).	10.0.4.0/24
pS3BucketName	El nombre del bucket de S3 existente en el que cargó el código fuente de Lambda.	us-w2- yourname-lambda-functions
pS3KeyPrefix	El prefijo del bucket de S3 en el que cargó el código fuente de Lambda.	aod-test
pAWSSecretName4Slack	El nombre del secreto que contiene la URL de Slack.	SlackEnpoint-Cfn
pSlackChannelName	El nombre del canal de Slack que creó.	somename-notifications
pSlackUserName	Nombre de usuario de Slack.	Usuario de Slack
pSecretKey	Puede ser cualquier clave. Se recomienda usar la configuración predeterminada.	webhookUrl
pWebHookUrl	El valor de la URL de Slack.	https://hooks.slack.com/services/T???9T??/A031885JRM7/9D4Y??????

`pAlertS3Bucket`	El nombre del bucket de S3 que se utilizará como el destino de la alerta del firewall de red. Este bucket se creará automáticamente.	us-w2- yourname-security-aod-alerts
`pSecretTagName`	El nombre de la etiqueta del secreto.	AppName
`pSecretTagValue`	El valor de la etiqueta para el nombre de etiqueta indicado.	LambdaSlackIntegration
`pdestCidr`	El filtro para el rango CIDR de destino. Para obtener más información, consulte la siguiente sección, Filtro comportamiento.	10.0.0.0/16
`pdestCondition`	Un indicador que indica si se debe excluir o incluir la coincidencia de destino. Para obtener más informaci ón, consulte la siguiente sección. Los valores válidos son `include` y `exclude`.	incluir
`psrcCidr`	El filtro del rango de CIDR de origen al que se debe alertar. Para obtener más información, consulte la siguiente sección.	118.2.0.0/16
`psrcCondition`	El indicador para excluir o incluir la coincidencia de origen. Para obtener más información, consulte la siguiente sección.	incluir

Comportamiento del filtro

Si no ha configurado ningún filtro en AWS Lambda, todas las alertas generadas se envían a su canal de Slack. Las IP de origen y destino de las alertas generadas coinciden con los rangos de CIDR que configuró al implementar la plantilla. CloudFormation Si hay una coincidencia, se aplica la condición. Si el origen o el destino se encuentran dentro del rango CIDR configurado y al menos uno de ellos está configurado con la condición `include`, se genera una alerta. Las siguientes tablas proporcionan ejemplos de valores, condiciones y resultados del CIDR.

	CIDR configurado	IP de alerta	Configured	Alerta
Origen	10.0.0.0/16	10.0.0.25	incluir	Sí
Destino	100.0.0.0/16	202.0.0.13	incluir	

	CIDR configurado	IP de alerta	Configured	Alerta
Origen	10.0.0.0/16	10,00,25	excluya	No
Destino	100.0.0.0/16	202.0.0.13	incluir	

	CIDR configurado	IP de alerta	Configured	Alerta
Origen	10.0.0.0/16	10,00,25	incluir	Sí
Destino	100.0.0.0/16	100,0,0,13	incluir	

	CIDR configurado	IP de alerta	Configured	Alerta
Origen	10.0.0.0/16	90,0,25	incluir	Sí

Destino	Nulo	202,0,0,13	incluir	
	CIDR configurado	IP de alerta	Configured	Alerta
Origen	10.0.0.0/16	90,0,25	incluir	No
Destino	100.0.0.0/16	202.0.0.13	incluir	

Simplifique la administración de certificados privados mediante AWS Private CA y AWS RAM

Creado por Everett Hinckley (AWS) y Vivek Goyal (AWS)

Repositorio de código: ACMPCA Hierarchy	Entorno: producción	Tecnologías: seguridad, identidad, conformidad; infraestructura; migración
Servicios de AWS: AWS Certificate Manager (ACM); AWS Organizations; AWS RAM		

Resumen

Puede usar AWS Private Certificate Authority (AWS Private CA) para emitir certificados privados para autenticar los recursos internos y firmar el código informático. Este patrón proporciona una CloudFormation plantilla de AWS para la implementación rápida de una jerarquía de CA de varios niveles y una experiencia de aprovisionamiento coherente. De forma opcional, puede usar AWS Resource Access Manager (AWS RAM) para compartir de forma segura la CA con sus organizaciones o unidades organizativas (OU) en AWS Organizations y centralizar la CA mientras usa la RAM de AWS para administrar los permisos. No es necesario tener una CA privada en cada cuenta, por lo que este enfoque le permite ahorrar dinero. Además, puede utilizar Amazon Simple Storage Service (Amazon S3) para almacenar la lista de revocación de certificados (CRL) y los registros de acceso.

Esta implementación ofrece los siguientes beneficios y características:

- Centraliza y simplifica la administración de la jerarquía de CA privadas mediante AWS Private CA.
- Exporta certificados y claves a dispositivos gestionados por el cliente en AWS y en las instalaciones.
- Utiliza una CloudFormation plantilla de AWS para una implementación rápida y una experiencia de aprovisionamiento coherente.
- Crea una CA raíz privada junto con una jerarquía de 1, 2, 3 o 4 CA subordinadas.

- Si lo desea, utiliza la RAM de AWS para compartir la CA subordinada de la entidad final con otras cuentas a nivel de organización o unidad organizativa.
- Ahorra dinero al eliminar la necesidad de una CA privada en cada cuenta mediante el uso de AWS RAM.
- Crea un bucket de S3 opcional para la CRL.
- Crea un bucket de S3 opcional para los registros de acceso a la CRL.

Requisitos previos y limitaciones

Requisitos previos

Si desea compartir la CA dentro de una estructura de AWS Organizations, identifique o configure lo siguiente:

- Una cuenta de seguridad para crear la jerarquía de CA y compartirla.
- Una unidad organizativa o cuenta independiente para realizar pruebas.
- El uso compartido está habilitado en la cuenta de administración de AWS Organizations. Para obtener más información, consulte Habilitar el uso compartido con AWS Organizations en la documentación de AWS RAM.

Limitaciones

- Las CA son recursos regionales. Todas las CA residen en una sola cuenta de AWS y una única región de AWS.
- No se admiten los certificados y las claves generados por los usuarios. Para este caso de uso, le recomendamos que personalice esta solución para utilizar una CA raíz externa.
- No se admite un bucket de CRL público. Le recomendamos que utilice la CRL como privada. Si se requiere acceso a Internet a la CRL, consulte la sección sobre el uso de Amazon CloudFront para servir las CRL en Habilitación de la función S3 Block Public Access (BPA) en la documentación de AWS Private CA.
- Este patrón implementa un enfoque de una sola región. Si necesita una autoridad de certificación multirregional, puede implementar subordinadas en una segunda región de AWS o de forma en las instalaciones. Esta complejidad queda fuera del ámbito de este patrón, ya que la implementación depende del caso de uso específico, del volumen de carga de trabajo, de las dependencias y de los requisitos.

Arquitectura

Pila de tecnología de destino

- CA
- AWS RAM
- Amazon S3
- AWS Organizations
- AWS CloudFormation

Arquitectura de destino

Este patrón ofrece dos opciones para compartir con AWS Organizations:

Opción 1: Crear el recurso compartido a nivel de la organización. Todas las cuentas de la organización pueden emitir los certificados privados mediante la CA compartida, como se muestra en el siguiente diagrama.

Opción 2 : Crear el recurso compartido a nivel de unidad organizativa (OU). Solo las cuentas de la OU especificada pueden emitir los certificados privados mediante la CA compartida. Por ejemplo, en el siguiente diagrama, si el recurso compartido se crea en el nivel de unidad en un entorno aislado, tanto el desarrollador 1 como el desarrollador 2 pueden emitir certificados privados mediante la CA compartida.

Herramientas

Servicios de AWS

- AWS Private CA: AWS Private Certificate Authority (AWS Private CA) es un servicio de CA privada alojado para emitir y revocar certificados digitales privados. Le permite crear jerarquías de entidades de certificación (CA) privadas, incluidas las entidades de certificación raíz y subordinadas, sin los costos de inversión y mantenimiento de operar una entidad de certificación en las instalaciones.
- AWS RAM: AWS Resource Access Manager (AWS RAM) le ayuda a compartir sus recursos de forma segura entre las cuentas de AWS y dentro de su organización o unidades organizativas en

AWS Organizations. Para reducir la sobrecarga operativa en un entorno de varias cuentas, puede crear un recurso y utilizar la RAM de AWS para compartir ese recurso entre cuentas.

- AWS Organizations: AWS Organizations es un servicio de administración de cuentas que le permite unificar varias cuentas de AWS en una organización que crea y administra de forma centralizada.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos. Puede utilizar Amazon S3 para almacenar y recuperar cualquier cantidad de datos en cualquier momento y desde cualquier parte de la web. Este patrón utiliza Amazon S3 para almacenar la lista de revocación de certificados (CRL) y los registros de acceso.
- AWS CloudFormation: AWS le CloudFormation ayuda a modelar y configurar sus recursos de AWS, a aprovisionarlos de forma rápida y coherente y a gestionarlos durante todo su ciclo de vida. Facilita poder usar una plantilla para describir los recursos y sus dependencias, y lanzarlos y configurarlos juntos como una pila, en lugar de administrarlos de forma individual. Este patrón utiliza AWS CloudFormation para implementar automáticamente una jerarquía de CA de varios niveles.

Código

El código fuente de este patrón está disponible en el GitHub repositorio jerárquico de CA privadas de AWS. El repositorio incluye:

- La CloudFormation plantilla de AWS`ACMPCA-RootCASubCA.yaml`. Puede utilizar esta plantilla para implementar la jerarquía de CA para esta implementación.
- Pruebe los archivos para casos de uso, como la solicitud, la exportación, la descripción y la eliminación de un certificado.

Para utilizar estos archivos, siga las instrucciones de la sección Epics.

Epics

Diseñe la jerarquía de CA

Tarea	Descripción	Habilidades requeridas
Recopile la información sobre el tema del certificado.	Recopile la información sobre el titular del certifica do: nombre de la organizac	Arquitecto de la nube, arquitecto de seguridad e ingeniero de PKI

Tarea	Descripción	Habilidades requeridas
	ión, unidad organizativa, país, estado, en las instalaciones y nombre común.	
Recopile información opcional sobre AWS Organizations.	Si la CA formará parte de una estructura de AWS Organizations y desea compartir la jerarquía de CA dentro de esa estructura, recopile el número de cuenta de administración, el Identificador de la organización y, opcionalmente, el Identificador de la OU (si desea compartir la jerarquía de CA solo con una OU específica). Además, determine las cuentas u OU de AWS Organizations, si las hubiera, con las que quiere compartir la CA.	Arquitecto de la nube, arquitecto de seguridad e ingeniero de PKI
Diseñe la jerarquía de CA.	Determine qué cuenta alojará a las CA raíz y subordinadas. Determine cuántos niveles subordinados requiere la jerarquía entre los certificados raíz y de entidad final. Para obtener más información, consulte Diseñar una jerarquía de CA en la documentación de CA privadas de AWS.	Arquitecto de la nube, arquitecto de seguridad e ingeniero de PKI

Tarea	Descripción	Habilidades requeridas
Determine las convenciones de nomenclatura y etiquetado para la jerarquía de CA.	Determine los nombres de los recursos de AWS: la CA raíz y cada CA subordinada. Determine qué etiquetas deben asignarse a cada CA.	Arquitecto de la nube, arquitecto de seguridad e ingeniero de PKI
Determine los algoritmos de cifrado y firma necesarios.	Determine lo siguiente: • Los requisitos del algoritmo de cifrado de su organización para las claves públicas que la CA utiliza cuando emite un certificado. El valor predeterminado es RSA_2048. • El algoritmo clave que utiliza su CA para la firma de certificados. El valor predeterminado es SHA256WITHRSA.	Arquitecto de la nube, arquitecto de seguridad e ingeniero de PKI
Determine los requisitos de revocación de certificados para la jerarquía de CA.	Si se requieren capacidades de revocación de certificados, establezca una convención de nomenclatura para el bucket de S3 que contiene la lista de revocación de certificados (CRL).	Arquitecto de la nube, arquitecto de seguridad e ingeniero de PKI
Determine los requisitos de registro para la jerarquía de CA.	Si se requieren capacidades de registro de acceso, establezca una convención de nomenclatura para el bucket de S3 que contiene los registros de acceso.	Arquitecto de la nube, arquitecto de seguridad e ingeniero de PKI

Tarea	Descripción	Habilidades requeridas
Determine los períodos de caducidad de los certificados.	Determine la fecha de caducidad del certificado raíz (el valor predeterminado es de 10 años), los certificados de la entidad final (el valor predeterminado es de 13 meses) y los certificados de CA subordinados (el valor predeterminado es de 3 años). Los certificados de CA subordinados deben caducar antes que los certificados de CA de los niveles superiores de la jerarquía. Para obtener más información, consulte Administrar el ciclo de vida de las CA privadas en la documentación de las CA privadas de AWS.	Arquitecto de la nube, arquitecto de seguridad e ingeniero de PKI

Implemente la jerarquía de CA

Tarea	Descripción	Habilidades requeridas
Completar los requisitos previos.	Complete los pasos de la sección de requisitos previos de este patrón.	Administrador de la nube, ingenieros de seguridad e ingenieros de PKI
Cree funciones de CA para varias personas.	1. Determine los tipos de funciones o usuarios de AWS Identity and Access Management (IAM) en AWS IAM Identity Center (sucesor de AWS Single	Administrador de la nube, ingenieros de seguridad e ingenieros de PKI

Tarea	Descripción	Habilidades requeridas
	Sign-On) necesarios para administrar los distintos niveles de la jerarquía de CA, como RootCAAdmin, SubordinateCAAdmin y. CertificateConsumer 2. Determine la granularidad de las políticas necesarias para separar las funciones. 3. Cree los roles o usuarios de IAM necesarios en el Centro de Identidad de IAM en la cuenta en la que reside la jerarquía de CA.	

Tarea	Descripción	Habilidades requeridas
Implemente la pila. CloudFormation	1. Desde el GitHub repositorio de este patrón, descarga la plantilla AWSPCA - RootcaSubca.yaml. 2. Implemente la plantilla desde la CloudFormation consola de AWS o desde la interfaz de línea de comandos de AWS (AWS CLI). Para obtener más información, consulte Cómo trabajar con pilas en la CloudFormation documentación. 3. Complete los parámetros de la plantilla, incluidos el nombre de la organización, el nombre de la OU, el algoritmo clave, el algoritmo de firma y otras opciones.	Administrador de la nube, ingenieros de seguridad e ingenieros de PKI

Tarea	Descripción	Habilidades requeridas
Diseñe una solución para actualizar los certificados utilizados por los recursos administrados por los usuarios.	Los recursos de los servicios integrados de AWS, como Elastic Load Balancing, actualizan los certificados automáticamente antes de que caduquen. Sin embargo, los recursos gestionados por los usuarios, como los servidores web que se ejecutan en instancias de Amazon Elastic Compute Cloud (Amazon EC2), requieren otro mecanismo. 1. Determine qué recursos administrados por el usuario requieren certificados de entidad final de la entidad emisora de certificados privada. 2. Planifique un proceso para recibir notificaciones sobre la caducidad de los recursos y certificados administrados por los usuarios. Para ver ejemplos, consulte los siguientes: • Uso de una regla gestionada por AWS Config • Uso de Amazon CloudWatch y Amazon EventBridge	Administrador de la nube, ingenieros de seguridad e ingenieros de PKI

Tarea	Descripción	Habilidades requeridas
	3. Escriba scripts personalizados para actualizar los certificados en los recursos administrados por los usuarios e intégrelos con los servicios de AWS para automatizar las actualizaciones. Para obtener más información sobre los servicios de AWS integrados, consulte Servicios integrados con AWS Certificate Manager en la documentación de ACM.	

Valide y documente la jerarquía de CA

Tarea	Descripción	Habilidades requeridas
Valide el uso compartido opcional de RAM en AWS.	Si la jerarquía de CA se comparte con otras cuentas de AWS Organizations, inicie sesión en una de esas cuentas desde la consola de administración de AWS, navegue hasta la consola de CA privada de AWS y confirme que la CA recién creada se comparte con esta cuenta. Solo estará visible la CA de nivel inferior de la jerarquía, ya que es la CA que genera los certificados de	Administrador de la nube, ingenieros de seguridad e ingenieros de PKI

Tarea	Descripción	Habilidades requeridas
	la entidad final. Repita este procedimiento para ver una muestra de las cuentas con las que se comparte la CA.	
Valide la jerarquía de las entidades de certificación con pruebas del ciclo de vida de los certificados.	En el GitHub repositorio de este patrón, localice las pruebas del ciclo de vida. Ejecute las pruebas desde la AWS CLI para solicitar un certificado, exportarlo, describirlo y eliminarlo.	Administrador de la nube, ingenieros de seguridad e ingenieros de PKI
Importe la cadena de certifica dos a almacenes fiduciarios.	Para que los navegadores y otras aplicaciones confíen en un certificado, el emisor del certificado debe estar incluido en el almacén de confianza del navegador, que es una lista de entidades certifica doras de confianza. Añada la cadena de certificados de la nueva jerarquía de CA al almacén de confianza del navegador y de la aplicació n. Confirme que los certifica dos de la entidad final son de confianza.	Administrador de la nube, ingenieros de seguridad e ingenieros de PKI

Tarea	Descripción	Habilidades requeridas
Cree un manual de procedimientos para documentar la jerarquía de las CA.	Cree un manual de procedimientos preliminar para describir la arquitectura de la jerarquía de las entidades de certificación, la estructura contable que puede solicitar los certificados de la entidad final, el proceso de creación y las tareas de administración básicas, como la emisión de certificados de la entidad final (a menos que desee permitir el autoservicio por parte de las cuentas secundarias), el uso y el seguimiento.	Administrador de la nube, ingenieros de seguridad e ingenieros de PKI

Recursos relacionados

- Diseño de una jerarquía de CA (documentación de CA privada de AWS)
- Creación de una CA privada (documentación de CA privada de AWS)
- Cómo usar la RAM de AWS para compartir su cuenta cruzada de CA privada de AWS (entrada del blog de AWS)
- Prácticas recomendadas para las CA privadas de AWS (entrada del blog de AWS)
- Habilite el uso compartido de recursos en AWS Organizations (documentación de AWS RAM)
- Administración del ciclo de vida de las CA privadas (documentación de las CA privadas de AWS)
- acm-certificate-expiration-check para AWS Config (documentación de AWS Config)
- AWS Certificate Manager ahora supervisa la caducidad de los certificados a través de Amazon CloudWatch (anuncio de AWS)
- Servicios integrados con AWS Certificate Manager (documentación de ACM)

Información adicional

Cuando exporte certificados, utilice una contraseña que sea segura desde el punto de vista criptográfico y que se ajuste a la estrategia de prevención de pérdidas de datos de su organización.

Cómo desactivar los controles estándar de seguridad en todas las cuentas de los miembros de Security Hub en un entorno de varias cuentas

Creado por Michael Fuellbier (AWS) y Ahmed Bakry (AWS)

Entorno: producción	Tecnologías: seguridad, identidad, conformidad; sin servidor	Servicios de AWS: Amazon DynamoDB; EventBridge Amazon; AWS Lambda; AWS Security Hub; AWS Step Functions

Resumen

Importante: AWS Security Hub ahora admite la configuración centralizada de los estándares y controles de seguridad en todas las cuentas. Esta nueva función aborda muchos de los escenario s que cubre la solución en este patrón APG. Antes de implementar la solución siguiendo este patrón, consulte Configuración central en Security Hub.

En la nube de Amazon Web Services (AWS), los controles estándar de AWS Security Hub, como CIS AWS Foundations Benchmark o AWS Foundational Security Best Practices, solo se pueden desactivar (deshabilitar) manualmente desde una única cuenta de AWS. En un entorno con varias cuentas, no puede desactivar los controles de varias cuentas de miembros de Security Hub con «un clic» (es decir, una llamada a la API). Este patrón muestra cómo utilizar un clic para desactivar los controles estándar del Security Hub en todas las cuentas de los miembros del Security Hub administradas por la cuenta de administrador del Security Hub.

Requisitos previos y limitaciones

Requisitos previos

- Un entorno de varias cuentas compuesto por una cuenta de administrador de Security Hub que administra varias cuentas de miembros
- Interfaz de la línea de comandos de AWS (AWS CLI) versión 2, instalada

- Interfaz de la línea de comandos del modelo de aplicaciones sin servidor de AWS (AWS SAM CLI), instalada

Limitaciones

- Este patrón solo funciona en un entorno de varias cuentas en el que una sola cuenta de administrador de Security Hub administra varias cuentas de miembros.
- El inicio del evento provoca múltiples invocaciones paralelas si cambias muchos controles en un período de tiempo muy corto. Esto puede provocar una limitación de la API y provocar un error en las invocaciones. Por ejemplo, este escenario puede ocurrir si cambia muchos controles mediante programación mediante la CLI de controles del Security Hub.

Arquitectura

Pila de tecnología de destino

- Amazon DynamoDB
- Amazon EventBridge
- CLI de AWS
- AWS Lambda
- AWS SAM CLI
- AWS Security Hub
- AWS Step Functions

Arquitectura de destino

El siguiente diagrama muestra un ejemplo de un flujo de trabajo de Step Functions que desactiva los controles estándar de Security Hub en varias cuentas de miembros de Security Hub (tal como se ve desde la cuenta de administrador de Security Hub).

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Una EventBridge regla se inicia de forma diaria e invoca la máquina de estados. Puede modificar la temporización de la regla actualizando el parámetro Schedule en su CloudFormation plantilla de AWS.

2. Se inicia una EventBridge regla cada vez que se activa o desactiva un control en la cuenta de administrador de Security Hub.
3. Una máquina de estados de Step Functions propaga el estado de los controles estándar de seguridad (es decir, los controles que están activados o desactivados) de la cuenta de administrador de Security Hub a las cuentas de los miembros.
4. Se implementa un rol de AWS Identity and Access Management (IAM) multicuenta en cada cuenta miembro y es asumido por la máquina de estado. La máquina estatal activa o desactiva los controles de cada cuenta de miembro.
5. Una tabla de DynamoDB contiene excepciones e información sobre los controles que se deben activar o desactivar en una cuenta concreta. Esta información anula las configuraciones obtenidas de la cuenta de administrador de Security Hub para la cuenta de miembro especificada.

Nota: El propósito de la EventBridge regla programada es garantizar que las cuentas de los miembros de Security Hub recién agregadas tengan el mismo estado de control que las cuentas existentes.

Herramientas

- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, las funciones de Lambda de AWS, los puntos de conexión de invocación HTTP que utilizan destinos de API o los buses de eventos de otras cuentas de AWS.
- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Serverless Application Model (AWS SAM) es un marco de código abierto que permite crear aplicaciones sin servidor en la nube de AWS.

- AWS Security Hub proporciona una visión completa de su estado de seguridad en AWS. También le permite comprobar si su entorno de AWS cumple con los estándares y las prácticas recomendadas del sector de seguridad.
- AWS Step Functions es un servicio de orquestación sin servidor que le permite combinar funciones de Lambda AWS y otros servicios de AWS para crear aplicaciones esenciales desde el punto de vista empresarial.

Código

El código de este patrón está disponible en el repositorio GitHub AWS Security Hub Cross-Account Controls Disabler. El repositorio de código contiene los siguientes archivos y carpetas:

- `UpdateMembers/template.yaml`— Este archivo contiene los componentes desplegados en la cuenta de administrador de Security Hub, incluida la máquina de estados Step Functions y las EventBridge reglas.
- `member-iam-role/template.yaml`: este archivo contiene el código para implementar el rol de IAM multicuenta en la cuenta de un miembro.
- `stateMachine.json`: este archivo define el flujo de trabajo de la máquina de estados.
- `GetMembers/index.py`— Este archivo contiene el código de la máquina de GetMembersestados. Un script recupera el estado de los controles estándar de seguridad en todas las cuentas de los miembros de Security Hub existentes.
- `UpdateMember/index.py`: este archivo contiene un script que actualiza el estado de control de cada cuenta de miembro.
- `CheckResult/index.py`: este archivo contiene un script que comprueba el estado de la invocación del flujo de trabajo (aceptada o fallida).

Epics

Implemente un rol de IAM multicuenta en las cuentas de los miembros de Security Hub

Tarea	Descripción	Habilidades requeridas
Identifique el ID de cuenta de administrador de Security Hub.	Configure una cuenta de administrador de Security Hub	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	y, a continuación, anote el ID de la cuenta de administrador.	
Implemente la CloudFormation plantilla que incluye la función de IAM multicuenta en las cuentas de los miembros.	Para implementar la plantilla de `member-iam-role/template.yaml` en todas las cuentas de miembros administradas por la cuenta de administrador de Security Hub, ejecute el siguiente comando: `aws cloudformation deploy --template-file member-iam-role/template.yaml --capabilities CAPABILITY_NAMED_IAM --stack-name <your-stack-name> --parameter-overrides SecurityHubAdminAccountId=<your-account-ID>` El parámetro `SecurityHubAdminAccountId` debe coincidir con el ID de cuenta de administrador de Security Hub que indicó anteriormente.	AWS DevOps

Implemente una máquina de estados en la cuenta de administrador de Security Hub

Tarea	Descripción	Habilidades requeridas
Package la CloudFormation plantilla que incluye la	Para empaquetar la plantilla de `UpdateMembers/temp`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
máquina de estados con AWS SAM.	late.yaml en la cuenta de administrador de Security Hub, ejecute el siguiente comando: `sam package --templat e-file UpdateMem bers/template.yaml --output-template- file UpdateMembers/ template-out.yaml -- s3-bucket <your-s3- bucket-name>` Nota: Su depósito de Amazon Simple Storage Service (Amazon S3) debe estar en la misma región de AWS en la que implementa CloudForm ation la plantilla.	

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation plantilla empaquetada en la cuenta de administrador de Security Hub.	Para implementar la CloudFormation plantilla en la cuenta de administrador de Security Hub, ejecute el siguiente comando: `aws cloudformation deploy --template-file UpdateMembers/template-out.yaml --capabilities CAPABILITY_IAM --stack-name <your-stack-name>` En la **`member-iam-role/template.yaml`** plantilla, el parámetro MemberIAM debe coincidir con el RolePath parámetro IAM y MemberIAM RolePath debe coincidir con RoleName IAM. RoleName Nota: Dado que Security Hub es un servicio regional, debe implementar la plantilla de forma individual en cada región de AWS. Asegúrese de empaquetar primero la solución en un bucket de S3 en cada región.	AWS DevOps

Recursos relacionados

- Designación de una cuenta de administrador de Security Hub (documentación de Security Hub)

- Gestión de errores, reintentos y adición de alertas a las ejecuciones automáticas de Step Function State Machine (entrada del blog de AWS)

Actualice las credenciales de la CLI de AWS desde el centro de identidad de IAM de AWS mediante PowerShell

Creado por Chad Miles (AWS) y Andy Bowen (AWS)

Entorno: Producción	Tecnologías: seguridad, identidad, conformidad; nativas en la nube	Carga de trabajo: código abierto
Servicios de AWS: herramientas de AWS para PowerShell; centro de identidad de AWS IAM		

Resumen

Cuando desea usar las credenciales del AWS IAM Identity Center (sucesor de AWS Single Sign-On) con la interfaz de la línea de comandos de AWS (AWS CLI), los SDK de AWS o el AWS Cloud Development Kit (AWS CDK), suele ser necesario copiar y pegar las credenciales de la consola del IAM Identity Center en la interfaz de línea de comandos. Este proceso puede llevar un tiempo considerable, y debe repetirse en cada cuenta a la que se desea acceder.

Una solución habitual consiste en usar el comando `aws sso configure` de la CLI de AWS. Este comando añade un perfil habilitado para el IAM Identity Center a su CLI o SDK de AWS. Sin embargo, la desventaja de esta solución es que debe ejecutar el comando `aws sso login` para cada perfil o cuenta de CLI de AWS que haya configurado de esta manera.

Como solución alternativa, este patrón describe cómo utilizar los perfiles con nombre de la CLI de AWS y las herramientas de AWS PowerShell para almacenar y actualizar las credenciales de varias cuentas desde una única instancia del IAM Identity Center de forma simultánea. El script también almacena los datos de sesión del IAM Identity Center en memoria para poder actualizar las credenciales sin tener que volver a iniciar sesión en el IAM Identity Center.

Requisitos previos y limitaciones

Requisitos previos

- PowerShell, instalado y configurado. Para obtener más información, consulte Instalación PowerShell (documentación de Microsoft).
- Herramientas de AWS para PowerShell, instaladas y configuradas. Por motivos de rendimiento, le recomendamos encarecidamente que instale la versión modularizada de las herramientas de AWS para PowerShell, llamada. `AWS.Tools` Cada servicio de AWS es compatible con su pequeño módulo propio. En el PowerShell indicador, introduzca los siguientes comandos para instalar los módulos necesarios para este patrón: `AWS.Tools.InstallerSSO`, y. `SSOIDC`

```
Install-Module AWS.Tools.Installer
Install-AWSToolsModule SSO, SSOOIDC
```

  Para obtener más información, consulte Instalar AWS.Tools en Windows o Instalar AWS.Tools en Linux o macOS.
- La CLI de AWS o el SDK de AWS deben configurarse previamente con credenciales de trabajo mediante una de las siguientes acciones:
  - Utilice el comando `aws configure` de la CLI de AWS. Para más información, consulte Configuración rápida (documentación de AWS CLI).
  - Configure la CLI de AWS o el CDK de AWS para obtener acceso temporal a través de un rol de IAM. Para obtener más información, consulte Obtener credenciales de rol de IAM para acceder a la CLI (documentación del IAM Identity Center).

Limitaciones

- Este script no se puede usar en un proceso ni en una solución totalmente automatizada. Al implementar este script, deberá autorizar manualmente el acceso desde el IAM Identity Center. El script continuará automáticamente.

Versiones de producto

- Para todos los sistemas operativos, se recomienda utilizar la PowerShell versión 7.0 o posterior.

Arquitectura

Puede usar el script de este patrón para actualizar simultáneamente varias credenciales del IAM Identity Center, así como crear un archivo de credenciales para usarlo con la CLI de AWS, los SDK de AWS o el CDK de AWS.

Herramientas

Servicios de AWS

- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que permite interactuar con los servicios de AWS mediante comandos en el intérprete de comandos de línea de comandos.
- AWS IAM Identity Center le ayuda a gestionar de forma centralizada el acceso de inicio de sesión único (SSO) a todas sus cuentas y aplicaciones en la nube de AWS.
- Las herramientas de AWS PowerShell son un conjunto de PowerShell módulos que le ayudan a programar operaciones en sus recursos de AWS desde la línea de PowerShell comandos.

Otras herramientas

- PowerShelles un programa de administración de automatización y configuración de Microsoft que se ejecuta en Windows, Linux y macOS.

Prácticas recomendadas

Conserve una copia de este script para cada instancia de IAM Identity Center. No es posible usar un script en múltiples instancias.

Epics

Ejecutar el script SSO

Tarea	Descripción	Habilidades requeridas
Personalice el script de SSO.	1. Copie el script de SSO en la sección de Información adicional. 2. En la sección `Param`, en su entorno de AWS, defina los valores de las siguientes variables:	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	• `DefaultRoleName` – El rol de IAM o conjunto de permisos que se va a usar de forma predeterminada. • `Region`: la Región de AWS en la que se implementa IAM Identity Center. Para obtener una lista completa de las regiones y sus códigos, consulte Puntos de conexión regionales. • `StartUrl` – La URL utilizada para acceder a la página de inicio de sesión de IAM Identity Center. Use el mismo formato que el valor de ejemplo del script. • `EnvironmentName` – Un nombre abreviado para hacer referencia a esta copia del script. Se usará cuando se ejecuten varias copias del script en la misma sesión. 3. En la línea 10, en `# Add your Account Information` , edite los siguientes valores de las tablas hash para que reflejen su entorno:	

Tarea	Descripción	Habilidades requeridas
	• `Profile` – El nombre del perfil de CLI de AWS en el que se van a almacenar las credencia les temporales. • `AccountId` – La ID de la cuenta de AWS de la que está recuperando las credenciales. • `RoleName` – El nombre del rol o conjunto de permisos de IAM Identity Center que desea usar. Puede dejarlo como `$DefaultRoleName` si desea usar el mismo rol que definió en la sección `Param`. Cada línea de la tabla de hash debe terminar con una coma, excepto la última.	

Tarea	Descripción	Habilidades requeridas
Ejecutar el script SSO.	Se recomienda ejecutar el script personalizado en el PowerShell shell con el siguiente comando. `./Set-AwsCliSsoCredentials.ps1` Si lo desea, también puede ejecutar el script desde otro intérprete de comandos introduciendo el siguiente comando. `pwsh Set-AwsCliSsoCredentials.ps1`	Administrador de la nube

Solución de problemas

Problema	Solución
Error de `No Access`	El rol de IAM que está usando no tiene permisos para acceder a la función o al conjunto de permisos que ha definido en el parámetro `RoleName`. Actualice los permisos del rol que está usando o defina un rol o conjunto de permisos diferente en el script.

Recursos relacionados

- ¿Dónde se almacenan las opciones de configuración? (documentación de la CLI de AWS)
- Configurar la CLI de AWS para usar AWS IAM Identity Center (documentación de la CLI de AWS)
- Uso de perfiles con nombre (documentación de la CLI de AWS)

Información adicional

Script de SSO

En el siguiente script, sustituya los marcadores de posición de los corchetes angulares (**<>**) por su propia información y elimine los corchetes angulares.

```
Set-AwsCliSsoCredentials.ps1
Param(
    $DefaultRoleName = '<AWSAdministratorAccess>',
    $Region          = '<us-west-2>',
    $StartUrl        = "<https://d-12345abcde.awsapps.com/start/>",
    $EnvironmentName = "<CompanyName>"
)
Try {$SsoAwsAccounts = (Get-Variable -name "$($EnvironmentName)SsoAwsAccounts" -Scope
 Global -ErrorAction 'SilentlyContinue').Value.Clone()}
Catch {$SsoAwsAccounts = $False}
if (-not $SsoAwsAccounts) { $SsoAwsAccounts = @(
# Add your account information in the list of hash tables below, expand as necessary,
 and do not forget the commas
    @{Profile = "<Account1>"      ; AccountId = "<012345678901 >"; RoleName =
 $DefaultRoleName },
    @{Profile = "<Account2>"      ; AccountId = "<123456789012>"; RoleName =
 "<AWSReadOnlyAccess>" }
)}
$ErrorActionPreference = "Stop"
if (-not (Test-Path ~\.aws))      { New-Item ~\.aws -type Directory }
if (-not (Test-Path ~\.aws\credentials)) { New-Item ~\.aws\credentials -type File }
$CredentialFile = Resolve-Path ~\.aws\credentials
$PsuedoCreds    = @{AccessKey =
 'AKAEXAMPLE123ACCESS';SecretKey='PsuedoS3cret4cceSSKey123PsuedoS3cretKey'} # Pseudo
 Creds, do not edit.
Try {$SSOTokenExpire = (Get-Variable -Scope Global -Name
 "$($EnvironmentName)SSOTokenExpire" -ErrorAction 'SilentlyContinue').Value} Catch
 {$SSOTokenExpire = $False}
Try {$SSOToken       = (Get-Variable -Scope Global -Name "$($EnvironmentName)SSOToken"
 -ErrorAction 'SilentlyContinue').Value }      Catch {$SSOToken       = $False}
if ( $SSOTokenExpire -lt (Get-Date) ) {
    $SSOToken = $Null
    $Client   = Register-SSOOIDCClient -ClientName cli-sso-client -ClientType public -
Region $Region @PsuedoCreds
    $Device   = $Client | Start-SSOOIDCDeviceAuthorization -StartUrl $StartUrl -Region
 $Region @PsuedoCreds
```

```
    Write-Host "A Browser window should open. Please login there and click ALLOW." -
NoNewline
    Start-Process $Device.VerificationUriComplete
    While (-Not $SSOToken){
        Try {$SSOToken = $Client | New-SSOOIDCToken -DeviceCode $Device.DeviceCode -
GrantType "urn:ietf:params:oauth:grant-type:device_code" -Region $Region @PsuedoCreds}
        Catch {If ($_.Exception.Message -notlike "*AuthorizationPendingException*")
{Write-Error $_.Exception} ; Start-Sleep 1}
    }
    $SSOTokenExpire = (Get-Date).AddSeconds($SSOToken.ExpiresIn)
    Set-Variable -Name "$($EnvironmentName)SSOToken" -Value $SSOToken -Scope Global
    Set-Variable -Name "$($EnvironmentName)SSOTokenExpire" -Value $SSOTokenExpire -
Scope Global
}
$CredsTime     = $SSOTokenExpire - (Get-Date)
$CredsTimeText = ('{0:D2}:{1:D2}:{2:D2} left on SSO Token' -f $CredsTime.Hours,
 $CredsTime.Minutes, $CredsTime.Seconds).TrimStart("0 :")
for ($i = 0; $i -lt $SsoAwsAccounts.Count; $i++) {
    if (([DateTimeOffset]::FromUnixTimeSeconds($SsoAwsAccounts[$i].CredsExpiration /
 1000)).DateTime -lt (Get-Date).ToUniversalTime()) {
        Write-host "`r
    `rRegistering Profile $($SsoAwsAccounts[$i].Profile)" -NoNewline
        $TempCreds = $SSOToken | Get-SSORoleCredential -AccountId
 $SsoAwsAccounts[$i].AccountId -RoleName $SsoAwsAccounts[$i].RoleName -Region $Region
 @PsuedoCreds
        [PSCustomObject]@{AccessKey = $TempCreds.AccessKeyId; SecretKey =
 $TempCreds.SecretAccessKey; SessionToken = $TempCreds.SessionToken
        } | Set-AWSCredential -StoreAs $SsoAwsAccounts[$i].Profile -ProfileLocation
 $CredentialFile
        $SsoAwsAccounts[$i].CredsExpiration = $TempCreds.Expiration
    }
}
Set-Variable -name "$($EnvironmentName)SsoAwsAccounts" -Value $SsoAwsAccounts.Clone() -
Scope Global
Write-Host "`r$($SsoAwsAccounts.Profile) Profiles registered, $CredsTimeText"
```

Utilice AWS Config para supervisar las configuraciones de seguridad de Amazon Redshift

Creado por Lucas Kauffman (AWS) y abhishek sengar (AWS)

Repositorio de código: awslabs/ aws-config-rules	Entorno: producción	Tecnologías: seguridad, identidad, conformidad
Servicios de AWS: AWS Config; Amazon Redshift; AWS Lambda		

Resumen

Con AWS Config, puede evaluar las configuraciones de seguridad de sus recursos de AWS. AWS Config puede supervisar los recursos y, si los ajustes de configuración infringen las reglas definidas, AWS Config marca el recurso como no conforme.

Puede utilizar AWS Config para evaluar y supervisar sus clústeres y bases de datos de Amazon Redshift. Para obtener más información sobre las recomendaciones y funciones de seguridad, consulte Seguridad en Amazon Redshift. Este patrón incluye reglas de AWS Lambda personalizadas para AWS Config. Puede implementar estas reglas en su cuenta para supervisar las configuraciones de seguridad de sus clústeres y bases de datos de Amazon Redshift. Las reglas de este patrón le ayudan a usar AWS Config para confirmar que:

- El registro de auditoría está habilitado para las bases de datos del clúster de Amazon Redshift
- Se requiere SSL para conectarse al clúster de Amazon Redshift
- Se utilizan sistemas de cifrado del estándar federal de procesamiento de información (FIPS)
- Las bases de datos del clúster de Amazon Redshift están cifradas
- La supervisión de la actividad de los usuarios está habilitada

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- AWS Config debe estar habilitada en la cuenta de AWS. Para obtener más información, consulte Configuración de AWS Config con la consola o Configuración de AWS Config con AWS CLI.
- Se debe usar Python 3.9 o posterior para el controlador de AWS Lambda. Para obtener más información, consulte Trabajar con Python (documentación de AWS Lambda).

Versiones de producto

- Python, versión 3.9 o posterior

Arquitectura

Pila de tecnología de destino

- AWS Config

Arquitectura de destino

1. AWS Config ejecuta periódicamente la regla personalizada.
2. La regla personalizada invoca la función de Lambda.
3. La función de Lambda comprueba si hay configuraciones no conformes en los clústeres de Amazon Redshift.
4. La función de Lambda informa del estado de conformidad de cada clúster de Amazon Redshift a AWS Config.

Automatizar y escalar

Las reglas personalizadas de AWS Config se escalan para evaluar todos los clústeres de Amazon Redshift de su cuenta. No se requiere ninguna acción adicional para escalar esta solución.

Herramientas

Servicios de AWS

- AWS Config proporciona una visión detallada de los recursos de su cuenta de AWS y de cómo están configurados. Le ayuda a identificar cómo se relacionan los recursos entre sí y cómo han cambiado sus configuraciones a lo largo del tiempo.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Redshift es un servicio de almacenamiento de datos administrado de varios petabytes en la nube de AWS.

Repositorio de código

El código de este patrón está disponible en el repositorio. GitHub aws-config-rules Las reglas personalizadas de este repositorio son reglas Lambda en el lenguaje de programación Python. Este repositorio contiene muchas reglas personalizadas para AWS Config. En este patrón, solo se utilizan las siguientes reglas:

- `REDSHIFT_AUDIT_ENABLED`: Confirme que el registro de auditoría esté habilitado en el clúster de Amazon Redshift. Si también quiere confirmar que la supervisión de la actividad de los usuarios está habilitada, implemente la regla `REDSHIFT_USER_ACTIVITY_MONITORING_ENABLED` en su lugar.
- `REDSHIFT_SSL_REQUIRED`: Confirme que se requiere SSL para conectarse al clúster de Amazon Redshift. Si también quiere confirmar que se utilizan los sistemas de cifrado de las normas federales de procesamiento de información (FIPS), implemente la regla `REDSHIFT_FIPS_REQUIRED` en su lugar.
- `REDSHIFT_FIPS_REQUIRED`: Confirme que se requiere SSL y que se utilizan los cifrados FIPS.
- `REDSHIFT_DB_ENCRYPTED`: Confirme que las bases de datos del clúster de Amazon Redshift estén cifradas.
- `REDSHIFT_USER_ACTIVITY_MONITORING_ENABLED`: Confirme que el registro de auditorías y la supervisión de la actividad de los usuarios estén habilitados.

Epics

Prepárese para implementar las reglas

Tarea	Descripción	Habilidades requeridas
Configuración de políticas de IAM.	1. Cree una política de IAM personalizada basada en la identidad que permita a la función de ejecución de Lambda leer las configuraciones del clúster de Amazon Redshift. Para obtener más información, consulte Administrar el acceso a los recursos (documentación de Amazon Redshift) y Crear políticas de IAM (documentación de IAM). `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "redshift:DescribeClusterParameterGroups", "redshift:DescribeClusterParameters", "redshift:DescribeClusters", "redshift:DescribeClusterSecurityGroups",`	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	<pre>"redshift :DescribeClusterSn apshots", "redshift :DescribeClusterSu bnetGroups", "redshift :DescribeEventSubs criptions", "redshift :DescribeLoggingSt atus"], "Resource": "*" }] }</pre> 2. AWSLambda Execute Asigne las políticas AWSConfigRulesExecutionRole administradas como una política de permisos para la función de ejecución de Lambda. Para obtener instrucciones, consulte Cómo añadir permisos de identidad de IAM (documentación de IAM).	

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	En un intérprete de comandos de Bash, ejecute el siguiente comando. Esto clona el aws-config-rulesrepositorio desde GitHub. `git clone https://github.com/awslabs/aws-config-rules.git`	AWS general

Implemente las reglas en AWS Config

Tarea	Descripción	Habilidades requeridas
Implemente las reglas en AWS Config.	Siguiendo las instrucciones de Creación de reglas Lambda personalizadas (documentación de AWS Config), implemente una o varias de las siguientes reglas en su cuenta: • `REDSHIFT_AUDIT_ENABLED` • `REDSHIFT_SSL_REQUIRED` • `REDSHIFT_FIPS_REQUIRED` • `REDSHIFT_DB_ENCRYPTED` • `REDSHIFT_USER_ACTIVITY_MONITORING_ENABLED`	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Compruebe que las reglas funcionan.	Tras implementar las reglas, siga las instrucciones de Evaluación de sus recursos (documentación de AWS Config) para confirmar que AWS Config está evaluando correctamente sus recursos de Amazon Redshift.	AWS general

Recursos relacionados

Documentación de servicio de AWS

- Seguridad en Amazon Redshift (documentación de Amazon Redshift)
- Administración de la seguridad de las bases de datos (documentación de Amazon Redshift)
- Reglas personalizadas de AWS Config (documentación de AWS Config)

Recomendaciones de AWS

- Compruebe que los nuevos clústeres de Amazon Redshift tengan puntos de conexión SSL necesarios
- Asegúrese de que el clúster de Amazon Redshift esté cifrado en el momento de su creación

Información adicional

Puede usar las siguientes reglas administradas por AWS en AWS Config para confirmar las siguientes configuraciones de seguridad para Amazon Redshift:

- redshift-cluster-configuration-check— Utilice esta regla para confirmar que el registro de auditoría está habilitado para las bases de datos del clúster de Amazon Redshift y para confirmar que las bases de datos están cifradas.
- redshift-require-tls-ssl— Utilice esta regla para confirmar que se requiere SSL para conectarse al clúster de Amazon Redshift.

Utilice Network Firewall para capturar los nombres de dominio DNS de la indicación del nombre del servidor (SNI) para el tráfico saliente

Creado por Kirankumar Chandrashekar (AWS)

Entorno: PoC o piloto	Tecnologías: seguridad, identidad y conformidad; redes; aplicaciones web y móviles	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: AWS Lambda; AWS Network Firewall; Amazon VPC; Amazon Logs CloudWatch		

Resumen

Este patrón le muestra cómo utilizar el Network Firewall de Amazon Web Services (AWS) para recopilar los nombres de dominio DNS que proporciona la indicación del nombre del servidor (SNI) en el encabezado HTTPS del tráfico de red saliente. Network Firewall es un servicio gestionado que facilita la implementación de protecciones de red críticas para Amazon Virtual Private Cloud (Amazon VPC), incluida la capacidad de proteger el tráfico saliente con un firewall que bloquea los paquetes que no cumplen determinados requisitos de seguridad. Proteger el tráfico saliente dirigido a nombres de dominio DNS específicos se denomina filtrado de salida, que consiste en monitorear y, potencialmente, restringir el flujo de información saliente de una red a otra.

Tras capturar los datos del SNI que pasan por Network Firewall, puede utilizar Amazon CloudWatch Logs y AWS Lambda para publicar los datos en un tema del Amazon Simple Notification Service (Amazon SNS) que genere notificaciones por correo electrónico. Las notificaciones por correo electrónico incluyen el nombre del servidor y otra información relevante sobre el SNI. Además, puede utilizar el resultado de este patrón para permitir o restringir el tráfico saliente por nombre de dominio en el SNI mediante reglas de firewall. Para obtener más información, consulte Trabajo con grupos de reglas con estado en AWS Network Firewall en la documentación de Network Firewall.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Interfaz de la línea de comandos de AWS (AWS CLI) versión 2, instalada y configurada en Linux, macOS o Windows
- Network Firewall, instalado y configurado en Amazon VPC y utilizado para inspeccionar el tráfico saliente

Nota: Network Firewall puede usar cualquiera de las siguientes configuraciones de VPC:

- Arquitectura simple de una sola zona con una puerta de enlace de Internet
- Arquitectura de un varias zonas con una puerta de enlace de Internet
- Arquitectura con una puerta de enlace de Internet y una puerta de enlace NAT

Arquitectura

El siguiente diagrama muestra cómo usar Network Firewall para recopilar datos de SNI del tráfico de red saliente y, a continuación, publicar esos datos en un tema de SNS mediante Logs CloudWatch y Lambda.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Network Firewall recopila los nombres de dominio de los datos del SNI del encabezado HTTPS del tráfico de red saliente.
2. CloudWatch Logs supervisa los datos del SNI e invoca una función Lambda cada vez que el tráfico de red saliente pasa a través de Network Firewall.
3. La función Lambda lee los datos del SNI capturados por los CloudWatch registros y, a continuación, los publica en un tema de SNS.
4. El tema de SNS le envía una notificación por correo electrónico que incluye los datos del SNI.

Automatizar y escalar

- Puede usar AWS CloudFormation para crear este patrón mediante el uso de la infraestructura como código.

Pila de tecnología

- Amazon CloudWatch Logs
- Amazon SNS
- Amazon VPC
- AWS Lambda
- AWS Network Firewall

Herramientas

Servicios de AWS

- Amazon CloudWatch Logs: puede usar Amazon CloudWatch Logs para monitorear, almacenar y acceder a sus archivos de registro desde instancias de Amazon Elastic Compute Cloud (Amazon EC2), CloudTrail AWS, Amazon Route 53 y otras fuentes.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) es un servicio administrado con el que se ofrece la entrega de mensajes de los publicadores a los suscriptores (también conocido como productores y consumidores).
- Amazon VPC: Amazon Virtual Private Cloud (Amazon VPC) le permite aprovisionar una sección aislada de forma lógica de la nube de AWS donde puede lanzar recursos de AWS en una red virtual que haya definido. Dicha red virtual es prácticamente idéntica a las redes tradicionales que se utilizan en sus propios centros de datos, con los beneficios que supone utilizar la infraestructura escalable de AWS.
- AWS Lambda: AWS Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores.
- AWS Network Firewall: AWS Network Firewall es un servicio administrado que facilita la implementación de las protecciones de red esenciales para todas sus VPC de Amazon.

Epics

Crear un grupo de CloudWatch registros para Network Firewall

Tarea	Descripción	Habilidades requeridas
Cree un grupo de CloudWatch registros.	1. Inicie sesión en la consola de administración de AWS y abra la CloudWatch consola. 2. En el panel de navegación, selecione Grupos de registro. 3. Elija Actions (Acciones) y, a continuación, elija Create log group (Crear grupo de registros). 4. Escriba el nombre del grupo de registros y, a continuación, seleccione Crear grupo de registros. Para obtener más información, consulte Trabajar con grupos de registros y flujos de registros en la CloudWatch documentación.	Administrador de la nube

Crear un tema de SNS y una suscripción

Tarea	Descripción	Habilidades requeridas
Cree un tema de SNS.	Para crear un tema de SNS, siga las instrucciones de la	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	documentación de Amazon SNS.	
Suscriba un punto de conexión a un tema SNS.	Para suscribir una dirección de correo electrónico como punto de conexión al tema de SNS que ha creado, siga las instrucciones de la documentación de Amazon SNS. En Protocolo, elija Email/Email-JSON. Nota: También puede elegir un punto de conexión diferente en función de sus requisitos.	Administrador de la nube

Configurar el registro en Network Firewall

Tarea	Descripción	Habilidades requeridas
Habilite el registro de firewall.	1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon VPC. 2. En el panel de navegación, en NETWORK FIREWALL, elija Firewalls. 3. En la sección Firewalls, elija el firewall en el que desee capturar el nombre del servidor del SNI para el tráfico saliente. 4. Seleccione la pestaña de Detalles del firewall y, a	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	continuación, elija Editar en la sección Registro. 5. En Tipo de registro, seleccione Alerta. En el destino del registro para las alertas, selecciona el grupo de CloudWatch registros. 6. Para el grupo de CloudWatch registros, busque y elija el grupo de registros que creó anteriormente y, a continuación, elija Guardar. Para obtener más información sobre el uso de CloudWatch Logs como destino de registro para Network Firewall, consulte Amazon CloudWatch Logs en la documentación de Network Firewall.	

Configurar una regla con estado en Network Firewall

Tarea	Descripción	Habilidades requeridas
Crear un grupo de reglas con estado.	1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon VPC. 2. En el panel de navegación, en NETWORK FIREWALL,	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	seleccione Grupos de regla de Network Firewall. 3. Elija Crear grupo de reglas de Network Firewall. 4. En la página de grupo Crear grupo de reglas de Network Firewall, para el Tipo de grupo de reglas, elija Grupo de reglas con estado. Nota: Para obtener más información, consulte Trabajar con grupos de reglas con estado en AWS Network Firewall. 5. En la sección Grupo de reglas con estado, introduzca un nombre y una descripción para el grupo de reglas. 6. En Capacidad, defina la capacidad máxima que desea permitir para el grupo de reglas con estado (hasta un máximo de 30 000). Nota: No puede cambiar esta configuración después de crear el grupo de reglas. Para obtener información sobre cómo calcular la capacidad, consulte Configuración de la capacidad de los grupos de reglas en AWS Network Firewall. Para	

Tarea	Descripción	Habilidades requeridas
	obtener información sobre la configuración máxima, consulte Cuotas de AWS Network Firewall. 7. Para Opciones de grupos de reglas con estado, seleccione 5-tuple. 8. En la sección Orden de reglas con estado, seleccione Predeterminado. 9. En la sección Variables de regla, mantenga los valores predeterminados. 10. En la sección Agregar regla, elija TLS para Protocolo. En Origen, elija Cualquiera. En Puerto de origen, elija Cualquier puerto. En Destino, seleccione Cualquier a. En Puerto de destino, seleccione Cualquier puerto. En Dirección del tráfico, seleccione Adelante. En Acción, seleccione Alerta. Seleccione Agregar regla. 11. Elija Crear grupo de reglas con estado.	

Tarea	Descripción	Habilidades requeridas
Asocie la regla con estado a Network Firewall.	1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon VPC. 2. En el panel de navegación, en NETWORK FIREWALL, elija Firewalls. 3. Elija el firewall en el que desee capturar el nombre del servidor del SNI para el tráfico saliente. 4. En la sección Grupos de reglas con estado, elija Acciones y, a continuac ión, elija Agregar grupos de reglas con estado no administrados. 5. En la página Agregar grupos de reglas con estado no administrados, seleccione el grupo de reglas con estado que creó anteriormente y, a continuación, elija Agregar grupo de reglas con estado.	Administrador de la nube

Cree una función de Lambda para leer los registros

Tarea	Descripción	Habilidades requeridas
Crear el código para la función de Lambda.	En un entorno de desarroll o integrado (IDE) que pueda leer el evento CloudWatch	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	Logs de Network Firewall para el tráfico saliente, pegue el siguiente código de Python 3 y <SNS-topic-ARN> sustitúyalo por su valor: `import json` `import gzip` `import base64` `import boto3` `sns_client = boto3.client('sns')` `def lambda_handler(event, context):` `  decoded_event = json.loads(gzip.decompress(base64.b64decode(event['awslogs']['data'])))` `  body = '''` `  {filtermatch}` `  '''.format(` `  loggroup=decoded_event['logGroup'],` `  logstream=decoded_event['logStream'],` `  filtermatch=decoded_event['logEvents'][0]['message'],` `  )` `  print(body)` `  filterMatch = json.loads(body)` `  data = []` `  if 'http' in filterMatch['event']:` `  data.append(filterMatch['ev`	

Tarea	Descripción	Habilidades requeridas
	<pre>ent']['http']['hos tname']) elif 'tls' in filterMatch['event']: data.appe nd(filterMatch['ev ent']['tls']['sni']) result = 'Domain accessed ' + 1*' ' + (data[0]) + 1*' ' 'via AWS Network Firewall ' + 1*' ' + (filterMa tch['firewall_name']) print(result) message = {'ServerN ame': result} send_to_sns = sns_client.publish(TargetArn=<SNS- topic-ARN>, #Replace with the SNS topic ARN Message=j son.dumps({'default': json.dumps(message), 'sms': json.dump s(message), 'email': json.dump s(message)}), Subject='Server Name passed through the Network Firewall', MessageSt ructure='json')</pre> Este ejemplo de código analiza el contenido de CloudWatch los registros y	

Tarea	Descripción	Habilidades requeridas
	captura el nombre del servidor proporcionado por el SNI en el encabezado HTTPS.	
Crear la función de Lambda.	Para crear la función de Lambda, siga las instrucciones de la documentación de Lambda y elija Python 3.9 para el Tiempo de ejecución.	Administrador de la nube
Añada el código a la función de Lambda.	Para añadir el código Python a la función de Lambda que creó anteriormente, siga las instrucciones de la documentación de Lambda.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
Agregue CloudWatch registros como activador a la función Lambda.	1. Inicie sesión en la consola de administración de AWS y abra la consola de Lambda. 2. En el panel de navegación, seleccione Funciones y, a continuación, elija la función que creó anteriormente. 3. En la sección Informaci ón general de la función, seleccione Agregar desencadenador. 4. En la página Agregar activador, en la sección Configuración del disparado r, elija CloudWatch Registros y, a continuación, elija Agregar. 5. En Grupo de registros, elija el grupo de CloudWatch registros que creó anteriorm ente. 6. En Nombre del filtro, especifique un nombre para el filtro. 7. Seleccione Agregar. 8. En la pestaña Configura ción de la página de la función, en la sección Activadores, seleccione el activador que acabas de añadir y, a continuación, seleccione Activar.	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	Para obtener más información, consulte Uso de Lambda con CloudWatch registros en la documentación de Lambda.	

Tarea	Descripción	Habilidades requeridas
Agregue permisos de publicación de SNS.	Agregue el permiso sns:Publish a la función de ejecución de Lambda para que Lambda pueda realizar llamadas a la API para publicar mensajes en SNS. 1. Busque el rol de ejecución de la función de Lambda que creó anteriormente. 2. Agregue la siguiente política a su AWS Identity and Access Management (rol de IAM): `{ "Version": "2012-10-17", "Statement": [ { "Sid": "AllowSNSPublish", "Effect": "Allow", "Action": [ "sns:GetTopicAttributes", "sns:Subscribe", "sns:Unsubscribe", "sns:Publish" ], "Resource": "*" }`	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	<pre>] }</pre>	

Pruebe la funcionalidad de su notificación de SNS

Tarea	Descripción	Habilidades requeridas
Envíe tráfico a través de Network Firewall.	1. Envíe o espere a que el tráfico HTTPS pase a través de Network Firewall. 2. Compruebe el correo electrónico de notificación de SNS que recibe de AWS cuando el tráfico pasa a través de Network Firewall. El correo electrónico incluye los detalles del SNI del tráfico saliente. Por ejemplo, el correo electrónico generado a partir del código de Lambda anterior tendrá el siguiente contenido si el nombre de dominio al que se ha accedido es https://aws.amazon.com y el protocolo de suscripción es EMAIL-JSON: <pre>{ "Type": "Notification", "MessageId": "<messageID>",</pre>	Ingeniero de pruebas

Tarea	Descripción	Habilidades requeridas
	<pre>"TopicArn": "arn:aws:sns:us-west-2:123456789:testSNSTopic", "Subject": "Server Name passed through the Network Firewall", "Message": "{\"ServerName\": \"Domain 'aws.amazon.com' accessed via AWS Network Firewall 'AWS-Network-Firewall-Multi-AZ-firewall\"}", "Timestamp": "2022-03-22T04:10:04.217Z", "SignatureVersion": "1", "Signature": "<Signature>", "SigningCertURL": "<SigningCertUrl>", "UnsubscribeURL": "<UnsubscribeURL>" }</pre> A continuación, consulte el registro de alertas de Network Firewall en Amazon CloudWatch siguiendo las instrucciones de la CloudWatch documentación de Amazon. El registro de alerta muestra el siguiente resultado: <pre>{</pre>	

Tarea	Descripción	Habilidades requeridas
	"firewall_name": "AWS-Network-Firewall-Multi-AZ-firewall", "availability_zone": "us-east-2b", "event_timestamp": "<event timestamp>", "event": { "timestamp": "2021-03-22T04:10:04.214222+0000", "flow_id": <flow ID>, "event_type": "alert", "src_ip": "10.1.3.76", "src_port": 22761, "dest_ip": "99.86.59.73", "dest_port": 443, "proto": "TCP", "alert": { "action": "allowed", "signature_id": 2, "rev": 0, "signature": "", "category": "", "severity": 3 }, "tls": { "subject": "CN=aws.amazon.com",	

Tarea	Descripción	Habilidades requeridas
	"issuerdn ": "C=US, O=Amazon, OU=Server CA 1B, CN=Amazon", "serial": "<serial number>", "fingerpr int": "<fingerprint ID>", "sni": "aws.amazon.com", "version": "TLS 1.2", "notbefor e": "2020-09-30T00:00: 00", "notafter ": "2021-09-23T12:00: 00", "ja3": {}, "ja3s": {} }, "app_proto": "tls" } }	

Usa Terraform para habilitar Amazon automáticamente GuardDuty para una organización

Creado por Aarthi Kannan (AWS)

Repositorio de código: - amazon-guardduty-for-aws organizations-with-terraform	Entorno: producción	Tecnologías: seguridad, identidad y cumplimiento; nativas de la nube; DevOps
Carga de trabajo: todas las demás cargas de trabajo	Servicios de AWS: Amazon GuardDuty; AWS Organizations	

Resumen

Amazon supervisa GuardDuty continuamente sus cuentas de Amazon Web Services (AWS) y utiliza información sobre amenazas para identificar actividades inesperadas y potencialmente maliciosas en su entorno de AWS. La activación manual GuardDuty de varias cuentas u organizaciones, en varias regiones de AWS o a través de la consola de administración de AWS puede resultar engorrosa. Puede automatizar el proceso mediante una herramienta de infraestructura como código (IaC) como Terraform, capaz de aprovisionar y administrar servicios y recursos de múltiples cuentas y regiones en la nube.

AWS recomienda usar AWS Organizations para configurar y administrar varias cuentas en GuardDuty. Este patrón sigue dicha recomendación. Una de las ventajas de este enfoque es que, cuando se creen o agreguen nuevas cuentas a la organización, se GuardDuty habilitarán automáticamente en estas cuentas para todas las regiones compatibles, sin necesidad de intervención manual.

Este patrón muestra cómo usar HashiCorp Terraform para habilitar Amazon GuardDuty para tres o más cuentas de Amazon Web Services (AWS) en una organización. El código de ejemplo proporcionado en este patrón hace lo siguiente:

- Se habilita GuardDuty para todas las cuentas de AWS que son miembros actuales de la organización objetivo en AWS Organizations

- Activa la función de activación automática en GuardDuty, que se habilita automáticamente GuardDuty para cualquier cuenta que se añada a la organización de destino en el futuro
- Te permite seleccionar las regiones en las que quieres activarlas GuardDuty
- Utiliza la cuenta de seguridad de la organización como GuardDuty administrador delegado
- Crea un depósito de Amazon Simple Storage Service (Amazon S3) en la cuenta de registro y se GuardDuty configura para publicar los resultados agregados de todas las cuentas de este depósito
- Asigna una política de ciclo de vida que, de forma predeterminada, transfiere los resultados del bucket de S3 al almacenamiento de Amazon S3 Glacier Flexible Retrieval después de 365 días

Puede ejecutar manualmente este código de ejemplo o bien integrarlo en su proceso de integración y entrega continuas (CI/CD).

Público objetivo

Este patrón se recomienda para los usuarios que tengan experiencia con Terraform GuardDuty, Python y AWS Organizations.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una organización configurada en AWS Organizations que contenga, al menos, las tres cuentas siguientes:
  - Una cuenta de administración: esta es la cuenta desde la que se implementa el código de Terraform, ya sea de forma independiente o como parte del proceso de CI/CD. El estado de Terraform también se almacena en esta cuenta.
  - Una cuenta de seguridad: esta cuenta se utiliza como administrador GuardDuty delegado. Para obtener más información, consulte Consideraciones importantes para los administradores GuardDuty delegados (GuardDuty documentación).
  - Una cuenta de registro: esta cuenta contiene el depósito de S3, donde se GuardDuty publican los resultados agregados de todas las cuentas de los miembros.

  Para obtener más información sobre cómo configurar la organización con los ajustes requeridos, consulte Crear una estructura de cuentas (AWS Well-Architected Labs).
- Un bucket de Amazon S3 y una tabla de Amazon DynamoDB que sirvan como backend remoto para almacenar el estado de Terraform en la cuenta de administración. Para obtener más

información sobre el uso de backends remotos para el estado de Terraform, consulte los backends de S3 (documentación de Terraform). Para ver un ejemplo de código que configura la administración remota del estado con un backend de S3, consulte remote-state-s3-backend (Terraform Registry). Tenga en cuenta los siguientes requisitos:

  - El bucket de S3 y la tabla de DynamoDB deben estar en la misma región.
  - Al crear la tabla de DynamoDB, la clave de partición debe ser `LockID` (distingue entre mayúsculas y minúsculas), y el tipo de clave de partición debe ser String. Todos los demás valores de la tabla deben estar en sus valores predeterminados. Para obtener más información, consulte Acerca de las claves principales y Creación de una tabla (documentación de DynamoDB).

- Un depósito de S3 que se utilizará para almacenar los registros de acceso del depósito de S3 en el que GuardDuty se publicarán los resultados. Para obtener más información, consulte Habilitar el registro de acceso al servidor de Amazon S3 (documentación de Amazon S3). Si va a realizar la implementación en una zona de aterrizaje de AWS Control Tower, puede reutilizar el bucket de S3 de la cuenta del archivo de registros para este fin.
- Terraform version 0.14.6 o versión posterior, instalada y configurada. Para obtener más información, consulte Introducción - AWS (documentación de Terraform).
- Python versión 3.9.6 o una versión posterior, instalada y configurada. Para obtener más información, consulte Versiones de origen (sitio web de Python).
- AWS SDK para Python (Boto3) instalado. Para obtener más información, consulte Instalación (documentación de Boto3).
- jq está instalado y configurado. Para obtener más información, consulte Descargar jq (documentación de jq).

Limitaciones

- Este patrón es compatible con los sistemas operativos macOS y Amazon Linux 2. No se ha probado el uso de este patrón en sistemas operativos Windows.
- GuardDuty no debe estar ya habilitado en ninguna de las cuentas ni en ninguna de las regiones de destino.
- La solución IaC de este patrón no implementa los requisitos previos.
- Este patrón ha sido diseñado para una AWS Landing Zone que satisfaga las siguientes prácticas recomendadas:
  - Zona de aterrizaje creada mediante AWS Control Tower.

- Cuentas de AWS independientes para la seguridad y el registro.

Versiones de producto

- Versión de Terraform 0.14.6 o posterior. El código de ejemplo se ha probado en la versión 1.2.8.
- Python, versión 3.9.6 o posterior.

Arquitectura

En esta sección se ofrece información general de alto nivel sobre esta solución y la arquitectura establecida en el código de ejemplo. El siguiente diagrama muestra los recursos implementados en las distintas cuentas de la organización, dentro de una única región de AWS.

1. Terraform crea el rol GuardDutyTerraformOrgRoleAWS Identity and Access Management (IAM) en la cuenta de seguridad y en la cuenta de registro.
2. Terraform crea un bucket de S3 en la región de AWS predeterminada de la cuenta de registro. Este segmento se usa como destino de publicación para agregar todos los GuardDuty hallazgos de todas las regiones y de todas las cuentas de la organización. Terraform también crea una clave de AWS Key Management Service (AWS KMS) en la cuenta de seguridad usada para cifrar los resultados del bucket de S3, y configura el archivo automático de los resultados del bucket de S3 en el almacenamiento de S3 Glacier Flexible Retrieval.
3. Desde la cuenta de administración, Terraform designa la cuenta de seguridad como la administradora delegada. GuardDuty Esto significa que la cuenta de seguridad ahora administra el GuardDuty servicio para todas las cuentas de los miembros, incluida la cuenta de administración. Las cuentas de los miembros individuales no se pueden suspender ni deshabilitar GuardDuty por sí mismas.
4. Terraform crea el GuardDuty detector en la cuenta de seguridad para el administrador GuardDuty delegado.
5. Si aún no está activado, Terraform habilita la protección de S3. GuardDuty Para obtener más información, consulte la protección de Amazon S3 en Amazon GuardDuty (GuardDuty documentación).
6. Terraform inscribe como miembros a todas las cuentas actuales y activas de la organización. GuardDuty

7. Terraform configura al administrador GuardDuty delegado para que publique los resultados agregados de todas las cuentas de los miembros en el segmento S3 de la cuenta de registro.
8. Terraform repite los pasos 3 a 7 para cada región de AWS que elija.

Automatizar y escalar

El código de muestra proporcionado está modularizado para que pueda integrarlo en su proceso de CI/CD con el fin de lograr una implementación automatizada.

Herramientas

Servicios de AWS

- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- Amazon GuardDuty es un servicio de supervisión continua de la seguridad que analiza y procesa los registros para identificar actividades inesperadas y potencialmente no autorizadas en su entorno de AWS.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Key Management Service (AWS KMS) le ayuda a crear y controlar claves criptográficas para proteger sus datos.
- AWS Organizations es un servicio de administración de cuentas que le permite agrupar varias cuentas de AWS en una organización que usted crea y administra de manera centralizada.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS SDK para Python (Boto3) es un kit de desarrollo de software que permite integrar su aplicación, biblioteca o script de Python con los servicios de AWS.

Otras herramientas y servicios

- HashiCorp Terraform es una aplicación de interfaz de línea de comandos que le ayuda a usar código para aprovisionar y administrar la infraestructura y los recursos de la nube.
- Python es un lenguaje de programación informático de uso general.
- jq es un procesador de línea de comandos que le ayuda a trabajar con archivos JSON.

Repositorio de código

El código de este patrón está disponible en el GitHub repositorio -. amazon-guardduty-for-aws organizations-with-terraform

Epics

Habilitar GuardDuty en la organización

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	En un intérprete de comandos de Bash, ejecute el siguiente comando. En Clonar el repositorio, en la sección de información adicional, puedes copiar el comando completo que contiene la URL del GitHub repositorio. Esto clona el organizations-with-terraform repositorio amazon-guardduty-for-aws- desde GitHub. `git clone <github-repository-url>`	DevOps ingeniero
Edite el archivo de configuración de Terraform.	1. En la carpeta `root` del repositorio clonado, replique el archivo configuration.json.sample ejecutando el siguiente comando. `cp configuration.json.sample configuration.json` 2. Edite el nuevo archivo configuration.json y defina	DevOps ingeniero, AWS general, Terraform, Python

Tarea	Descripción	Habilidades requeridas
	los valores de cada una de las siguientes variables: • `management_acc_id` – ID de cuenta de la cuenta de administración. • `delegated_admin_acc_id` – ID de cuenta de la cuenta de seguridad. • `logging_acc_id` – ID de cuenta de la cuenta de registro. • `target_regions` — Lista separada por comas de las regiones de AWS en las que desea activarlas. GuardDuty • `organization_id` — ID de AWS Organizations de la organización en la que está realizando la activación GuardDuty. • `default_region` – Región en la que se almacena su estado de Terraform en la cuenta de administración. Es la misma región en la que implementó el bucket de S3 y la tabla de DynamoDB para el backend de Terraform. • `role_to_assume_for_role_creation`	

Tarea	Descripción	Habilidades requeridas
	– Nombre que desea asignar a un nuevo rol de IAM en las cuentas de seguridad y registro. Creará este nuevo rol en la siguiente historia. Terraform asume este rol para crear el rol de IAM `GuardDutyTerraformOrgRole` en las cuentas de seguridad y registro. • `finding_publishing_frequency` — Frecuencia con la que se GuardDuty publican los resultados en el segmento S3. • `guardduty_findings_bucket_region` – Región preferida en la que desea crear el bucket de S3 para los resultados publicados. • `logging_acc_s3_bucket_name` – Nombre preferido del bucket de S3 para los resultados publicados. • `security_acc_kms_key_alias` — Alias de AWS KMS para la clave utilizada para cifrar GuardDuty los hallazgos.	

Tarea	Descripción	Habilidades requeridas
	• `s3_access_log_bucket_name` — Nombre de un depósito de S3 preexistente en el que desea recopilar los registros de acceso del depósito de S3 utilizado para GuardDuty las búsquedas. Este depósito debe estar en la misma región de AWS que el depósito de GuardDuty hallazgos. • `tfm_state_backend_s3_bucket` – Nombre del bucket de S3 preexistente para almacenar el estado del backend remoto de Terraform. • `tfm_state_backend_dynamodb_table` – Nombre de la tabla de DynamoDB preexistente para bloquear el estado de Terraform. 3. Guarde y cierre el archivo de configuración.	

Tarea	Descripción	Habilidades requeridas
Genere CloudFormation plantillas para nuevas funciones de IAM.	Este patrón incluye una solución de IaC para crear dos CloudFormation plantilla s. Estas plantillas crean dos roles de IAM que Terraform usará durante el proceso de configuración. Estas plantilla s satisfacen las prácticas recomendadas de seguridad de permisos con privilegio mínimo. 1. En un intérprete de comandos de Bash, en la carpeta `root` del repositor io, acceda a `cfn-templ ates/` . Esta carpeta contiene archivos de CloudFormation plantillas con talones. 2. Ejecute el siguiente comando de la . Este paso reemplaza los stubs por los valores que proporcionó en el archivo configuration.json . `bash scripts/r eplace_config_stub s.sh` 3. Confirme que se hayan creado CloudFormation las siguientes plantillas	DevOps ingeniero, AWS general

Tarea	Descripción	Habilidades requeridas
	en la `cfn-templates/` carpeta: • management-account-role.yaml: este archivo contiene la definición del rol y los permisos asociados al rol de IAM en la cuenta de administración, que tiene los permisos mínimos necesarios para completar este patrón. • role-to-assume-for-role-creation.yaml: este archivo contiene la definición del rol y los permisos asociados al rol de IAM en las cuentas de seguridad y registro. Terraform asume esta función para crear la función en estas cuentas. GuardDutyTerraform OrgRole	

Tarea	Descripción	Habilidades requeridas
Cree el rol de IAM.	Siguiendo las instrucciones de Creación de una pila (CloudFormation documentación), haga lo siguiente: 1. Implemente la pila role-to-assume-for-role-creation.yaml tanto en la cuenta de seguridad como en la de registro. 2. Implemente la pila .yaml en la cuenta de administraciónmanagement-account-role. Cuando haya creado correctamente la pila y el resultado muestre el estado `CREATE_COMPLETE` , anote el nombre de recurso de Amazon (ARN) de este nuevo rol.	DevOps ingeniero, AWS general
Asuma el rol de IAM de la cuenta de administración	Como práctica recomendada de seguridad, le recomendamos que asuma la nueva función de management-account-roleIAM antes de continuar. En la interfaz de la línea de comandos de AWS (AWS CLI), ejecute el comando de Asumir el rol de IAM de la cuenta de administración, en la sección Información adicional.	DevOps ingeniero, AWS general

Tarea	Descripción	Habilidades requeridas
Ejecute el script de configuración.	En la carpeta `root` del repositorio, ejecute el siguiente comando para iniciar el script de configuración. `bash scripts/full-setup.sh` El script full-setup.sh realiza las siguientes acciones: • Exporta todos los valores de configuración como variables de entorno • Genera los archivos de código backend.tf y terraform.tfvars para cada módulo de Terraform • Permite un acceso confiable a GuardDuty la organización a través de la AWS CLI. • Importa el estado de la organización al estado de Terraform • Crea el bucket de S3 para publicar los resultados en la cuenta de registro • Crea la clave de AWS KMS para cifrar los resultados en la cuenta de seguridad • Se habilita GuardDuty en toda la organización y en todas las regiones seleccionadas, tal y como se describe	DevOps ingeniero, Python

Tarea	Descripción	Habilidades requeridas
	en la sección de arquitectura	

(Opcional) Desactivar GuardDuty en la organización

Tarea	Descripción	Habilidades requeridas
Ejecute el script de limpieza.	Si utilizó este patrón GuardDuty para activarlo en la organización y desea deshabilitarlo GuardDuty, ejecute el siguiente comando en la `root` carpeta del repositorio para iniciar el script cleanup-gd.sh. `bash scripts/cleanup-gd.sh` Este script se desactiva GuardDuty en la organización de destino, elimina todos los recursos desplegados y restaura la organización a su estado anterior antes de utilizar Terraform para activarlo. GuardDuty Nota: Este script no elimina los archivos de estado de Terraform ni bloquea los archivos de los backends locales y remotos. Si necesita hacerlo, debe llevar a cabo estas acciones manualmente. Este script tampoco elimina	DevOps ingeniero, AWS general, Terraform, Python

Tarea	Descripción	Habilidades requeridas
	la organización importada ni las cuentas que gestiona. El acceso seguro para GuardDuty no está desactiva do como parte del script de limpieza.	
Elimine los roles de IAM.	Elimine las pilas que se crearon con las plantilla s role-to-assume-for-role-creation.yaml y .yaml. management-account-role CloudFormation Para obtener más información, consulta Eliminar una pila (document ación). CloudFormation	DevOps ingeniero, AWS general

Recursos relacionados

Documentación de AWS

- Administrar varias cuentas (GuardDuty documentación)
- Otorgar privilegio mínimo (documentación de IAM)

Marketing de AWS

- Amazon GuardDuty
- AWS Organizations

Otros recursos

- Terraform
- Documentación de Terraform CLI

Información adicional

Clone el repositorio

Ejecute el siguiente comando para clonar el GitHub repositorio.

```
git clone https://github.com/aws-samples/amazon-guardduty-for-aws-organizations-with-terraform
```

Asuma el rol de IAM de la cuenta de administración

Para asumir el rol de IAM en la cuenta de administración, ejecute el siguiente comando. Sustituya `<IAM role ARN>` con el ARN del rol de IAM.

```
export ROLE_CREDENTIALS=$(aws sts assume-role --role-arn <IAM role ARN> --role-session-name AWSCLI-Session --output json)
export AWS_ACCESS_KEY_ID=$(echo $ROLE_CREDENTIALS | jq .Credentials.AccessKeyId | sed 's/"//g')
export AWS_SECRET_ACCESS_KEY=$(echo $ROLE_CREDENTIALS | jq .Credentials.SecretAccessKey | sed 's/"//g')
export AWS_SESSION_TOKEN=$(echo $ROLE_CREDENTIALS | jq .Credentials.SessionToken | sed 's/"//g')
```

Compruebe que los nuevos clústeres de Amazon Redshift tengan puntos de conexión SSL necesarios

Creado por Priyanka Chaudhary (AWS)

Entorno: producción	Tecnologías: seguridad, identidad; conformidad; análisis; lagos de datos	Servicios de AWS: AWS CloudTrail; Amazon CloudWatch Events; Amazon Redshift; Amazon SNS; AWS Lambda

Resumen

Este patrón proporciona una CloudFormation plantilla de Amazon Web Services (AWS) que le notifica automáticamente cuando se lanza un nuevo clúster de Amazon Redshift sin puntos de enlace de Secure Sockets Layer (SSL).

Amazon Redshift es un servicio de almacenamiento de datos en la nube de varios petabytes totalmente administrado. Está diseñado para el almacenamiento y el análisis de conjuntos de datos a gran escala. También se utiliza para realizar migraciones de bases de datos a gran escala. Por motivos de seguridad, Amazon Redshift admite SSL para cifrar la conexión entre la aplicación cliente de SQL Server del usuario y el clúster de Amazon Redshift. Para configurar que su clúster requiera una conexión SSL, establezca el parámetro `require_SSL` en `true` en el grupo de parámetros asociado al clúster durante el lanzamiento.

El control de seguridad que se proporciona con este patrón monitorea las llamadas a la API de Amazon Redshift en CloudTrail los registros de AWS e inicia un evento de Amazon CloudWatch Events para las API CreateCluster, ModifyCluster, RestoreFromClusterSnapshotCreateClusterParameterGroup, y. ModifyClusterParameterGroup Cuando el evento detecta una de estas API, llama a AWS Lambda, que ejecuta un script de Python. La función Python analiza el CloudWatch evento en busca de los CloudTrail eventos listados. Cuando se crea, modifica o restaura un clúster de Amazon Redshift a partir de una instantánea existente, se crea un nuevo grupo de parámetros para el clúster o se modifica un grupo de parámetros existente, la función comprueba el parámetro `require_SSL` del clúster. Si el valor del parámetro es `false`, la función envía una notificación de Amazon Simple Notification Service

(Amazon SNS) al usuario con la información pertinente: el nombre del clúster de Amazon Redshift, la región de AWS, la cuenta de AWS y el nombre de recurso de Amazon (ARN) para Lambda del que proviene esta notificación.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una nube privada virtual (VPC) con un grupo de subredes de clúster y un grupo de seguridad asociado.

Limitaciones

- Este control de seguridad es regional. Debe implementarlo en cada región de AWS que desee supervisar.

Arquitectura

Arquitectura de destino

Automatizar y escalar

- Si utiliza AWS Organizations, puede utilizar AWS Cloudformation StackSets para implementar esta plantilla en varias cuentas que desee supervisar.

Herramientas

Servicios de AWS

- AWS CloudFormation: AWS le CloudFormation ayuda a modelar y configurar sus recursos de AWS, a aprovisionarlos de forma rápida y coherente y a gestionarlos durante todo su ciclo de vida. Facilita poder usar una plantilla para describir los recursos y sus dependencias, y lanzarlos y configurarlos juntos como una pila, en lugar de administrarlos de forma individual.

- Amazon CloudWatch Events: Amazon CloudWatch Events ofrece una transmisión casi en tiempo real de los eventos del sistema que describen los cambios en los recursos de AWS.
- AWS Lambda: AWS Lambda es un servicio informático que permite ejecutar código sin aprovisionar ni administrar servidores.
- Amazon Redshift: Amazon Redshift es un servicio de almacenamiento de datos totalmente administrado de varios petabytes en la nube.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objeto. Puede utilizar Amazon S3 para almacenar y recuperar cualquier cantidad de datos en cualquier momento y desde cualquier parte de la web.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) coordina y gestiona la entrega o el envío de mensajes entre publicadores y clientes, incluyendo los servidores web y las direcciones de correo electrónico. Los suscriptores reciben todos los mensajes publicados de los temas a los que están suscritos y todos los suscriptores de un tema reciben los mismos mensajes.

Código

Este patrón incluye los siguientes archivos adjuntos:

- `RedshiftSSLEndpointsRequired.zip`: el código Lambda para el control de seguridad.
- `RedshiftSSLEndpointsRequired.yml`— La CloudFormation plantilla que configura el evento y la función Lambda.

Epics

Configure el bucket de S3

Tarea	Descripción	Habilidades requeridas
Elimine el bucket de S3.	En la consola Amazon S3, elija o cree un bucket de S3 para alojar el archivo .zip de código Lambda. Este bucket S3 deben estar en la misma región de AWS que el clúster de Amazon Redshift que	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	desea monitorizar. Un nombre de bucket S3 es globalmente único y todas las cuentas de AWS comparten el espacio de nombres. El nombre de bucket de S3 no puede incluir barras a la izquierda.	
Cargue el código Lambda.	Cargue el archivo .zip de código Lambda que se proporciona en la sección Adjuntos en el bucket S3.	Arquitecto de la nube

Implemente la plantilla CloudFormation

Tarea	Descripción	Habilidades requeridas
Lance la CloudFormation plantilla de AWS.	Abra la CloudFormation consola de AWS en la misma región de AWS que su bucket de S3 e implemente la plantilla adjunta`RedshiftSSLEndpointsRequired.yml` . Para obtener más información sobre la implementación de CloudFormation plantillas de AWS, consulte Crear una pila en la CloudFormation consola de AWS en la CloudFormation documentación.	Arquitecto de la nube
Complete los parámetros de la plantilla.	Al lanzar la plantilla, se le solicitará la siguiente información:	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	• Bucket de S3: especifique el bucket creado o seleccionado en la primera Epic. Aquí es donde cargó el código Lambda adjunto (archivo.zip). • Clave S3: especifique la ubicación del archivo .zip de Lambda en el bucket S3 (por ejemplo, nombre de archivo.zip o controls/nombre de archivo.zip). No incluya barras a la izquierda. • Correo de notificación: proporcione una dirección de email activa en la que desea recibir las notificaciones de Amazon SNS. • Nivel de registro Lamba: especifique el nivel y la frecuencia de registro de la función de Lambda. Utilice Info para registrar mensajes informativos detallados sobre el progreso, Error para los eventos de error que pudieran continuar con la implementación y Advertencia en caso de situaciones potencialmente dañinas.	

Confirmar la suscripción

Tarea	Descripción	Habilidades requeridas
Confirmar la suscripción.	Cuando la CloudFormation plantilla se implementa correctamente, envía un correo electrónico de suscripción a la dirección de correo electrónico que proporcionó. Debe confirmar esta suscripción de correo electrónico para recibir las notificaciones de infracciones.	Arquitecto de la nube

Recursos relacionados

- Creación de un bucket S3 (documentación de Amazon S3)
- Cargar de archivos en un bucket S3 (documentación de Amazon S3)
- Creación de una pila en la CloudFormation consola de AWS (CloudFormation documentación de AWS)
- Creación de una regla de CloudWatch eventos que se active en una llamada a la API de AWS mediante AWS CloudTrail (CloudTrail documentación de AWS)
- Creación de un clúster de Amazon Redshift (documentación de Amazon Redshift)
- Configuración de las opciones de seguridad para las conexiones (documentación de Amazon Redshift)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Compruebe que los nuevos clústeres de Amazon Redshift se lanzan en una VPC

Creado por Priyanka Chaudhary (AWS)

Entorno: producción	Tecnologías: seguridad, identidad y conformidad; análisis; bases de datos	Servicios de AWS: Amazon CloudWatch; AWS Lambda; Amazon Redshift

Resumen

Este patrón proporciona una CloudFormation plantilla de Amazon Web Services (AWS) que le notifica automáticamente cuando se lanza un clúster de Amazon Redshift fuera de una nube privada virtual (VPC).

Amazon Redshift es un servicio de almacenamiento de datos totalmente administrado de varios petabytes en la nube. Está diseñado para el almacenamiento y el análisis de conjuntos de datos a gran escala. También se utiliza para realizar migraciones de bases de datos a gran escala. Amazon Virtual Private Cloud (Amazon VPC) le permite aprovisionar una sección aislada de forma lógica de la nube de AWS donde puede lanzar recursos de AWS como clústeres de Amazon Redshift en una red virtual que defina.

El control de seguridad que se proporciona con este patrón monitorea las llamadas a la API de Amazon Redshift en CloudTrail los registros de AWS e inicia un evento de Amazon CloudWatch Events para las API y las CreateClusterAPI. RestoreFromClusterSnapshot Cuando el evento detecta una de estas API, llama a AWS Lambda, que ejecuta un script de Python. La función Python analiza el CloudWatch evento. Si se crea o restaura un clúster de Amazon Redshift a partir de una instantánea y aparece fuera de la red de Amazon VPC, la función envía una notificación de Amazon Simple Notification Service (Amazon SNS) al usuario con la información relevante: el nombre del clúster de Amazon Redshift, la región de AWS, la cuenta de AWS y el nombre de recurso de Amazon (ARN) para Lambda del que proviene esta notificación de.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una VPC con un grupo de subredes de clúster y un grupo de seguridad asociado.

Limitaciones

- La CloudFormation plantilla de AWS solo admite las RestoreFromClusterSnapshotacciones CreateClustery (nuevos clústeres). No detecta los clústeres de Amazon Redshift existentes que se crearon fuera de una VPC.
- Este control de seguridad es regional. Debe implementarlo en cada región de AWS que desee supervisar.

Arquitectura

Arquitectura de destino

Automatizar y escalar

Si utiliza AWS Organizations, puede utilizar AWS Cloudformation StackSets para implementar esta plantilla en varias cuentas que desee supervisar.

Herramientas

Servicios de AWS

- AWS CloudFormation: AWS le CloudFormation ayuda a modelar y configurar sus recursos de AWS, a aprovisionarlos de forma rápida y coherente y a gestionarlos durante todo su ciclo de vida. Facilita poder usar una plantilla para describir los recursos y sus dependencias, y lanzarlos y configurarlos juntos como una pila, en lugar de administrarlos de forma individual.
- AWS CloudTrail: AWS lo CloudTrail ayuda a implementar la gobernanza, el cumplimiento y la auditoría operativa y de riesgos de su cuenta de AWS. Las acciones realizadas por un usuario, un rol o un servicio de AWS se registran como eventos en CloudTrail.
- Amazon CloudWatch Events: Amazon CloudWatch Events ofrece una transmisión casi en tiempo real de los eventos del sistema que describen los cambios en los recursos de AWS.

- AWS Lambda: AWS Lambda es un servicio informático que permite ejecutar código sin aprovisionar ni administrar servidores. AWS Lambda ejecuta el código solo cuando es necesario y amplia la capacidad de manera automática, pasando de pocas solicitudes al día a miles por segundo.
- Amazon Redshift: Amazon Redshift es un servicio de almacenamiento de datos administrado de varios petabytes en la nube. Amazon Redshift está integrado en el lago de datos, lo que permite usar los datos para adquirir nueva información para su empresa y sus clientes.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos altamente escalable que se puede utilizar para una amplia gama de soluciones de almacenamiento, incluidos sitios web, aplicaciones móviles, copias de seguridad y lagos de datos.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) coordina y gestiona la entrega o el envío de mensajes entre publicadores y clientes, incluyendo los servidores web y las direcciones de correo electrónico.

Código

Este patrón incluye los siguientes archivos adjuntos:

- `RedshiftMustBeInVPC.zip`: el código Lambda para el control de seguridad.
- `RedshiftMustBeInVPC.yml`— La CloudFormation plantilla que configura el evento y la función Lambda.

Para usar el código de muestra, realice los pasos de la siguiente sección.

Epics

Configure el bucket de S3

Tarea	Descripción	Habilidades requeridas
Elimine el bucket de S3.	En la consola Amazon S3, elija o cree un bucket de S3 para alojar el archivo .zip de código Lambda. Este bucket S3 debe estar en la misma región de AWS que el clúster de Amazon Redshift que	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	desea monitorizar. Un nombre de bucket de S3 es globalmente único y todas las cuentas de AWS comparten el espacio de nombres. El nombre de bucket de S3 no puede incluir barras a la izquierda.	
Cargue el código Lambda.	Cargue el código Lambda (archivo `RedshiftMustBeInVPC.zip`) que se proporciona en la sección Adjuntos en el bucket S3.	Arquitecto de la nube

Implemente la plantilla CloudFormation

Tarea	Descripción	Habilidades requeridas
Lanza la CloudFormation plantilla.	Abra la CloudFormation consola de AWS en la misma región de AWS que su bucket de S3 e implemente la plantilla adjunta (`RedshiftMustBeInVPC.yml`). Para obtener más información sobre la implementación de CloudFormation plantillas de AWS, consulte Crear una pila en la CloudFormation consola de AWS en la CloudFormation documentación.	Arquitecto de la nube
Complete los parámetros de la plantilla.	Al lanzar la plantilla, se le solicitará la siguiente información:	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	• Bucket de S3: especifique el bucket creado o seleccionado en la primera Epic. Aquí es donde cargó el código Lambda adjunto (archivo.zip). • Clave S3: especifique la ubicación del archivo .zip de Lambda en el bucket S3 (por ejemplo, nombre de archivo.zip o controls/nombre de archivo.zip). No incluya barras a la izquierda. • Correo de notificación: proporcione una dirección de email activa en la que desea recibir las notificaciones de Amazon SNS. • Nivel de registro Lamba: especifique el nivel y la frecuencia de registro de la función de Lambda. Utilice Info para registrar mensajes informativos detallados sobre el progreso, Error para los eventos de error que pudieran continuar con la implementación y Advertencia en caso de situaciones potencialmente dañinas.	

Confirmar la suscripción

Tarea	Descripción	Habilidades requeridas
Confirmar la suscripción.	Cuando la CloudFormation plantilla se implementa correctamente, envía un correo electrónico de suscripción a la dirección de correo electrónico que proporcionó. Debe confirmar esta suscripción de correo electrónico para recibir las notificaciones de infracciones.	Arquitecto de la nube

Recursos relacionados

- Creación de un bucket S3 (documentación de Amazon S3)
- Cargar de archivos en un bucket S3 (documentación de Amazon S3)
- Creación de una pila en la CloudFormation consola de AWS (CloudFormation documentación de AWS)
- Creación de una regla de CloudWatch eventos que se active en una llamada a la API de AWS mediante AWS CloudTrail (CloudTrail documentación de AWS)
- Creación de un clúster de Amazon Redshift (documentación de Amazon Redshift)

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Más patrones

- Acceder a un host bastión mediante Session Manager y Amazon EC2 Instance Connect
- Acceda a las aplicaciones de contenedores de forma privada en Amazon ECS mediante AWS Fargate PrivateLink, AWS y un Network Load Balancer
- Acceda a las aplicaciones de contenedores de forma privada en Amazon ECS mediante AWS PrivateLink y un Network Load Balancer
- ???
- Permitir a las instancias de EC2 el acceso de escritura a los buckets de S3 en las cuentas de AMS
- Asocie un CodeCommit repositorio de AWS en una cuenta de AWS con SageMaker Studio en otra cuenta
- Automatice la adición o actualización de entradas de registro de Windows con AWS Systems Manager
- ???
- Adjunte automáticamente una política administrada de AWS para Systems Manager a los perfiles de instancia de EC2 mediante Cloud Custodian y AWS CDK
- Cifrar automáticamente los volúmenes de Amazon EBS nuevos y existentes
- Bloquee el acceso público a Amazon RDS mediante Cloud Custodian
- ???
- Consulte las aplicaciones o CloudFormation plantillas de CDK de AWS para conocer las prácticas recomendadas mediante los paquetes de reglas de cdk-nag
- Compruebe las instancias EC2 para ver si hay etiquetas obligatorias en el lanzamiento
- Configurar el acceso entre cuentas a Amazon DynamoDB
- Configure el cifrado HTTPS para Oracle JD Edwards EnterpriseOne en Oracle WebLogic mediante un Application Load Balancer
- Configure el registro y la supervisión de eventos de seguridad en su entorno de AWS IoT
- Configure autenticación TLS mutua para aplicaciones ejecutadas en Amazon EKS
- ???
- Crear una aplicación React con AWS Amplify y añadir autenticación con Amazon Cognito
- Crear un informe con los resultados del Analizador de acceso a la red sobre el acceso entrante a Internet en varias cuentas de AWS
- Personalice CloudWatch las alertas de Amazon para AWS Network Firewall

- Implemente un firewall con AWS Network Firewall y AWS Transit Gateway
- Documente el diseño de su zona de aterrizaje de AWS
- Habilite conexiones cifradas para instancias de base de datos de PostgreSQL en Amazon RDS
- Cifrar una instancia de base de datos de Amazon RDS para PostgreSQL existente
- Imponga el etiquetado automático de las bases de datos de Amazon RDS en el lanzamiento
- Imponga el etiquetado de los clústeres de Amazon EMR en el lanzamiento
- Asegúrese de que el registro de Amazon EMR en Amazon S3 esté habilitado en el lanzamiento
- Encuentre los recursos de AWS en función de su fecha de creación mediante las consultas avanzadas de AWS Config.
- Genere una CloudFormation plantilla de AWS que contenga las reglas administradas por AWS Config mediante Troposphere
- Reciba notificaciones de Amazon SNS cuando cambie el estado de clave de una clave de AWS KMS
- ???
- Identifique y avise cuando los recursos de Amazon Data Firehose no estén cifrados con una clave de AWS KMS
- Mejore el rendimiento operativo al habilitar Amazon DevOps Guru en varias regiones, cuentas y unidades organizativas de AWS con la AWS CDK
- Incorporar y migrar instancias de Windows de EC2 a una cuenta de AWS Managed Services
- Migrar Amazon RDS para Oracle a Amazon RDS para PostgreSQL en modo SSL mediante AWS DMS
- Migre ELK Stack a Elastic Cloud en AWS
- Migración de una carga de trabajo de F5 BIG-IP a F5 BIG-IP VE en la nube de AWS
- Supervisar Amazon Aurora en busca de instancias sin cifrado
- Rotar las credenciales de la base de datos sin reiniciar los contenedores
- Proteja y optimice el acceso de los usuarios a una base de datos de federación DB2 en AWS mediante contextos de confianza
- ???
- Sirva contenido estático en un bucket de Amazon S3 a través de una VPC mediante Amazon CloudFront
- Configure el end-to-end cifrado para aplicaciones en Amazon EKS mediante cert-manager y Let's Encrypt

- Verifique que los equilibradores de carga ELB requieran la terminación de TLS
- Vea los registros y las métricas de AWS Network Firewall mediante Splunk
- Visualice los informes de credenciales de IAM para todas las cuentas de AWS que utilizan Amazon QuickSight

Sin servidor

Temas

- Cree una aplicación móvil React Native sin servidor con AWS Amplify
- Entregue registros de DynamoDB a Amazon S3 mediante Kinesis Data Streams y Amazon Data Firehose con AWS CDK
- Integre Amazon API Gateway con Amazon SQS para gestionar las API REST asíncronas
- Procese eventos de forma asíncrona con Amazon API Gateway y AWS Lambda
- Procese eventos de forma asíncrona con Amazon API Gateway y Amazon DynamoDB Streams
- Procese eventos de forma asíncrona con Amazon API Gateway, Amazon SQS y AWS Fargate
- Ejecute las tareas de AWS Systems Manager Automation de forma sincrónica desde AWS Step Functions
- Ejecute lecturas paralelas de objetos de S3 mediante Python en una función de AWS Lambda
- Configure el acceso privado a un bucket de Amazon S3 a través de un punto de enlace de VPC
- Encadene los servicios de AWS mediante un enfoque sin servidor
- Más patrones

Cree una aplicación móvil React Native sin servidor con AWS Amplify

Creado por Deekshitulu Pentakota (AWS)

Repositorio de código: - aws-amplify-react-native ios-todo-app	Entorno: producción	Origen: NA
Objetivo: AWS Amplify AppSync, AWS, Amazon Cognito, Amazon DynamoDB	Tipo R: renovar arquitectura	Carga de trabajo: código abierto
Tecnologías: sin servidor; aplicaciones web y móviles	Servicios de AWS: AWS Amplify AppSync; AWS; Amazon Cognito; Amazon DynamoDB	

Resumen

Este patrón muestra cómo crear un backend sin servidor para una aplicación móvil React Native mediante AWS Amplify y los siguientes servicios de AWS:

- AWS AppSync
- Amazon Cognito
- Amazon DynamoDB

Tras configurar e implementar el backend de la aplicación mediante Amplify, Amazon Cognito autentica a los usuarios y los autoriza a acceder a la aplicación. AppSync A continuación, AWS interactúa con la aplicación de interfaz y con una tabla de DynamoDB de backend para crear y obtener datos.

Nota: Este patrón usa una simple aplicación «ToDoList» como ejemplo, pero puede usar un procedimiento similar para crear cualquier aplicación móvil de React Native.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Interfaz de la línea de comandos de Amplify (Amplify CLI) instalada y configurada
- XCode (cualquier versión)
- Microsoft Visual Studio (cualquier versión, cualquier editor de código, cualquier editor de texto)
- Familiaridad con Amplify
- Familiaridad con Amazon Cognito
- Familiaridad con AWS AppSync
- Familiaridad con DynamoDB
- Familiaridad con Node.js
- Familiarización con npm
- Familiaridad con React y React Native
- Familiaridad con ECMAScript JavaScript 6 (ES6)
- Familiaridad con GraphQL

Arquitectura

El siguiente diagrama muestra un ejemplo de arquitectura para ejecutar el backend de una aplicación móvil React Native en la nube de AWS:

En el siguiente diagrama se muestra la arquitectura:

1. Amazon Cognito autentica a los usuarios y los autoriza a acceder a la aplicación.
2. Para crear y obtener datos, AWS AppSync utiliza una API de GraphQL para interactuar con la aplicación de interfaz y una tabla de DynamoDB de backend.

Herramientas

Servicios de AWS

- AWS Amplify es un conjunto de herramientas y funciones diseñadas específicamente que permiten a los desarrolladores web y móviles front-end crear aplicaciones de pila completa en AWS de manera rápida.
- AWS AppSync proporciona una interfaz GraphQL escalable que ayuda a los desarrolladores de aplicaciones a combinar datos de varias fuentes, incluidas las API de Amazon DynamoDB, AWS Lambda y HTTP.
- Amazon Cognito ofrece autenticación, autorización y administración de usuarios para aplicaciones móviles y web.
- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.

Código

El código de la aplicación de muestra que se utiliza en este patrón está disponible en el repositorio -. GitHub aws-amplify-react-native ios-todo-app Para usar los archivos de ejemplo, siga las instrucciones de la sección Épica de este patrón.

Epics

Cree y ejecute su aplicación React Native

Tarea	Descripción	Habilidades requeridas
Configure un entorno de desarrollo React Native.	Para obtener instrucciones, consulte Configurar el entorno de desarrollo en la documenta ción de React Native.	Desarrollador de aplicaciones
Cree y ejecute la aplicación móvil ToDoList React Native en el simulador de iOS.	1. Cree un nuevo directorio de proyecto de aplicación móvil React Native en su entorno local ejecutando el siguiente comando en una nueva ventana de terminal:	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`npx react-native init ToDoListAmplify` 2. Navegue hasta el directorio raíz del proyecto ejecutando el siguiente comando: `cd ToDoListAmplify` 3. Ponga en marcha la aplicación ejecutando el siguiente comando: `npx react-native run-ios`	

Inicialice un nuevo entorno backend para la aplicación

Tarea	Descripción	Habilidades requeridas
Cree los servicios de backend necesarios para respaldar la aplicación en Amplify.	1. En tu entorno local, ejecuta el siguiente comando desde el directorio raíz del proyecto (ToDoListAmplify): `amplify init` 2. Aparecerá un mensaje solicitando informaci ón sobre la aplicación. Introduzca la información requerida en función del caso de uso. A continuac ión, pulse Intro.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	Para la configuración de la ToDoList aplicación utilizada en este patrón, aplique la siguiente configuración de ejemplo. Ejemplo de ajustes de configuración de aplicación React Native en Amplify `? Name: ToDoListAmplify` `? Environment: dev` `? Default editor: Visual Studio Code` `? App type: javascript` `? Javascript framework : react-native` `? Source Directory Path: src` `? Distribution Directory Path: /` `? Build Command: npm run-script build` `? Start Command: npm run-script start` `? Select the authentication method you want to use: AWS profile`	

Tarea	Descripción	Habilidades requeridas
	`? Please choose the profile you want to use: default` Para obtener más informaci ón, consulte Crear un nuevo backend de Amplify en la documentación de Amplify Dev Center. Nota: El `amplify init` comando proporciona los siguientes recursos mediante AWS CloudFormation: • Roles de AWS Identity and Access Management (IAM) para usuarios autenticados y no autenticados (rol Auth y rol Unauth) • Un bucket de Amazon Simple Storage Service (Amazon S3) para implementación (para la aplicación de ejemplo de este patrón, Amplify-m eta.json. • Un entorno de backend en Amplify Hosting	

Añada la autenticación de Amazon Cognito a su aplicación React Native de Amplify

Tarea	Descripción	Habilidades requeridas
Cree un servicio de autenticación de Amazon Cognito.	1. En su entorno local, ejecute el siguiente comando desde el directorio raíz del proyecto (ToDoListAmplify): `amplify add auth` 2. Aparecerá un mensaje solicitando información sobre los ajustes de configuración del servicio de autenticación. Introduzca la información requerida en función del caso de uso. A continuación, pulse Intro. Para la configuración de la ToDoList aplicación utilizada en este patrón, aplique la siguiente configuración de ejemplo. Ejemplo de ajustes de configuración del servicio de autenticación `? Do you want to use the default authentication and security configuration? \` `Default configuration` `? How do you want users to be able to sign in? \`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	Username ? Do you want to configure advanced settings? \ No, I am done Nota: El comando `amplify add auth` crea las carpetas, archivos y archivos de dependencia necesarios en una carpeta local (amplify) dentro del directorio raíz del proyecto. Para la configuración de la ToDoList aplicación utilizada en este patrón, se crea el archivo aws-exports.js con este fin.	

Tarea	Descripción	Habilidades requeridas
Implemente el servicio de Amazon Cognito en la nube de AWS.	1. Desde el directorio raíz del proyecto, ejecute el siguiente comando en la CLI de Amplify: `amplify push` 2. Aparecerá un mensaje para confirmar la implement ación. Introduzca Sí. A continuación, pulse Intro. Nota: Para ver los servicios implementados en su proyecto, acceda a la consola de Amplify ejecutando el siguiente comando: `amplify console`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Instala las bibliotecas Amplify necesarias para React Native y las CocoaPods dependencias para iOS.	1. Instale las bibliotecas cliente de código abierto de Amplify necesarias ejecutando el siguiente comando desde el directorio raíz del proyecto: `npm install aws-amplify aws-amplify-react-native \ amazon-cognito-identity-js @react-native-community/netinfo \ @react-native-async-storage/async-storage` 2. Instala CocoaPods las dependencias necesarias para iOS ejecutando el siguiente comando: `npx pod-install`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Importe y configure el servicio Amplify.	En el archivo de punto de entrada de la aplicación (por ejemplo, App.js), importe y cargue el archivo de configuración del servicio Amplify introduciendo las siguientes líneas de código: `import Amplify from 'aws-amplify'` `import config from './src/aws-exports'` `Amplify.configure(config)` Nota: Si recibe un error después de importar el servicio Amplify en el archivo de punto de entrada de la aplicación, deténgala. A continuación, abre XCode, selecciona el ToDoListAmplifyarchivo.xcworkspace de la carpeta iOS del proyecto y ejecuta la aplicación.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Actualice el archivo de punto de entrada de la aplicación para usar el componente de orden superior (HOC) withAuthenticator.	Nota: El HOC `withAuthenticator` proporciona flujos de trabajo para iniciar sesión, registrarse y recuperar contraseñas en su aplicación con unas pocas líneas de código. Para obtener más información, consulte Opción 1: usar componentes de interfaz de usuario precompilados en Amplify Dev Center. También puede consultar Componentes de orden superior en la documentación de React. 1. En el archivo de punto de entrada de la aplicación (por ejemplo,App.js), importe el HOC `withAuthenticator` introduciendo las siguientes líneas de código: `import { withAuthenticator } from 'aws-amplify-react-native'` 2. Exporte el HOC withAuthenticator introduciendo el siguiente código: `export default withAuthenticator(App)`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	Ejemplo de código de HOC withAuthenticator `import Amplify from 'aws-amplify'` `import config from './src/aws-exports'` `Amplify.configure(config)` `import { withAuthenticator } from 'aws-amplify-react-native';` `const App = () => {` `  return null;` `};` `export default withAuthenticator(App);` Nota: En el simulador de iOS, la aplicación muestra la pantalla de inicio de sesión proporcionada por el servicio Amazon Cognito.	

Tarea	Descripción	Habilidades requeridas
Pruebe la configuración del servicio de autenticación.	En el simulador de iOS, haga lo siguiente: 1. Cree una cuenta nueva en la aplicación con una dirección de correo electrónico real. Se enviará un código de verificación al correo electrónico registrado. 2. Verifique la cuenta configurada con el código que ha recibido en el correo electrónico de verificación. 3. Introduzca el nombre de usuario y la contraseña que ha creado. A continuación, seleccione Iniciar sesión. Aparecerá una pantalla de bienvenida. Nota: También puede abrir la consola de Amazon Cognito y comprobar si se ha creado un nuevo usuario en el grupo de identidades.	Desarrollador de aplicaciones

Conectar una AppSync API de AWS y una base de datos de DynamoDB a la aplicación

Tarea	Descripción	Habilidades requeridas
Cree una AppSync API de AWS y una base de datos de DynamoDB.	1. Añada una AppSync API de AWS a su aplicación y aprovisione automátic	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	amente una base de datos de DynamoDB ejecutando el siguiente comando de Amplify CLI desde el directorio raíz del proyecto: `amplify add api` 2. Aparecerá un aviso que le pedirá información sobre la API y los ajustes de configuración de la base de datos. Introduzca la información requerida en función del caso de uso. A continuación, pulse Intro. La CLI de Amplify abre el archivo de esquema de GraphQL en su editor de texto. Para la configuración de la ToDoList aplicación utilizada en este patrón, aplique la siguiente configuración de ejemplo. Ejemplo de ajustes de configuración de API y base de datos `? Please select from one of the below mentioned services: \ GraphQL`	

Tarea	Descripción	Habilidades requeridas
	? Provide API name: todolistamplify ? Choose the default authorization type for the API \ Amazon Cognito User Pool Do you want to use the default authentication and security configura tion ? Default configuration How do you want users to be able to sign in? \ Username Do you want to configure advanced settings? \ No, I am done. ? Do you want to configure advanced settings for the GraphQL API \ No, I am done. ? Do you have an annotated GraphQL schema? \ No ? Choose a schema template: \ Single object with fields (e.g., “Todo” with ID, name, description)	

Tarea	Descripción	Habilidades requeridas
	`` ? Do you want to edit the schema now? \ Yes ``` Ejemplo de esquema de GraphQL ``` type Todo @model { id: ID! name: String! description: String } ```	

Tarea	Descripción	Habilidades requeridas
Implemente la AppSync API de AWS.	1. Desde el directorio raíz del proyecto, ejecute el siguiente comando en la CLI de Amplify: `amplify push` 2. Aparecerá un aviso que le pedirá más información sobre la API y los ajustes de configuración de la base de datos. Introduzca la información requerida en función del caso de uso. A continuación, pulse Intro. Su aplicación ahora puede interactuar con la AppSync API de AWS. Para la configuración de la ToDoList aplicación utilizada en este patrón, aplique la siguiente configuración de ejemplo. Ejemplo de ajustes de configuración AppSync de la API de AWS Nota: La siguiente configura ción crea la API GraphQL en AWS AppSync y una tabla Todo en Dynamo DB. `? Are you sure you want to continue? Yes`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	? Do you want to generate code for your newly created GraphQL API Yes ? Choose the code generation language target javascript ? Enter the file name pattern of graphql queries, mutations and subscriptions src/ graphql/**/*.js ? Do you want to generate/update all possible GraphQL operations - \ queries, mutations and subscriptions Yes ? Enter maximum statement depth \ [increase from default if your schema is deeply nested] 2	

Tarea	Descripción	Habilidades requeridas
Conecta la interfaz de la aplicación a la AppSync API de AWS.	Para usar la ToDoList aplicación de ejemplo que se proporciona en este patrón, copie el código del archivo App.js del ios-todo-app GitHub repositorio aws-amplify-react-native-. A continuación, integre el código de ejemplo en su entorno local. El código de ejemplo proporcionado en el archivo App.js del repositorio hace lo siguiente: • Muestra el formulario para crear un ToDo elemento con los campos de título y descripción • Muestra la lista de tareas pendientes (Título y Descripción) • Publica y recupera datos mediante métodos de `aws-amplify`	Desarrollador de aplicaciones

Recursos relacionados

- AWS Amplify
- Amazon Cognito
- AWS AppSync
- Amazon DynamoDB
- React (documentación de React)

Entregue registros de DynamoDB a Amazon S3 mediante Kinesis Data Streams y Amazon Data Firehose con AWS CDK

Creado por Shashank Shrivastava (AWS) y Daniel Matuki da Cunha (AWS)

Repositorio de código: incorporación de Amazon DynamoDB a Amazon S3	Entorno: PoC o piloto	Tecnologías: sin servidor; lagos de datos; bases de datos; almacenamiento y copia de seguridad
Servicios de AWS: AWS CDK; Amazon DynamoDB; Amazon Kinesis Data Firehose; Amazon Kinesis Data Streams; AWS Lambda; Amazon S3		

Resumen

Este patrón proporciona un código de muestra y una aplicación para entregar registros de Amazon DynamoDB a Amazon Simple Storage Service (Amazon S3) mediante Amazon Kinesis Data Streams y Amazon Data Firehose. El enfoque del patrón emplea constructos L3 de AWS Cloud Development Kit (AWS CDK) e incluye un ejemplo de cómo realizar la transformación de datos con AWS Lambda antes de entregarlos al bucket de S3 de destino en la nube de Amazon Web Services (AWS).

Kinesis Data Streams captura modificaciones a nivel de elemento en cualquier tabla de DynamoDB y las replica en una secuencia de datos de Kinesis. Sus aplicaciones pueden acceder al flujo de datos de Kinesis y ver los cambios a nivel de elemento casi en tiempo real. Kinesis Data Streams también proporciona acceso a otros servicios de Amazon Kinesis, como Firehose y Amazon Managed Service para Apache Flink. Puede crear aplicaciones que proporcionen paneles en tiempo real, generen alertas, apliquen precios y publicidad dinámicos y realicen análisis de datos sofisticados.

Puede usar este patrón para sus casos de uso de integración de datos. Por ejemplo, los vehículos de transporte o equipos industriales pueden enviar grandes volúmenes de datos a una tabla de DynamoDB. Estos datos se pueden transformar y almacenar en un lago de datos alojado en Amazon S3. A continuación, puede consultar y procesar los datos, así como predecir cualquier posible

defecto, mediante servicios sin servidor como Amazon Athena, Amazon Redshift Spectrum, Amazon Rekognition y AWS Glue.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada. Para más información, consulte Introducción a la CLI de AWS en la documentación de CLI de AWS.
- Node.js (18.x+) y npm, instalados y configurados. Para obtener más información, consulte Descargar e instalar Node.js y npm en la documentación de `npm`.
- aws-cdk (2.x+), instalado y configurado. Para más información, consulte Introducción a la CLI de AWS en la documentación de CLI de AWS.
- El repositorio GitHub aws-dynamodb-kinesisfirehose-s3-ingestion, clonado y configurado en su máquina local.
- Datos de ejemplo existentes para la tabla de DynamoDB. Los datos deben utilizar el siguiente formato: `{"SourceDataId": {"S": "123"},"MessageData":{"S": "Hello World"}}`

Arquitectura

El siguiente diagrama muestra un ejemplo de flujo de trabajo para entregar registros de DynamoDB a Amazon S3 mediante Kinesis Data Streams y Firehose.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Los datos se incorporan mediante Amazon API Gateway como proxy de DynamoDB. También puede usar cualquier otro origen para incorporar datos en DynamoDB.
2. Los cambios a nivel de elemento se generan prácticamente en tiempo real en Kinesis Data Streams para su entrega a Amazon S3.
3. Kinesis Data Streams envía los registros a Firehose para su transformación y entrega.
4. Una función de Lambda convierte los registros de un formato de registro de DynamoDB a un formato JSON, que contiene solo los nombres y valores de los atributos de los elementos del registro.

Herramientas

- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura de la nube de AWS en código.
- Kit de herramientas de AWS CDK es un kit de desarrollo en la nube de línea de comandos que ayuda a interactuar con la aplicación AWS Cloud Development Kit (AWS CDK).
- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.
- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.

Código

El código de este patrón está disponible en el repositorio GitHub aws-dynamodb-kinesisfirehose-s3-ingestion.

Epics

Instale y configure el código de muestra

Tarea	Descripción	Habilidades requeridas
Instale las dependencias.	En su máquina local, instale las dependencias de los archivos `package.json` en los directorios `pattern/aws-dynamodb-kinesisstreams-s3` y `sample-application` ejecutando los siguientes comandos: `cd <project_root>/pattern/aws-dynamodb-kinesisstreams-s3`	Desarrollador de aplicaciones, AWS general

Tarea	Descripción	Habilidades requeridas
	`npm install && npm run build` `cd <project_root>/sample-application/` `npm install && npm run build`	
Genere la CloudFormation plantilla de AWS.	1. Ejecute el comando `cd <project_root>/sample-application/` . 2. Ejecute el `cdk synth` comando para generar la CloudFormation plantilla de AWS. 3. Los resultados `AwsDynamodbKinesisfirehoseS3IngestionStack.template.json` quedan almacenados en el directorio `cdk.out`. 4. Utilice AWS CDK o la consola de administración de AWS para procesar la plantilla en AWS CloudFormation.	Desarrollador de aplicaciones, AWS general, AWS DevOps

Implementación de recursos

Tarea	Descripción	Habilidades requeridas
Compruebe e implemente los recursos.	1. Ejecute el comando `cdk diff` para identificar los tipos de recursos que crea el constructo de AWS CDK. 2. Ejecute el `cdk deploy` comando para implementar los recursos.	Desarrollador de aplicaciones, AWS general, AWS DevOps

Incorpore datos a la tabla de DynamoDB para probar la solución

Tarea	Descripción	Habilidades requeridas
Incorpore sus datos de muestra en la tabla de DynamoDB.	1. Envíe una solicitud a la tabla de DynamoDB ejecutando el siguiente comando en la CLI de AWS: `aws dynamodb put-item --table-name <your_table_name> --item '{"<table_partition_key>": {"S": "<partition_key_ID>"},"MessageData":{"S": "<data>"}}'` ejemplo: `aws dynamodb put-item --table-name SourceData_table --item '{"Source`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`DataId": {"S": "123"},"MessageData":{"S": "Hello World"}}'` De forma predeterminada, `put-item` no devuelve ningún valor como resultado si la operación se realiza correctamente. Si la operación falla, devuelve un error. Los datos se almacenan en DynamoDB y, a continuación, se envían a Kinesis Data Streams y Firehose. Nota: Puede adoptar diferentes enfoques para añadir datos a una tabla de DynamoDB. Para obtener más información, consulte la sección Cargar datos en tablas en la documentación de Amazon DynamoDB.	
Verifique que se crea un objeto nuevo en el bucket de S3.	Inicie sesión en la consola de administración de AWS y supervise el bucket de S3 para comprobar que se ha creado un objeto nuevo con los datos enviados. Para obtener más información, consulte `get-object` en la documentación de referencia de la API de Amazon S3.	Desarrollador de aplicaciones, AWS general

Eliminar recursos

Tarea	Descripción	Habilidades requeridas
Limpiar recursos.	Ejecute el comando `cdk destroy` para eliminar todos los recursos usados por este patrón.	Desarrollador de aplicaciones, AWS general

Recursos relacionados

- s3-static-site-stack.ts (repositorio) GitHub
- aws-apigateway-dynamodb módulo (repositorio) GitHub
- módulo aws-kinesisstreams-kinesisfirehose-s3 (repositorio) GitHub
- Captura de datos de cambios para DynamoDB Streams (documentación de Amazon DynamoDB)
- Utilizar Kinesis Data Streams para capturar cambios en DynamoDB (documentación de Amazon DynamoDB)

Integre Amazon API Gateway con Amazon SQS para gestionar las API REST asíncronas

Creado por Natalia Colantonio Favero (AWS) y Gustavo Martim (AWS)

Entorno: PoC o piloto	Tecnologías: sin servidor; mensajería y comunicaciones	Servicios de AWS: Amazon API Gateway; Amazon SQS

Resumen

Al implementar las API de REST, a veces es necesario exponer una cola de mensajes que las aplicaciones cliente puedan publicar. Por ejemplo, es posible que tenga problemas con la latencia de las API de terceros y que se produzcan retrasos en las respuestas, o puede que desee evitar el tiempo de respuesta de las consultas a la base de datos o escalar el servidor cuando hay un gran número de API simultáneas. En estos escenarios, las aplicaciones cliente que publican en la cola solo necesitan saber que la API ha recibido los datos, no lo que ocurre después de recibirlos.

Este patrón crea un punto final de la API REST mediante Amazon API Gateway para enviar un mensaje a Amazon Simple Queue Service (Amazon SQS). Crea una easy-to-implement integración entre los dos servicios que evita el acceso directo a la cola de SQS.

Requisitos previos y limitaciones

- Una cuenta activa AWS

Arquitectura

El diagrama ilustra estos pasos:

1. Solicita un punto final de la API REST POST mediante una herramienta como Postman, otra API u otras tecnologías.
2. API Gateway publica un mensaje, que se recibe en el cuerpo de la solicitud, en la cola.
3. Amazon SQS recibe el mensaje y envía una respuesta a API Gateway con un código de éxito o error.

Herramientas

- Amazon API Gateway le ayuda a crear, publicar, mantener, supervisar y proteger REST, HTTP y WebSocket API a cualquier escala.
- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- Amazon Simple Queue Service (Amazon SQS) ofrece una cola alojada segura, duradera y disponible que le permite integrar y desacoplar sistemas y componentes de software distribuidos.

Epics

Cree una cola de SQS

Tarea	Descripción	Habilidades requeridas
Creación de una cola.	Para crear una cola de SQS que reciba los mensajes de la API REST: 1. Inicie sesión en su Cuenta de AWS. 2. Abra la consola de Amazon SQS en https://console.aws.amazon.com/sqs/. 3. Elija Crear cola. 4. En la página Crear cola, elija la correcta en la lista Región de AWS desplegable de regiones. 5. En Tipo, mantenga la configuración predeterminada (Estándar). 6. Escriba un Nombre para la cola.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	7. Mantenga los valores predeterminados para todos los demás ajustes. 8. Elija Crear cola.	

Proporcione acceso a Amazon SQS

Tarea	Descripción	Habilidades requeridas
Crear un rol de IAM.	Esta función de IAM proporciona a los recursos de API Gateway acceso total a Amazon SQS. 1. Abra la consola de IAM en https://console.aws.amazon.com/iam/. 2. En el panel de navegación, seleccione Roles, Crear rol. 3. En Tipo de entidad de confianza, elija Servicio de AWS. 4. En Caso de uso, elija API Gateway en la lista desplegable y, a continuación, elija Siguiente, Siguiente. 5. En Nombre del rol, introduzca una descripción opcional AWSGatewayRoleForSQSy, a continuación, elija Crear rol.	Desarrollador de aplicaciones, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	6. En el panel Funciones AWSGatewayRoleForSQS, busque y active su casilla de verificación. 7. En la sección Políticas de permisos, elija Agregar permisos, Adjuntar políticas . 8. Busque AmazonSQS FullAccess y selecciónelo. 9. Elija Añadir permisos. 10. En la sección Resumen de AWSGatewayRoleForSQS, copie el número de recurso de Amazon (ARN). Utilizará este ID en un paso posterior.	

Crear una API de REST

Tarea	Descripción	Habilidades requeridas
Cree una API REST.	Esta es la API REST a la que se envían las solicitudes HTTP. 1. Abra la consola de API Gateway en https://console.aws.amazon.com/apigateway/. 2. En la sección API REST, selecciona Construir.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	3. En el nombre de la API, introduce un nombre y una descripción opcional para la API, conserva todas las demás configuraciones predeterminadas y, a continuación, selecciona Crear API.	

Tarea	Descripción	Habilidades requeridas
Conecte API Gateway a Amazon SQS.	Este paso permite que el mensaje fluya desde el interior del cuerpo de la solicitud HTTP hasta Amazon SQS. 1. En la consola de API Gateway, elige la API que has creado. 2. En la página Recursos, en la sección Métodos, selecciona Crear método. 3. En Tipo de método, elija POST. 4. En Tipo de integración, elija Servicio de AWS. 5. Para Región de AWS, elija la región en la que creó la cola de SQS. 6. Para Servicio de AWS, elija Simple Queue Service (SQS). 7. Para el método HTTP, elija POST. 8. En Tipo de acción, selecciona Usar anulación de ruta. 9. <name of SQS queue>Para Anulación de ruta, escriba/<AWS account ID>. 10. En Función de ejecución, pegue el ARN de la función que creó anteriormente.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	11 Elija Crear método.	

Pruebe la API REST

Tarea	Descripción	Habilidades requeridas
Pruebe la API REST.	Ejecute una prueba para comprobar si falta alguna configuración: 1. En la consola de API Gateway, elige la API REST que creaste. 2. En el panel Recursos, elige el método POST. 3. Elija la pestaña Prueba. (Usa la flecha derecha si no se muestra la pestaña). 4. En el cuerpo de la solicitud , pega el siguiente código JSON: `{ "message": "lorem ipsum" }` 5. Seleccione Probar. Recibirás un error similar al siguiente: `<UnknownOperationException/>`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Cambie la integración de la API para reenviar la solicitud correctamente a Amazon SQS.	Complete la configuración para corregir el error de integración: 1. En la consola de API Gateway, elija la API que creó y, a continuación, elija POST. 2. La sección Ejecución de métodos muestra el mapeo visual entre API Gateway y Amazon SQS. En esta sección, seleccion a Solicitud de integración y, a continuación, selecciona Editar. 3. Expanda la sección de encabezados HTTP y, a continuación, elija el parámetro Agregar encabezado de solicitud. • En Nombre, especifique el tipo de contenido. • En Mapeado desde, introduzca «application/». x-www-form-urlencoded Asegúrese de incluir las comillas simples. • Seleccione la casilla de verificación Almacenam iento en caché. 4. Amplíe la sección Plantillas de mapeo.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	• Elija Add mapping template (Añadir plantilla de asignación). • En Tipo de contenido, ingresa application/json. • En el cuerpo de la plantilla, pega este código: `Action=SendMessage&MessageBody=$input.body` • Seleccione Guardar.	

Tarea	Descripción	Habilidades requeridas
Pruebe y valide el mensaje en Amazon SQS.	Realice una prueba para confirmar que la prueba se completó correctamente: 1. En la consola de API Gateway, elige la API REST que creaste. 2. En el panel Recursos, elige el método POST. 3. Elija la pestaña Prueba. (Usa la flecha derecha si no se muestra la pestaña). 4. En el cuerpo de la solicitud , pega el siguiente código JSON: `{ "message": "lorem ipsum" }` 5. Seleccione Probar. 6. Abra la consola de Amazon SQS. 7. En el panel de navegació n, selecciona Colas y, a continuación, elige tu cola. 8. Seleccione Enviar y recibir mensajes. 9. Seleccione Sondeo de mensajes. 10. Elija Mensaje. Debería mostrar lo siguiente:	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`Body { "message": "lorem ipsum" }`	

Tarea	Descripción	Habilidades requeridas
Pruebe API Gateway con un carácter especial.	Realiza una prueba que incluya caracteres especiales (como &) que no sean aceptables en un mensaje: 1. En la consola de API Gateway, elige tu API. 2. Repite la prueba del paso anterior con el siguiente código JSON: `{ "message": "lorem ipsum &" }` 3. Seleccione Probar. Recibirá un error como el siguiente: `{ "Error": { "Code": "AccessDenied", "Message": "Access to the resource https://sqs.us-east-2.amazonaws.com/976166761794/Apg2 is denied.", "Type": "Sender" }, "RequestId": "e83c9c67-bcf6-5e9a-91e9-c737094b17ab"`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	<pre>}</pre> Esto se debe a que los caracteres especiales no se admiten de forma predeterminada en el cuerpo del mensaje. En el siguiente paso, configurará API Gateway para que admita caracteres especiales. Para obtener más información sobre las conversiones de tipos de contenido, consulta la documentación de API Gateway.	

Tarea	Descripción	Habilidades requeridas
Cambie la configuración de la API para que admita caracteres especiales.	Ajuste la configuración para que acepte caracteres especiales en el mensaje: 1. En la consola de API Gateway, elija la API que creó y, a continuación, elija POST. 2. Elija Solicitud de integración y, a continuación, Editar. 3. Cambia la gestión del contenido para convertirla en texto. 4. En la sección de plantillas de mapeo: • En Tipo de contenido, introduzca application/json. • En Cuerpo de la plantilla, especifique: `Action=SendMessage&MessageBody=$util.urlEncode($input.body)` • Seleccione Guardar. 5. Elija la pestaña Prueba. 6. En el cuerpo de la solicitud, introduce el código JSON anterior: `{`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	<pre>" message": "lorem ipsum &" }</pre> 7. Seleccione Probar. 8. Abra la consola de Amazon SQS. 9. Selecciona tu cola y, a continuación, selecciona Enviar y recibir mensajes, Sondear si hay mensajes y Enviar mensaje como antes. El nuevo mensaje debe incluir el carácter especial.	

Implemente la API REST

Tarea	Descripción	Habilidades requeridas
Implementar la API.	Para implementar la API REST: 1. Abra la consola de API Gateway. 2. Elija la API. 3. Elija Deploy API (Implementar API). Para obtener más información sobre este paso, consulta la documentación de API Gateway.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Realice la prueba con una herramienta externa.	Realice una prueba con una herramienta externa para confirmar que el mensaje se ha recibido correctamente: 1. Abre una herramienta como Postman, Insomnia o cURL. 2. Ejecuta tu API. 3. Abra la consola de Amazon SQS. 4. Selecciona tu cola. 5. Carga los mensajes para ver el mensaje nuevo.	Desarrollador de aplicaciones

Eliminación

Tarea	Descripción	Habilidades requeridas
Elimine la API.	En la consola de API Gateway, elija la API que creó y, a continuación, elija Eliminar.	Desarrollador de aplicaciones
Elimine el rol de IAM.	En la consola de IAM, en el panel Funciones, seleccione y, a continuación AWSGatewayRoleForSQS, elija Eliminar.	Desarrollador de aplicaciones
Elimine la cola de SQS.	En la consola Amazon SQS, en el panel Colas, elija la cola SQS que ha creado y, a continuación, elija Eliminar.	Desarrollador de aplicaciones

Recursos relacionados

- SQS- SendMessage (documentación de API Gateway)
- Conversiones de tipos de contenido en API Gateway (documentación de API Gateway)
- variables $util (documentación de API Gateway)
- ¿Cómo puedo integrar una API REST de API Gateway con Amazon SQS y resolver los errores más comunes? (Artículo de AWS Re:POST)

Procese eventos de forma asíncrona con Amazon API Gateway y AWS Lambda

Creado por Andrea Meroni (AWS), Nadim Majed (AWS), Mariem Kthiri (AWS) y Michael Wallner (AWS)

Repositorio de código: procesamiento de eventos asíncrono con API Gateway y Lambda	Entorno: PoC o piloto	Tecnologías: sin servidor
Servicios de AWS: Amazon API Gateway; Amazon DynamoDB; AWS Lambda		

Resumen

Amazon API Gateway es un servicio completamente administrado que los desarrolladores pueden utilizar para la creación, la publicación, el mantenimiento, la supervisión y la protección de las API a cualquier escala. Se encarga de las tareas que implica la aceptación y el procesamiento de hasta cientos de miles de llamadas simultáneas a la API, incluidas las siguientes:

- Gestión del tráfico
- Soporte para el intercambio de recursos entre orígenes (CORS)
- Autorización y control de acceso
- Limitación
- Supervisión
- Gestión de versiones de API

Una cuota de servicio importante de API Gateway es el tiempo de espera de la integración. El tiempo de espera es el tiempo máximo durante el que un servicio de backend debe devolver una respuesta antes de que la API REST devuelva un error. El límite estricto de 29 segundos suele ser aceptable para las cargas de trabajo sincrónicas. Sin embargo, ese límite representa un desafío para los desarrolladores que desean usar API Gateway con cargas de trabajo asíncronas.

Este patrón muestra un ejemplo de arquitectura para procesar eventos de forma asíncrona mediante API Gateway y. AWS Lambda La arquitectura admite la ejecución de trabajos de procesamiento de hasta 15 minutos de duración y utiliza una API REST básica como interfaz.

Projen se utiliza para configurar el entorno de desarrollo local y para implementar la arquitectura de ejemplo en un objetivo Cuenta de AWS, en combinación con el AWS Cloud Development Kit (AWS CDK) kit de herramientas, Docker y Node.js. Projen configura automáticamente un entorno virtual de Python con la confirmación previa y las herramientas que se utilizan para garantizar la calidad del código, escanear la seguridad y realizar pruebas unitarias. Para obtener más información, consulte la sección Herramientas.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Las siguientes herramientas están instaladas en su estación de trabajo:
  - AWS Cloud Development Kit (AWS CDK) Kit de herramientas, versión 2.85.0
  - Docker versión 20.10.21
  - Node.js versión 18.13.0
  - Projen versión 0.71.111
  - Python versión 3.9.16

Limitaciones

- El tiempo de ejecución máximo de un trabajo está limitado por el tiempo de ejecución máximo de las funciones Lambda (15 minutos).
- El número máximo de solicitudes de trabajo simultáneas está limitado por la simultaneidad reservada de la función Lambda.

Arquitectura

El siguiente diagrama muestra la interacción de la API de trabajos con las funciones Lambda de procesamiento de eventos y gestión de errores, con los eventos almacenados en un archivo de eventos de Amazon. EventBridge

Un flujo de trabajo típico incluye los siguientes pasos:

1. Se autentica con AWS Identity and Access Management (IAM) y se obtienen las credenciales de seguridad.
2. Se envía una `POST` solicitud HTTP al punto final de la API de `/jobs` trabajos y se especifican los parámetros del trabajo en el cuerpo de la solicitud.
3. La API de trabajos, que es una API REST de API Gateway, le devuelve una respuesta HTTP que contiene el identificador del trabajo.
4. La API jobs invoca de forma asíncrona la función Lambda de procesamiento de eventos.
5. La función de procesamiento de eventos procesa el evento y, a continuación, coloca los resultados del trabajo en la tabla Amazon DynamoDB de trabajos.
6. Debe enviar una `GET` solicitud HTTP al punto final de la API de `/jobs/{jobId}` trabajos, con el identificador del trabajo del paso 3 como tal. `{jobId}`
7. La API de trabajos consulta la tabla de `jobs` DynamoDB para recuperar los resultados del trabajo.
8. La API de trabajos devuelve una respuesta HTTP que contiene los resultados del trabajo.
9. Si se produce un error en el procesamiento del evento, la función de procesamiento de eventos envía el evento a la función de gestión de errores.
10. La función de gestión de errores coloca los parámetros del trabajo en la tabla de DynamoDB`jobs`.
11. Puede recuperar los parámetros del trabajo enviando una `GET` solicitud HTTP al punto final de la `/jobs/{jobId}` API de trabajos.
12. Si se produce un error en la gestión de errores, la función de gestión de errores envía el evento a un archivo de EventBridge eventos.

    Puede reproducir los eventos archivados utilizando. EventBridge

Herramientas

Servicios de AWS

- AWS Cloud Development Kit (AWS CDK)es un marco de desarrollo de software que le ayuda a definir y aprovisionar la Nube de AWS infraestructura en código.
- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que le ayuda a interactuar con los servicios de AWS mediante comandos en su shell de línea de comandos.
- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.

- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, funciones Lambda, puntos finales de invocación HTTP que utilizan destinos de API o buses de eventos en otros. Cuentas de AWS
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.

Otras herramientas

- autopep8 formatea automáticamente el código Python según la guía de estilo de la Propuesta de mejora de Python (PEP) 8.
- Bandit escanea el código Python para encontrar problemas de seguridad comunes.
- Commitizen es un verificador y generador de confirmaciones de Git. `CHANGELOG`
- cfn-lint es un linter AWS CloudFormation
- Checkov es una herramienta de análisis de código estático que comprueba la infraestructura como código (IaC) para detectar errores de configuración en materia de seguridad y conformidad.
- jq es una herramienta de línea de comandos para analizar JSON.
- Postman es una plataforma de API.
- pre-commit es un administrador de ganchos de Git.
- Projen es un generador de proyectos.
- pytest es un marco de Python para escribir pruebas pequeñas y legibles.

Repositorio de código

Este ejemplo de código de arquitectura se encuentra en el repositorio Lambda y GitHub Asynchronous Event Processing with API Gateway.

Prácticas recomendadas

- Esta arquitectura de ejemplo no incluye la supervisión de la infraestructura implementada. Si su caso de uso requiere supervisión, evalúe la posibilidad de añadir CDK Monitoring Constructs u otra solución de supervisión.

- Esta arquitectura de ejemplo usa permisos de IAM para controlar el acceso a la API de trabajos. Cualquier persona autorizada a asumir que `JobsAPIInvokeRole` podrá invocar la API de trabajos. Como tal, el mecanismo de control de acceso es binario. Si su caso de uso requiere un modelo de autorización más complejo, evalúe el uso de un mecanismo de control de acceso diferente.
- Cuando un usuario envía una `POST` solicitud HTTP al punto final de la API de `/jobs` trabajos, los datos de entrada se validan en dos niveles diferentes:
  - Amazon API Gateway se encarga de la validación de la primera solicitud.
  - La función de procesamiento de eventos realiza la segunda solicitud.

    No se realiza ninguna validación cuando el usuario realiza una `GET` solicitud HTTP al punto final de la API de `/jobs/{jobId}` trabajos. Si su caso de uso requiere una validación de entrada adicional y un mayor nivel de seguridad, evalúe el uso de AWS WAF para proteger su API.

Epics

Configuración del entorno

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Para clonar el repositor io localmente, ejecute el siguiente comando: `git clone https://github.com/aws-samples/asynchronous-event-processing-api-gateway-lambda-cdk.git`	DevOps ingeniero
Configure el proyecto.	Cambie el directorio a la raíz del repositorio y configure el entorno virtual Python y todas las herramientas mediante Projen:	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	`cd asynchronous-event-processing-api-gateway-api-gateway-lambda-cdk` `npx projen`	
Instala enlaces previos a la confirmación.	Para instalar los ganchos de preconfirmación, haz lo siguiente: 1. Active el entorno virtual de Python: `source .env/bin/activate` 2. Instale los ganchos previos a la confirmación: `pre-commit install` `pre-commit install --hook-type commit-msg`	DevOps ingeniero

Implemente la arquitectura de ejemplo

Tarea	Descripción	Habilidades requeridas
Bootstrap. AWS CDK	Para arrancar AWS CDK Cuenta de AWS, ejecuta el siguiente comando: `AWS_PROFILE=$YOUR_AWS_PROFILE npx projen bootstrap`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Implemente la arquitectura de ejemplo.	Para implementar la arquitect ura de ejemplo en su Cuenta de AWS dispositivo, ejecute el siguiente comando: `AWS_PROFILE=$YOUR_ AWS_PROFILE npx projen deploy`	AWS DevOps

Pruebe la arquitectura

Tarea	Descripción	Habilidades requeridas
Instale los requisitos previos de prueba.	Instale en su estación de trabajo the AWS Command Line Interface (AWS CLI), Postman y jq. Se sugiere usar Postman para probar esta arquitect ura de ejemplo, pero no es obligatorio. Si eliges una herramienta de prueba de API alternativa, asegúrate de que sea compatible con la autenticación AWS Signature versión 4 y consulta los puntos finales de la API expuestos, que se pueden inspeccionar exportando la API REST.	DevOps ingeniero
Suponga que`JobsAPIIn vokeRole` .	Suponga `JobsAPIIn vokeRole` que se imprimió como resultado del comando deploy:	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`CREDENTIALS=$(AWS_ PROFILE=$<YOUR_AWS _PROFILE> aws sts assume-role \ --no-cli-pager \ --role-arn $<JOBS_AP I_INVOKE_ROLE_ARN> \ --role-session-name JobsAPIInvoke) export AWS_ACCES S_KEY_ID=$(cat $CREDENTIALS \| jq '.Credentials''.Ac cessKeyId') export AWS_SECRE T_ACCESS_KEY=$(cat $CREDENTIALS \| jq '.Credentials''.Se cretAccessKey') export AWS_SESSI ON_TOKEN==$(cat $CREDENTIALS | jq '.Credentials''.Se ssionToken')`	

Tarea	Descripción	Habilidades requeridas
Configura Postman.	1. Para importar la colección de Postman que se incluye en el repositorio, sigue las instrucciones de la documentación de Postman. 2. Defina las `JobsAPI` variables con los siguientes valores: • `accessKey` – El valor del `Credentials.AccessKeyId` atributo del `assume-role` comando • `baseUrl`– El valor del `JobsApiJobsAPIEndpoint` resultado del comando deploy, sin la barra inclinada final • `region`– El valor del lugar en el que Región de AWS se implementó la arquitectura del ejemplo • `seconds`– El valor del parámetro de entrada para el trabajo de ejemplo. Debe ser un número entero positivo • `secretKey` – El valor del `Credentials.SecretAccessKey` atributo	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	del `assume-role` comando • `sessionToken` – El valor del `Credentials.SessionToken` atributo del `assume-role` comando	
Pruebe la arquitectura de ejemplo.	Para probar la arquitectura de ejemplo, envía las solicitudes a la API de trabajos. Para obtener más información, consulta la documentación de Postman.	DevOps ingeniero

Resolución de problemas

Problema	Solución
La destrucción y posterior redespliegue de la arquitectura de ejemplo fallan porque el grupo de CloudWatch registros de Amazon Logs `/aws/apigateway/JobsAPIAccessLogs` ya existe.	1. Si es necesario, exporte los datos de registro a Amazon S3. 2. Elimine el grupo de CloudWatch registros `/aws/apigateway/JobsAPIAccessLogs` . 3. Vuelva a implementar la arquitectura de ejemplo.

Recursos relacionados

- Plantilla de mapeo de API Gateway y referencia de variables de registro de acceso
- Configurar la invocación asíncrona de la función Lambda de backend

Procese eventos de forma asíncrona con Amazon API Gateway y Amazon DynamoDB Streams

Creado por Andrea Meroni (AWS), Alessandro Trisolini (AWS), Nadim Majed (AWS), Mariem Kthiri (AWS) y Michael Wallner (AWS)

Repositorio de código: procesamiento asíncrono con API Gateway y DynamoDB Streams	Entorno: PoC o piloto	Tecnologías: sin servidor
Servicios de AWS: Amazon API Gateway; Amazon DynamoDB; Amazon DynamoDB Streams; AWS Lambda; Amazon SNS		

Resumen

Amazon API Gateway es un servicio completamente administrado que los desarrolladores pueden utilizar para la creación, la publicación, el mantenimiento, la supervisión y la protección de las API a cualquier escala. Se encarga de las tareas que implica la aceptación y el procesamiento de hasta cientos de miles de llamadas simultáneas a la API, incluidas las siguientes:

- Gestión del tráfico
- Soporte para el intercambio de recursos entre orígenes (CORS)
- Autorización y control de acceso
- Limitación
- Supervisión
- Gestión de versiones de API

Una cuota de servicio importante de API Gateway es el tiempo de espera de la integración. El tiempo de espera es el tiempo máximo durante el que un servicio de backend debe devolver una respuesta antes de que la API REST devuelva un error. El límite estricto de 29 segundos suele ser aceptable

para las cargas de trabajo sincrónicas. Sin embargo, ese límite representa un desafío para los desarrolladores que desean usar API Gateway con cargas de trabajo asíncronas.

Este patrón muestra un ejemplo de arquitectura para procesar eventos de forma asíncrona mediante API Gateway, Amazon DynamoDB Streams y. AWS Lambda La arquitectura admite la ejecución de trabajos de procesamiento en paralelo con los mismos parámetros de entrada y utiliza una API REST básica como interfaz. En este ejemplo, el uso de Lambda como backend limita la duración de los trabajos a 15 minutos. Puede evitar este límite utilizando un servicio alternativo para procesar los eventos entrantes (por ejemplo, AWS Fargate).

Projen se utiliza para configurar el entorno de desarrollo local y para implementar la arquitectura de ejemplo en un objetivo Cuenta de AWS, en combinación con el AWS Cloud Development Kit (AWS CDK) kit de herramientas, Docker y Node.js. Projen configura automáticamente un entorno virtual de Python con la confirmación previa y las herramientas que se utilizan para garantizar la calidad del código, escanear la seguridad y realizar pruebas unitarias. Para obtener más información, consulte la sección Herramientas.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Las siguientes herramientas están instaladas en su estación de trabajo:
  - AWS Cloud Development Kit (AWS CDK) Kit de herramientas, versión 2.85.0 o posterior
  - Docker versión 20.10.21 o posterior
  - Node.js versión 18 o posterior
  - Projen versión 0.71.111 o posterior
  - Python versión 3.9.16 o posterior

Limitaciones

- El número máximo recomendado de lectores para DynamoDB Streams es de dos para evitar la limitación.
- El tiempo de ejecución máximo de un trabajo está limitado por el tiempo de ejecución máximo de las funciones Lambda (15 minutos).
- El número máximo de solicitudes de trabajo simultáneas está limitado por la simultaneidad reservada de las funciones de Lambda.

Arquitectura

Arquitectura

El siguiente diagrama muestra la interacción de la API de trabajos con DynamoDB Streams y las funciones Lambda de procesamiento y gestión de errores de eventos, con los eventos almacenados en un archivo de eventos de Amazon. EventBridge

Un flujo de trabajo típico incluye los siguientes pasos:

1. Se autentica con AWS Identity and Access Management (IAM) y se obtienen las credenciales de seguridad.
2. Se envía una `POST` solicitud HTTP al punto final de la API de `/jobs` trabajos y se especifican los parámetros del trabajo en el cuerpo de la solicitud.
3. La API de trabajos te devuelve una respuesta HTTP que contiene el identificador del trabajo.
4. La API de trabajos coloca los parámetros del trabajo en la tabla de `jobs_table` Amazon DynamoDB.
5. La secuencia `jobs_table` DynamoDB de la tabla DynamoDB invoca las funciones Lambda de procesamiento de eventos.
6. Las funciones Lambda de procesamiento de eventos procesan el evento y, a continuación, colocan los resultados del trabajo en la tabla de DynamoDB. `jobs_table` Para garantizar la coherencia de los resultados, las funciones de procesamiento de eventos implementan un mecanismo de bloqueo optimista.
7. Se envía una `GET` solicitud HTTP al punto final de la API de `/jobs/{jobId}` trabajos, con el identificador de trabajo del paso 3 como tal. `{jobId}`
8. La API de trabajos consulta la tabla de `jobs_table` DynamoDB para recuperar los resultados del trabajo.
9. La API de trabajos devuelve una respuesta HTTP que contiene los resultados del trabajo.
10. Si se produce un error en el procesamiento del evento, el mapeo de origen de la función de procesamiento de eventos envía el evento al tema Amazon Simple Notification Service (Amazon SNS), que trata los errores.
11. El tema de gestión de errores de SNS envía el evento de forma asíncrona a la función de gestión de errores.

12. La función de gestión de errores coloca los parámetros del trabajo en la tabla de DynamoDB`jobs_table`.

    Puede recuperar los parámetros del trabajo enviando una `GET` solicitud HTTP al punto final de la `/jobs/{jobId}` API de trabajos.

13. Si la gestión de errores falla, la función de gestión de errores envía el evento a un archivo de Amazon EventBridge .

    Puede reproducir los eventos archivados utilizando. EventBridge

Herramientas

Servicios de AWS

- AWS Cloud Development Kit (AWS CDK)es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura de la nube de AWS en código.
- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, las funciones de Lambda de AWS, los puntos de conexión de invocación HTTP que utilizan destinos de API o los buses de eventos de otras cuentas de AWS.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.

Otras herramientas

- autopep8 formatea automáticamente el código Python según la guía de estilo de la Propuesta de mejora de Python (PEP) 8.
- Bandit escanea el código Python para encontrar problemas de seguridad comunes.
- Commitizen es un verificador y generador de confirmaciones de Git. `CHANGELOG`

- cfn-lint es un linter AWS CloudFormation
- Checkov es una herramienta de análisis de código estático que comprueba la infraestructura como código (IaC) para detectar errores de configuración en materia de seguridad y conformidad.
- jq es una herramienta de línea de comandos para analizar JSON.
- Postman es una plataforma de API.
- pre-commit es un administrador de ganchos de Git.
- Projen es un generador de proyectos.
- pytest es un marco de Python para escribir pruebas pequeñas y legibles.

Repositorio de código

Este ejemplo de código de arquitectura se encuentra en el repositorio GitHub Asynchronous Processing with API Gateway y DynamoDB Streams.

Prácticas recomendadas

- Esta arquitectura de ejemplo no incluye la supervisión de la infraestructura implementada. Si su caso de uso requiere supervisión, evalúe la posibilidad de añadir CDK Monitoring Constructs u otra solución de supervisión.
- Esta arquitectura de ejemplo usa permisos de IAM para controlar el acceso a la API de trabajos. Cualquier persona autorizada a asumir que `JobsAPIInvokeRole` podrá invocar la API de trabajos. Como tal, el mecanismo de control de acceso es binario. Si su caso de uso requiere un modelo de autorización más complejo, evalúe el uso de un mecanismo de control de acceso diferente.
- Cuando un usuario envía una `POST` solicitud HTTP al punto final de la API de `/jobs` trabajos, los datos de entrada se validan en dos niveles diferentes:
  - API Gateway se encarga de la validación de la primera solicitud.
  - La función de procesamiento de eventos realiza la segunda solicitud.

    No se realiza ninguna validación cuando el usuario realiza una `GET` solicitud HTTP al punto final de la API de `/jobs/{jobId}` trabajos. Si su caso de uso requiere una validación de entrada adicional y un mayor nivel de seguridad, evalúe su uso AWS WAF para proteger su API.

- Para evitar limitaciones, la documentación de DynamoDB Streams desaconseja a los usuarios leer con más de dos consumidores del mismo fragmento de la transmisión. Para aumentar el número de consumidores, le recomendamos que utilice Amazon Kinesis Data Streams.
- En este ejemplo, se ha utilizado el bloqueo optimista para garantizar actualizaciones coherentes de los elementos de la tabla de `jobs_table` DynamoDB. Según los requisitos del caso de uso, es posible que necesite implementar mecanismos de bloqueo más fiables, como el bloqueo pesimista.

Epics

Configuración del entorno

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Para clonar el repositorio localmente, ejecute el siguiente comando: `git clone https://github.com/aws-samples/asynchronous-event-processing-api-gateway-dynamodb-streams-cdk.git`	DevOps ingeniero
Configure el proyecto.	Cambie el directorio a la raíz del repositorio y configure el entorno virtual de Python y todas las herramientas mediante Projen: `cd asynchronous-event-processing-api-gateway-api-gateway-dynamodb-streams-cdk` `npx projen`	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Instala enlaces previos a la confirmación.	Para instalar los ganchos de preconfirmación, haz lo siguiente: 1. Active el entorno virtual de Python: `source .env/bin/activate` 2. Instale los ganchos previos a la confirmación: `pre-commit install` `pre-commit install --hook-type commit-msg`	DevOps ingeniero

Implemente la arquitectura de ejemplo

Tarea	Descripción	Habilidades requeridas
Bootstrap. AWS CDK	Para arrancar AWS CDK Cuenta de AWS, ejecuta el siguiente comando: `AWS_PROFILE=$YOUR_AWS_PROFILE npx projen bootstrap`	AWS DevOps
Implemente la arquitectura de ejemplo.	Para implementar la arquitectura de ejemplo en su Cuenta de AWS dispositivo, ejecute el siguiente comando:	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`AWS_PROFILE=$YOUR_ AWS_PROFILE npx projen deploy`	

Pruebe la arquitectura

Tarea	Descripción	Habilidades requeridas
Instale los requisitos previos de prueba.	Instale en su estación de trabajo the AWS Command Line Interface (AWS CLI), Postman y jq. Se sugiere usar Postman para probar esta arquitectura de ejemplo, pero no es obligator io. Si elige una herramienta de prueba de API alternati va, asegúrese de que sea compatible con la autentica ción de la versión 4 de AWS Signature y consulte los puntos de enlace de la API expuestos que se pueden inspeccionar mediante la exportación de la API REST.	DevOps ingeniero
Suponga que `JobsAPIIn vokeRole` .	Suponga `JobsAPIIn vokeRole` que se imprimió como resultado del `deploy` comando: `CREDENTIALS=$(AWS_ PROFILE=$<YOUR_AWS`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	_PROFILE> aws sts assume-role \ --no-cli-pager \ --role-arn $<JOBS_API_INVOKE_ROLE_ARN> \ --role-session-name JobsAPIInvoke) export AWS_ACCESS_KEY_ID=$(cat $CREDENTIALS \| jq '.Credentials''.AccessKeyId') export AWS_SECRET_ACCESS_KEY=$(cat $CREDENTIALS \| jq '.Credentials''.SecretAccessKey') export AWS_SESSION_TOKEN==$(cat $CREDENTIALS | jq '.Credentials''.SessionToken')	

Tarea	Descripción	Habilidades requeridas
Configura Postman.	• Para importar la colección de Postman que se incluye en el repositorio, sigue las instrucciones de la documentación de Postman. • Defina las `JobsAPI` variables con los siguientes valores: • `accessKey` – El valor del `Credentials.AccessKeyId` atributo del `assume-role` comando. • `baseUrl`– El valor de la `JobsApiJobsAPIEndpoint` salida del `deploy` comando, sin la barra diagonal final. • `region`– El valor del lugar en el que Región de AWS se implementó la arquitectura de ejemplo. • `seconds`– El valor del parámetro de entrada para el trabajo de ejemplo. Debe ser un número entero positivo. • `secretKey` – El valor del `Credentials.SecretAccessKey` atributo del `assume-role` comando.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	• `sessionToken` – El valor del `Credentials.SessionToken` atributo del `assume-role` comando.	
Pruebe la arquitectura de ejemplo.	Para probar la arquitectura de ejemplo, envía las solicitudes a la API de trabajos. Para obtener más información, consulta la documentación de Postman.	DevOps ingeniero

Resolución de problemas

Problema	Solución
La destrucción y posterior redespliegue de la arquitectura de ejemplo fallan porque el grupo de CloudWatch registros de Amazon Logs `/aws/apigateway/JobsAPIAccessLogs` ya existe.	1. Si es necesario, exporte los datos de registro a Amazon Simple Storage Service (Amazon S3). 2. Elimine el grupo de CloudWatch registros `/aws/apigateway/JobsAPIAccessLogs` . 3. Vuelva a implementar la arquitectura de ejemplo.

Recursos relacionados

- Plantilla de mapeo de API Gateway y referencia de variables de registro de acceso
- Cambiar la captura de datos para DynamoDB Streams
- Bloqueo optimista con número de versión
- Uso de Kinesis Data Streams para capturar los cambios en DynamoDB

Procese eventos de forma asíncrona con Amazon API Gateway, Amazon SQS y AWS Fargate

Creado por Andrea Meroni (AWS), Alessandro Trisolini (AWS), Nadim Majed (AWS), Mariem Kthiri (AWS) y Michael Wallner (AWS)

Repositorio de código: procesamiento de eventos asíncrono con API Gateway y SQS	Entorno: PoC o piloto	Tecnologías: sin servidor
Servicios de AWS: Amazon API Gateway; Amazon DynamoDB; AWS Fargate; Amazon SQS; AWS Lambda		

Resumen

Amazon API Gateway es un servicio completamente administrado que los desarrolladores pueden utilizar para la creación, la publicación, el mantenimiento, la supervisión y la protección de las API a cualquier escala. Se encarga de las tareas que implica la aceptación y el procesamiento de hasta cientos de miles de llamadas simultáneas a la API, incluidas las siguientes:

- Gestión del tráfico
- Soporte para el intercambio de recursos entre orígenes (CORS)
- Autorización y control de acceso
- Limitación
- Supervisión
- Gestión de versiones de API

Una cuota de servicio importante de API Gateway es el tiempo de espera de la integración. El tiempo de espera es el tiempo máximo durante el que un servicio de backend debe devolver una respuesta antes de que la API REST devuelva un error. El límite estricto de 29 segundos suele ser aceptable

para las cargas de trabajo sincrónicas. Sin embargo, ese límite representa un desafío para los desarrolladores que desean usar API Gateway con cargas de trabajo asíncronas.

Este patrón muestra un ejemplo de arquitectura para procesar eventos de forma asíncrona mediante API Gateway, Amazon Simple Queue Service (Amazon SQS) y. AWS Fargate La arquitectura admite la ejecución de trabajos de procesamiento sin restricciones de duración y utiliza una API REST básica como interfaz.

Projen se utiliza para configurar el entorno de desarrollo local y para implementar la arquitectura de ejemplo en un destino Cuenta de AWS, en combinación con Docker y Node.js. AWS Cloud Development Kit (AWS CDK) Projen configura automáticamente un entorno virtual de Python con la confirmación previa y las herramientas que se utilizan para garantizar la calidad del código, escanear la seguridad y realizar pruebas unitarias. Para obtener más información, consulte la sección Herramientas.

Requisitos previos y limitaciones

Requisitos previos

- Un activo Cuenta de AWS
- Las siguientes herramientas están instaladas en su estación de trabajo:
  - AWS Cloud Development Kit (AWS CDK) Kit de herramientas, versión 2.85.0 o posterior
  - Docker versión 20.10.21 o posterior
  - Node.js versión 18 o posterior
  - Projen versión 0.71.111 o posterior
  - Python versión 3.9.16 o posterior

Limitaciones

- Los trabajos simultáneos están limitados a 500 tareas por minuto, que es el número máximo de tareas que Fargate puede aprovisionar.

Arquitectura

El siguiente diagrama muestra la interacción de la API de trabajos con la tabla `jobs` Amazon DynamoDB, el servicio Fargate de procesamiento de eventos y la función de gestión de errores. AWS Lambda Los eventos se almacenan en un archivo de EventBridge eventos de Amazon.

Un flujo de trabajo típico incluye los siguientes pasos:

1. Se autentica con AWS Identity and Access Management (IAM) y se obtienen las credenciales de seguridad.
2. Envía una `POST` solicitud HTTP al punto final de la API de `/jobs` trabajos y especifica los parámetros del trabajo en el cuerpo de la solicitud.
3. La API de trabajos, que es una API REST de API Gateway, le devuelve una respuesta HTTP que contiene el identificador del trabajo.
4. La API de trabajos envía un mensaje a la cola de SQS.
5. Fargate extrae el mensaje de la cola de SQS, procesa el evento y, a continuación, coloca los resultados del trabajo en la tabla de DynamoDB. `jobs`
6. Se envía una `GET` solicitud HTTP al punto final de la API de `/jobs/{jobId}` trabajos, con el identificador de trabajo del paso 3 como. `{jobId}`
7. La API de trabajos consulta la tabla de `jobs` DynamoDB para recuperar los resultados del trabajo.
8. La API de trabajos devuelve una respuesta HTTP que contiene los resultados del trabajo.
9. Si se produce un error en el procesamiento del evento, la cola de SQS envía el evento a la cola de mensajes sin salida (DLQ).
10. Un EventBridge evento inicia la función de gestión de errores.
11. La función de gestión de errores coloca los parámetros del trabajo en la tabla de DynamoDB`jobs`.
12. Puede recuperar los parámetros del trabajo enviando una `GET` solicitud HTTP al punto final de la `/jobs/{jobId}` API de trabajos.
13. Si se produce un error en la gestión de errores, la función de gestión de errores envía el evento a un EventBridge archivo.

    Puede reproducir los eventos archivados utilizando. EventBridge

Herramientas

Servicios de AWS

- AWS Cloud Development Kit (AWS CDK)es un marco de desarrollo de software que le ayuda a definir y aprovisionar la Nube de AWS infraestructura en código.
- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.

- AWS Fargatele ayuda a ejecutar contenedores sin necesidad de gestionar servidores o instancias de Amazon Elastic Compute Cloud (Amazon EC2). Se utiliza en conjunto con Amazon Elastic Container Service (Amazon ECS).
- Amazon EventBridge es un servicio de bus de eventos sin servidor que le ayuda a conectar sus aplicaciones con datos en tiempo real de diversas fuentes. Por ejemplo, funciones Lambda, puntos finales de invocación HTTP que utilizan destinos de API o buses de eventos en otros. Cuentas de AWS
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Queue Service (Amazon SQS) ofrece una cola alojada segura, duradera y disponible que le permite integrar y desacoplar sistemas y componentes de software distribuidos.

Otras herramientas

- autopep8 formatea automáticamente el código Python según la guía de estilo de la Propuesta de mejora de Python (PEP) 8.
- Bandit escanea el código de Python para encontrar problemas de seguridad comunes.
- Commitizen es un verificador y generador de confirmaciones de Git. `CHANGELOG`
- cfn-lint es un linter AWS CloudFormation
- Checkov es una herramienta de análisis de código estático que comprueba la infraestructura como código (IaC) para detectar errores de configuración de seguridad y cumplimiento.
- jq es una herramienta de línea de comandos para analizar JSON.
- Postman es una plataforma de API.
- pre-commit es un administrador de ganchos de Git.
- Projen es un generador de proyectos.
- pytest es un marco de Python para escribir pruebas pequeñas y legibles.

Repositorio de código

Este ejemplo de código de arquitectura se encuentra en el repositorio de SQS y procesamiento GitHub asíncrono con API Gateway.

Prácticas recomendadas

- Esta arquitectura de ejemplo no incluye la supervisión de la infraestructura implementada. Si su caso de uso requiere supervisión, evalúe la posibilidad de añadir CDK Monitoring Constructs u otra solución de supervisión.
- Esta arquitectura de ejemplo usa permisos de IAM para controlar el acceso a la API de trabajos. Cualquier persona autorizada a asumir que `JobsAPIInvokeRole` podrá invocar la API de trabajos. Como tal, el mecanismo de control de acceso es binario. Si su caso de uso requiere un modelo de autorización más complejo, evalúe el uso de un mecanismo de control de acceso diferente.
- Cuando un usuario envía una `POST` solicitud HTTP al punto final de la API de `/jobs` trabajos, los datos de entrada se validan en dos niveles diferentes:
  - API Gateway se encarga de la validación de la primera solicitud.
  - La función de procesamiento de eventos realiza la segunda solicitud.

    No se realiza ninguna validación cuando el usuario realiza una `GET` solicitud HTTP al punto final de la API de `/jobs/{jobId}` trabajos. Si su caso de uso requiere una validación de entrada adicional y un mayor nivel de seguridad, evalúe su uso AWS WAF para proteger su API.

Epics

Configuración del entorno

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Para clonar el repositor io localmente, ejecuta el siguiente comando: `git clone https://g ithub.com/aws-samp les/asynchronous-e vent-processing-api- gateway-sqs-cdk.git`	DevOps ingeniero
Configure el proyecto.	Cambie el directorio a la raíz del repositorio y configure	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	el entorno virtual de Python y todas las herramientas mediante Projen: `cd asynchronous-event-processing-api-gateway-api-gateway-sqs-cdk` `npx projen`	
Instala enlaces previos a la confirmación.	Para instalar los ganchos de preconfirmación, haz lo siguiente: 1. Active el entorno virtual de Python: `source .env/bin/activate` 2. Instale los ganchos previos a la confirmación: `pre-commit install` `pre-commit install --hook-type commit-msg`	DevOps ingeniero

Implemente la arquitectura de ejemplo

Tarea	Descripción	Habilidades requeridas
Bootstrap. AWS CDK	Para arrancar AWS CDK Cuenta de AWS, ejecuta el siguiente comando:	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`AWS_PROFILE=$YOUR_AWS_PROFILE npx projen bootstrap`	
Implemente la arquitectura de ejemplo.	Para implementar la arquitectura de ejemplo en su Cuenta de AWS dispositivo, ejecute el siguiente comando: `AWS_PROFILE=$YOUR_AWS_PROFILE npx projen deploy`	AWS DevOps

Pruebe la arquitectura

Tarea	Descripción	Habilidades requeridas
Instale los requisitos previos de prueba.	Instale en su estación de trabajo the AWS Command Line Interface (AWS CLI), Postman y jq. Se sugiere usar Postman para probar esta arquitectura de ejemplo, pero no es obligatorio. Si eliges una herramienta de prueba de API alternativa, asegúrate de que sea compatible con la autenticación AWS Signature versión 4 y consulta los puntos finales de la API expuestos, que se pueden inspeccionar exportando la API REST.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Suponga que`JobsAPIInvokeRole` .	Suponga `JobsAPIInvokeRole` que se imprimió como resultado del `deploy` comando: `CREDENTIALS=$(AWS_PROFILE=$<YOUR_AWS_PROFILE> aws sts assume-role \ --no-cli-pager \ --role-arn $<JOBS_API_INVOKE_ROLE_ARN> \ --role-session-name JobsAPIInvoke) export AWS_ACCESS_KEY_ID=$(cat $CREDENTIALS \| jq '.Credentials''.AccessKeyId') export AWS_SECRET_ACCESS_KEY=$(cat $CREDENTIALS \| jq '.Credentials''.SecretAccessKey') export AWS_SESSION_TOKEN==$(cat $CREDENTIALS | jq '.Credentials''.SessionToken')`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Configura Postman.	• Para importar la colección de Postman que se incluye en el repositorio, sigue las instrucciones de la documentación de Postman. • Defina las `JobsAPI` variables con los siguientes valores: • `accessKey` – El valor del `Credentials.AccessKeyId` atributo del `assume-role` comando. • `baseUrl`– El valor de la `JobsApiJobsAPIEndpoint` salida del `deploy` comando, sin la barra diagonal final. • `region`– El valor del lugar en el que Región de AWS se implementó la arquitectura de ejemplo. • `seconds`– El valor del parámetro de entrada para el trabajo de ejemplo. Debe ser un número entero positivo. • `secretKey` – El valor del `Credentials.SecretAccessKey` atributo del `assume-role` comando.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	• `sessionToken` – El valor del `Credentials.SessionToken` atributo del `assume-role` comando.	
Pruebe la arquitectura de ejemplo.	Para probar la arquitectura de ejemplo, envía las solicitudes a la API de trabajos. Para obtener más información, consulta la documentación de Postman.	DevOps ingeniero

Resolución de problemas

Problema	Solución
La destrucción y posterior redespliegue de la arquitectura de ejemplo fallan porque el grupo de CloudWatch registros de Amazon Logs `/aws/apigateway/JobsAPIAccessLogs` ya existe.	1. Si es necesario, exporte los datos de registro a Amazon Simple Storage Service (Amazon S3). 2. Elimine el grupo de CloudWatch registros `/aws/apigateway/JobsAPIAccessLogs` . 3. Vuelva a implementar la arquitectura de ejemplo.
La destrucción y posterior redistribución de la arquitectura del ejemplo fallan porque el grupo de CloudWatch registros ya existe. `/aws/ecs/EventProcessingServiceLogs`	1. Si es necesario, exporte los datos de registro a Amazon S3. 2. Elimine el grupo de CloudWatch registros `/aws/ecs/EventProcessingServiceLogs.` 3. Vuelva a implementar la arquitectura de ejemplo.

Recursos relacionados

- Plantilla de mapeo de API Gateway y referencia de variables de registro de acceso
- ¿Cómo puedo integrar una API REST de API Gateway con Amazon SQS y resolver los errores más comunes?

Ejecute las tareas de AWS Systems Manager Automation de forma sincrónica desde AWS Step Functions

Creado por Elie El khoury (AWS)

Repositorio de código: amazon-stepfunctions-ssm-waitfortasktoken	Entorno: producción	Tecnologías: sin servidor DevOps; informática para el usuario final; operaciones
Servicios de AWS: AWS Step Functions; AWS Systems Manager		

Resumen

Este patrón explica cómo integrarse AWS Step Functions con AWS Systems Manager. Utiliza las integraciones de servicios del AWS SDK para llamar a la startAutomationExecutionAPI de Systems Manager con un token de tarea de un flujo de trabajo de una máquina de estado y se detiene hasta que el token regresa con una llamada correcta o errónea. Para demostrar la integración, este patrón implementa un contenedor de documentos de automatización (runbook) alrededor del documento o y se utiliza `.waitForTaskToken` para llamar a `AWS-RunShellScript` o `AWS-RunPowerShellScript` de forma sincrónica. `AWS-RunShellScript` `AWS-RunPowerShellScript` Para obtener más información sobre las integraciones de servicios del AWS SDK en Step Functions, consulta la Guía para AWS Step Functions desarrolladores.

Step Functions es un servicio de flujo de trabajo visual de bajo código que puede utilizar para crear aplicaciones distribuidas, automatizar los procesos empresariales y de TI y crear canalizaciones de datos y aprendizaje automático mediante AWS el uso de servicios. Los flujos de trabajo gestionan los errores, los reintentos, la paralelización, las integraciones de servicios y la observabilidad para que pueda centrarse en una lógica empresarial de mayor valor.

La automatización, una capacidad de AWS Systems Manager, simplifica las tareas comunes de mantenimiento, implementación y corrección para empresas Servicios de AWS como Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Service (Amazon RDS), Amazon Redshift y Amazon Simple Storage Service (Amazon S3) (Simple Storage Service (Amazon S3). Automation le ofrece un control granular sobre la concurrencia de sus automatizaciones. Por

ejemplo, puede especificar a cuántos recursos desea dirigirse simultáneamente y cuántos errores pueden producirse antes de que se detenga una automatización.

Para obtener detalles sobre la implementación, incluidos los pasos, parámetros y ejemplos del manual de procedimientos, consulte la sección Información adicional.

Requisitos previos y limitaciones

Requisitos previos

- AWS Una cuenta activa
- AWS Identity and Access Management (IAM) para acceder a Step Functions y Systems Manager
- Una instancia EC2 con el agente Systems Manager (SSM Agent) instalado en la instancia
- Un perfil de instancia de IAM para Systems Manager adjunto a la instancia en la que planea ejecutar el manual de procedimientos
- Un rol de Step Functions que tiene los siguientes permisos de IAM (que siguen el principio de privilegios mínimos):

```
{
            "Effect": "Allow",
            "Action": "ssm:StartAutomationExecution",
            "Resource": "*"
 }
```

Versiones de producto

- Versión de esquema de documento de SSM 0.3 o posterior
- SSM Agent versión 2.3.672.0 o posterior

Arquitectura

Pila de tecnología de destino

- AWS Step Functions
- AWS Systems Manager Automation

Arquitectura de destino

Automatizar y escalar

- Este patrón proporciona una AWS CloudFormation plantilla que puede utilizar para implementar los manuales de ejecución en varias instancias. (Consulte el repositorio de implementación de GitHub Step Functions y Systems Manager).

Herramientas

Servicios de AWS

- AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y administrarlos a lo largo de su ciclo de vida en todas Cuentas de AWS las regiones.
- AWS Identity and Access Management (IAM) lo ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- AWS Step Functionses un servicio de organización sin servidor que le ayuda a combinar AWS Lambda funciones y otras Servicios de AWS para crear aplicaciones esenciales para la empresa.
- AWS Systems Manager le ayuda a administrar las aplicaciones y la infraestructura que se ejecutan en la Nube de AWS. Simplifica la administración de aplicaciones y recursos, reduce el tiempo necesario para detectar y resolver problemas operativos y le ayuda a administrar sus recursos de forma segura y a escala. AWS

Código

El código de este patrón está disponible en el repositorio de implementación de GitHub Step Functions y Systems Manager.

Epics

Creación de manuales de procedimientos

Tarea	Descripción	Habilidades requeridas
Descargue la CloudFormation plantilla.	Descarga la `ssm-automation-documents.cfn.json` plantilla de la	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`cloudformation` carpeta del GitHub repositorio.	
Cree manuales de procedimientos.	Inicie sesión en AWS Management Console, abra la AWS CloudFormation consola e implemente la plantilla. Para obtener más información sobre la implementación de CloudFormation plantillas, consulte Crear una pila en la AWS CloudFormation consola en la CloudFormation documentación. La CloudFormation plantilla implementa tres recursos: • `SfnRunCommandByInstanceIds` — Runbook que permite ejecutar `AWS-RunShellScript` o usar identificadores `AWS-RunPowerShellScript` de instancia. • `SfnRunCommandByTargets` — Manual de ejecución que te permite correr `AWS-RunShellScript` o usar `AWS-RunPowerShellScript` objetivos. • `SSMSyncRole` — La función de IAM que asumen los manuales.	AWS DevOps

Crear una máquina de estado de muestra

Tarea	Descripción	Habilidades requeridas
Crear una máquina de estado de prueba.	Siga las instrucciones de la guía para AWS Step Functions desarrolladores para crear y ejecutar una máquina de estados. Para la definición, utilice el siguiente código. Asegúrese de actualizar el valor `InstanceIds` con el ID de una instancia válida habilitada para Systems Manager en su cuenta. `{ "Comment": "A description of my state machine", "StartAt": "StartAutomationWaitForCallBack", "States": { "StartAutomationWaitForCallBack": { "Type": "Task", "Resource": "arn:aws:states:::aws-sdk:ssm:startAutomationExecution.waitForTaskToken", "Parameters": { "DocumentName": "SfnRunCommandByInstanceIds", "Parameters": { "InstanceIds": ["i-1234567890abcdef0"`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	<pre>], "taskToken. $": "States.Array($$.T ask.Token)", "workingD irectory": ["/home/ssm- user/"], "Commands": ["echo \"This is a test running automation waitForTa skToken\" >> automatio n.log", "sleep 100"], "executio nTimeout": ["10800"], "delivery Timeout": ["30"], "shell": ["Shell"] } }, "End": true } } }</pre> Este código llama al manual de procedimientos para ejecutar dos comandos que demuestran la llamada	

Tarea	Descripción	Habilidades requeridas
	`waitForTaskToken` a Systems Manager Automation. El valor del `shell` parámetro (`ShelloPowerShell`) determina si el documento de automatización se ejecuta `AWS-RunShellScript` o`AWS-RunPowerShellScript` . La tarea escribe «Se trata de un waitForTask token de automatización en ejecución de pruebas» en el `/home/ssm-user/automation.log` archivo y, a continuación, permanece en reposo durante 100 segundos antes de responder con el token de la tarea y lanzar la siguiente tarea del flujo de trabajo. Si, en vez de eso, quiere llamar al manual de procedimientos `SfnRunCommandByTargets` , sustituya la sección `Parameters` del código anterior por la siguiente : `"Parameters": { "Targets": [ { "Key": "InstanceIds",`	

Tarea	Descripción	Habilidades requeridas
	<pre>"Values": ["i-02573cafcfEXAMPLE", "i-0471e04240EXAMPLE"] }],</pre>	
Actualice el rol de IAM de la máquina de estado.	El paso anterior crea automáticamente un rol de IAM dedicado para la máquina de estados. Sin embargo, no concede permisos para llamar al manual de procedimientos. Actualice el rol añadiendo los permisos siguientes: <pre>{ "Effect": "Allow", "Action": "ssm:StartAutomationExecution", "Resource": "*" }</pre>	AWS DevOps
Valide las llamadas sincrónicas.	Ejecute la máquina de estados para validar la llamada sincrónica entre Step Functions y Systems Manager Automation. Para ver un ejemplo de salida, consulte la sección Información adicional.	AWS DevOps

Recursos relacionados

- Cómo empezar con AWS Step Functions (Guía para AWS Step Functions desarrolladores)
- Espere a que le devuelvan la llamada con el token de la tarea (guía para AWS Step Functions desarrolladores, patrones de integración de servicios)
- Llamadas a las API send_task_success y send_task_failure (documentación de Boto3)
- AWS Systems Manager Automatización (guía AWS Systems Manager del usuario)

Información adicional

Detalles de la implementación

Este patrón proporciona una CloudFormation plantilla que despliega dos manuales de ejecución de Systems Manager:

- `SfnRunCommandByInstanceId`sejecuta el `AWS-RunPowerShellScript` comando `AWS-RunShellScript` o mediante los identificadores de instancia.
- `SfnRunCommandByTargets`sejecuta el `AWS-RunPowerShellScript` comando `AWS-RunShellScript` o mediante objetivos.

Cada runbook implementa cuatro pasos para lograr una llamada sincrónica cuando se usa la `.waitForTaskToken` opción de Step Functions.

Paso	Action	Descripción
1	`Branch`	Comprueba el valor (`ShelloPowerShell`) del `shell` parámetro para decidir si se va a ejecutar `AWS-RunShellScript` en Linux o `AWS-RunPowerShellScript` en Windows.
2	`RunCommand_Shell` o `RunCommand_PowerShell`	Toma varias entradas y ejecuta el `RunPowerShellScript` comando

		`RunShellScript` o. Para obtener más información, consulte la pestaña Detalles del documento `RunCommand_Shell` o `RunCommand_PowerShell` Automatización en la consola de Systems Manager.
3	`SendTaskFailure`	Se ejecuta cuando se anula o cancela el paso 2. Llama a la API send_task_failure de Step Functions, que acepta tres parámetros como entrada: el token pasado por la máquina de estados, el error de error y una descripción de la causa del error.
4	`SendTaskSuccess`	Se ejecuta cuando el paso 2 se realiza correctamente. Llama a la API send_task_success de Step Functions, que acepta el token pasado por la máquina de estados como entrada.

Parámetros del manual de procedimientos

`SfnRunCommandByInstanceIds`manual de instrucciones:

Nombre del parámetro	Tipo	Opcional u obligatorio	Descripción
`shell`	Cadena	Obligatoria	El shell de instancias para decidir si se va a ejecutar `AWS-RunSh`

			`ellScript` para Linux o `AWS-RunPowerShellScript` para Windows.
`deliveryTimeout`	Entero	Opcional	El tiempo, en segundos, que se tarda en esperar a que se entregue un comando al agente SSM de una instancia. Este parámetro tiene un valor mínimo de 30 (0,5 minutos) y un valor máximo de 2592000 (720 horas).
`executionTimeout`	Cadena	Opcional	El tiempo, en segundos, para que un comando se complete antes de considerar que se ha producido un error. El valor predeterminado es 3600 (1 hora). El valor máximo es 172800 (48 horas).
`workingDirectory`	Cadena	Opcional	La ruta al directorio de trabajo en la instancia.
`Commands`	StringList	Obligatoria	El script o comando del intérprete de comandos que se va a ejecutar.

`InstanceIds`	StringList	Obligatoria	Los ID de las instancias en las que desea ejecutar el comando.
`taskToken`	Cadena	Obligatoria	El token de tarea que se utilizará para las respuesta s de devolución de llamada.

`SfnRunCommandByTargets`manual de ejecución:

Nombre	Tipo	Opcional u obligatorio	Descripción
`shell`	Cadena	Obligatoria	El shell de instancias para decidir si se va a ejecutar `AWS-RunSh ellScript` para Linux o `AWS-RunPo werShellScript` para Windows.
`deliveryTimeout`	Entero	Opcional	El tiempo, en segundos, que se tarda en esperar a que se entregue un comando al agente SSM de una instancia . Este parámetro tiene un valor mínimo de 30 (0,5 minutos) y un valor máximo de 2592000 (720 horas).
`execution Timeout`	Entero	Opcional	El tiempo, en segundos, para

			que un comando se complete antes de considerar que se ha producido un error. El valor predeterminado es 3600 (1 hora). El valor máximo es 172800 (48 horas).
`workingDirectory`	Cadena	Opcional	La ruta al directorio de trabajo en la instancia.
`Commands`	StringList	Obligatoria	El script o comando del intérprete de comandos que se va a ejecutar.
`Targets`	MapList	Obligatoria	Una matriz de criterios de búsqueda que identifica las instancias utilizando los pares clave-valor que usted especifique. Por ejemplo: `[{"Key":"InstanceIds","Values":["i-02573cafcfEXAMPLE","i-0471e04240EXAMPLE"]}]`

`taskToken`	Cadena	Obligatoria	El token de tarea que se utilizará para las respuesta s de devolución de llamada.

Resultados de ejemplo

La siguiente tabla proporciona un ejemplo de salida de la función step. Muestra que el tiempo total de ejecución es superior a 100 segundos entre el paso 5 (`TaskSubmitted`) y el paso 6 (`TaskSucceeded`). Esto demuestra que la función step esperó a que finalizara el `sleep 100` comando antes de pasar a la siguiente tarea del flujo de trabajo.

ID	Tipo	Paso	Resource	Tiempo transcurrido (ms)	Timestamp
1	`Execution Started`		-	0	11 de marzo de 2022 02:50:34.303 p.m.
2	`TaskState Entered`	`StartAuto mationWai tForCallB ack`	-	40	11 de marzo de 2022 02:50:34.343 p.m.
3	`TaskSched uled`	`StartAuto mationWai tForCallB ack`	-	40	11 de marzo de 2022 02:50:34.343 p.m.
4	`TaskStart ed`	`StartAuto mationWai tForCallB ack`	-	154	11 de marzo de 2022 02:50:34.457 p.m.

5	TaskSubmitted	StartAutomationWaitForCallBack	-	657	11 de marzo de 2022 02:50:34.960 p.m.
6	TaskSucceeded	StartAutomationWaitForCallBack	-	103835	11 de marzo de 2022 02:52:18.138 p.m.
7	TaskStateExited	StartAutomationWaitForCallBack	-	103860	11 de marzo de 2022 02:52:18.163 p.m.
8	ExecutionSucceeded		-	103897	11 de marzo de 2022 02:52:18.200 p.m.

Ejecute lecturas paralelas de objetos de S3 mediante Python en una función de AWS Lambda

Creado por Eduardo Bortoluzzi

Repositorio de código: aws-lambda-parallel-download	Entorno: PoC o piloto	Tecnologías: sin servidor
Servicios de AWS: AWS Lambda; Amazon S3; AWS Step Functions		

Resumen

Puede utilizar este patrón para recuperar y resumir una lista de documentos de los buckets de Amazon Simple Storage Service (Amazon S3) en tiempo real. El patrón proporciona código de ejemplo para leer objetos en paralelo desde buckets de S3 en Amazon Web Services (AWS). El patrón muestra cómo ejecutar de manera eficiente tareas vinculadas a E/S con funciones de AWS Lambda mediante Python.

Una empresa financiera utilizó este patrón en una solución interactiva para aprobar o rechazar manualmente las transacciones financieras correlacionadas en tiempo real. Los documentos de las transacciones financieras se almacenaban en un depósito S3 relacionado con el mercado. Un operador seleccionó una lista de documentos del depósito de S3, analizó el valor total de las transacciones calculadas por la solución y decidió aprobar o rechazar el lote seleccionado.

Las tareas vinculadas a E/S admiten varios subprocesos. En este código de ejemplo, el concurrent.futures. ThreadPoolExecutorse utiliza con un máximo de 1000 subprocesos simultáneos. Las funciones Lambda admiten hasta 1024 subprocesos, y uno de esos subprocesos es el proceso principal. También debe aumentar el número máximo de conexiones del grupo para que todos los subprocesos puedan realizar la descarga del objeto S3 simultáneamente. `botocore`

El código de ejemplo usa un objeto de 8,3 KB, con datos JSON, en un bucket de S3. El objeto se lee varias veces. Una vez que la función Lambda lee el objeto, los datos JSON se decodifican en un objeto de Python. Tras ejecutar este ejemplo, se procesaron 1000 lecturas en 2,3 segundos y se procesaron 10 000 lecturas en 26 segundos mediante una función Lambda configurada con 2048

MB de memoria. El aumento de la memoria Lambda no ayudó a reducir el tiempo de ejecución de la tarea.

La herramienta AWS Lambda Power Tuning se utilizó para probar diferentes configuraciones de memoria Lambda y verificar la mejor performance-to-cost proporción para la tarea. Para ver los resultados de las pruebas, consulte la sección de información adicional.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Competencia con el desarrollo de Python

Limitaciones

- Una función Lambda puede tener como máximo 1024 procesos o subprocesos de ejecución.
- Las nuevas cuentas de AWS tienen un límite de memoria Lambda de 3008 MB. Ajuste la herramienta de ajuste de potencia de AWS Lambda en consecuencia. Para obtener más información, consulte la sección de solución de problemas.
- La versión 3.8 de Python es la versión mínima recomendada porque introdujo la reutilización de subprocesos del grupo de ejecución de subprocesos.
- Amazon S3 tiene un límite de 5500 solicitudes GET/HEAD por segundo por prefijo particionado.

Versiones de producto

- Python 3.8 o posterior
- Kit de desarrollo en la nube de AWS (AWS CDK) v2
- Interfaz de la línea de comandos de AWS (AWS CLI) versión 2
- AWS Lambda Power Tuning 4.3.3 (opcional)

Arquitectura

Pila de tecnología de destino

- AWS Lambda

- Amazon S3
- AWS Step Functions (si se ha implementado AWS Lambda Power Tuning)

Arquitectura de destino

El siguiente diagrama muestra una función Lambda que lee objetos de un bucket de S3 en paralelo. El diagrama también incluye un flujo de trabajo de Step Functions para que la herramienta AWS Lambda Power Tuning ajuste con precisión la memoria de funciones de Lambda. Este ajuste fino ayuda a lograr un buen equilibrio entre el costo y el rendimiento.

Automatizar y escalar

Las funciones Lambda se escalan rápidamente cuando es necesario. Para evitar los 503 errores de ralentización de Amazon S3 cuando hay mucha demanda, le recomendamos que ponga algunos límites al escalado.

Herramientas

Servicios de AWS

- El AWS Cloud Development Kit (AWS CDK) v2 es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura de la nube de AWS en código. La infraestructura de ejemplo se creó para implementarse con AWS CDK.
- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que le ayuda a interactuar con los servicios de AWS mediante comandos en su shell de línea de comandos. En este patrón, la versión 2 de la AWS CLI se utiliza para cargar un archivo JSON de ejemplo.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- AWS Step Functions es un servicio de orquestación sin servidor que le permite combinar funciones de Lambda AWS y otros servicios de AWS para crear aplicaciones esenciales desde el punto de vista empresarial.

Otras herramientas

- Python es un lenguaje de programación informático de uso general. La reutilización de subprocesos de trabajo inactivos se introdujo en la versión 3.8 de Python y para esta versión se creó el código de la función Lambda en este patrón.

Repositorio de código

El código de este patrón está disponible en el repositorio. aws-lambda-parallel-download GitHub

Prácticas recomendadas

- Esta construcción de AWS CDK se basa en los permisos de usuario de su cuenta de AWS para implementar la infraestructura. Si planea usar AWS CDK Pipelines o implementaciones entre cuentas, consulte Sintetizadores Stack.
- Esta aplicación de ejemplo no tiene los registros de acceso habilitados en el bucket de S3. Se recomienda habilitar los registros de acceso en el código de producción.

Epics

Prepare el entorno de desarrollo

Tarea	Descripción	Habilidades requeridas
Compruebe la versión instalada de Python.	El código proporcionado se creó y probó en Python 3.8 y versiones posterior es. Para comprobar la versión de Python instalada , ejecute`python3 -V`. Si es necesario, descarga e instala una versión más reciente. Para comprobar que los módulos necesarios están instalados, ejecute`python3 -c "import pip, venv"`. Si	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	los módulos están instalados, no se devolverá ningún error.	
Instale y configure AWS CDK.	Para instalar la AWS CDK y arrancarla si aún no está configurada, siga las instrucciones de Introducción a la AWS CDK. Para confirmar que la versión de AWS CDK instalada es 2.0 o posterior, ejecute`cdk -version`: Al arrancar, pase el parámetro a. `--cloudformation-execution-policies "arn:aws:iam::aws:policy/job-function/ViewOnlyAccess" cdk bootstrap` En este ejemplo no se usa la función definida para implementar la pila y este parámetro hace que la implementación sea más segura.	Arquitecto de la nube

Clona el repositorio de ejemplo

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Para clonar la última versión del repositorio, ejecute el siguiente comando: `git clone --depth 1 --branch v1.1.2 \`	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	`git@github.com:aws-samples/aws-lambda-parallel-download.git`	
Cambie el directorio de trabajo al repositorio clonado.	Ejecute el siguiente comando: `cd aws-lambda-parallel-download`	Arquitecto de la nube
Cree el entorno virtual de Python.	Para crear un entorno virtual de Python, ejecute el siguiente comando: `python3 -m venv .venv`	Arquitecto de la nube
Active el entorno virtual.	Para activar el entorno virtual, ejecute el siguiente comando: `source .venv/bin/activate`	Arquitecto de la nube
Instalar las dependencias.	Para instalar las dependencias de Python, ejecuta el `pip` comando: `pip install -r requirements.txt`	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Examine el código.	(Opcional) El código de ejemplo que descarga un objeto del bucket de S3 está en `resources/parallel.py`. El código de infraestructura está en la `parallel_download` carpeta.	Arquitecto de la nube

Implemente y pruebe la aplicación

Tarea	Descripción	Habilidades requeridas
Implemente la aplicación.	Ejecute `cdk deploy`. Anote los resultados de AWS CDK: • `ParallelDownloadStack.LambdaFunctionARN` • `ParallelDownloadStack.SampleS3BucketName` • `ParallelDownloadStack.StateMachineARN`	Arquitecto de la nube
Cargue un archivo JSON de ejemplo.	El repositorio contiene un archivo JSON de ejemplo de unos 9 KB. Para cargar el archivo en el depósito S3 de la pila creada, ejecuta el siguiente comando:	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	`aws s3 cp sample.json s3://<ParallelDownloadStack.SampleS3BucketName>` `<ParallelDownloadStack.SampleS3BucketName>` Sustitúyalo por el valor correspondiente de la salida de AWS CDK.	
Ejecute la aplicación.	1. Inicie sesión en la consola de administración de AWS, navegue hasta la consola de Lambda y localice la función Lambda que tiene el ARN en la salida de la CDK de AWS. `ParallelDownloadStack.LambdaFunctionARN` 2. En la pestaña Prueba, cambie el JSON del evento por el siguiente: `{"objectKey": "sample.json"}` 3. Seleccione Probar. 4. Para ver el resultado, selecciona los detalles. Los detalles mostrarán las estadísticas de la descarga paralela, la información de la ejecución y los registros.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Añade el número de descargas.	(Opcional) Para ejecutar 1500 llamadas a get object, usa el siguiente JSON en el JSON de eventos del `Test` parámetro: `{"repeat": 1500, "objectKey": "sample.json"}`	Arquitecto de la nube

Opcional: ejecute AWS Lambda Power Tuning

Tarea	Descripción	Habilidades requeridas
Ejecute la herramienta AWS Lambda Power Tuning.	1. Inicie sesión en la consola y vaya a Step Functions. 2. Localice la máquina de estado con el ARN en la salida de la CDK de AWS. `ParallelDownloadStack.StateMachineARN` 3. Elija Iniciar ejecución y pegue el siguiente JSON: `{ "lambdaARN": "<ParallelDownloadStack.LambdaFunctionARN>", "num": 5, "payload": {"repeat": 2000, "objectKey": "sample.json"}`	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	`}` Recuerde `<ParallelDownloadStack.LambdaFunctionARN>` reemplazarlo por el valor de la salida del CDK. Al final de la ejecución, el resultado aparecerá en la pestaña de entrada y salida de la ejecución.	
Vea los resultados de AWS Lambda Power Tuning en un gráfico.	En la pestaña de entrada y salida de ejecución, copie el enlace de la `visualization` propiedad y péguelo en una nueva pestaña del navegador.	Arquitecto de la nube

Limpieza

Tarea	Descripción	Habilidades requeridas
Elimine los objetos del depósito de S3.	Antes de destruir los recursos desplegados, debe eliminar todos los objetos del depósito de S3: `aws s3 rm s3://<ParallelDownloadStack.SampleS3BucketName> \` `--recursive`	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	Recuerde sustituirlo por `<ParallelDownloadStack.SampleS3BucketName>` el valor de las salidas de CDK de AWS.	
Destruye los recursos.	Para destruir todos los recursos que se crearon para este piloto, ejecuta el siguiente comando: `cdk destroy`	Arquitecto de la nube

Solución de problemas

Problema	Solución
`'MemorySize' value failed to satisfy constraint: Member must have value less than or equal to 3008`	En el caso de las cuentas nuevas, es posible que no pueda configurar más de 3008 MB en las funciones de Lambda. Para realizar una prueba con AWS Lambda Power Tuning, añada la siguiente propiedad en el JSON de entrada al iniciar la ejecución de Step Functions: `"powerValues": [ 512, 1024, 1536, 2048, 2560, 3008 ]`

Recursos relacionados

- Python: futuros simultáneos. ThreadPoolExecutor
- Cuotas Lambda: configuración, despliegue y ejecución de funciones
- Trabajar con el CDK de AWS en Python
- Funciones de creación de perfiles con AWS Lambda Power Tuning

Información adicional

Código

El siguiente fragmento de código realiza el procesamiento de E/S en paralelo:

```
with ThreadPoolExecutor(max_workers=MAX_WORKERS) as executor:
  for result in executor.map(a_function, (the_arguments)):
    ...
```

`ThreadPoolExecutor`Reutiliza los hilos cuando están disponibles.

Pruebas y resultados

La primera prueba procesó 2500 lecturas de objetos y obtuvo el siguiente resultado.

A partir de 3.009 MB, el nivel de tiempo de procesamiento se mantuvo igual para cualquier aumento de memoria, pero el coste aumentó a medida que aumentaba el tamaño de la memoria.

En otra prueba, se investigó el intervalo entre 1.536 MB y 3.072 MB de memoria, utilizando valores que eran múltiplos de 256 MB y procesando 10 000 lecturas de objetos, y se obtuvieron los siguientes resultados.

La mejor performance-to-cost relación fue con la configuración Lambda de 2.048 MB de memoria.

A modo de comparación, un proceso secuencial de 2500 lecturas de objetos tardó 40 segundos. El proceso paralelo con la configuración Lambda de 2.048 MB tardó 5,8 segundos, un 85 por ciento menos.

Configure el acceso privado a un bucket de Amazon S3 a través de un punto de enlace de VPC

Creado por Martin Maritsch (AWS), Gabriel Rodríguez García (AWS), Shukhrat Khodjaev (AWS), Nicolas Jacob Baer (AWS), Mohan Gowda Purushothama (AWS) y Joaquin Rinaudo (AWS)

Repositorio de código: Private S3 VPCE	Entorno: producción	Tecnologías: Sin servidor
Servicios de AWS: Amazon API Gateway; Amazon S3; Amazon VPC; Elastic Load Balancing (ELB)		

Resumen

En Amazon Simple Storage Service (Amazon S3), las URL prefirmadas le permiten compartir archivos de tamaño arbitrario con los usuarios de destino. De forma predeterminada, se puede acceder a las URL prefirmadas de Amazon S3 desde Internet dentro de un período de tiempo de caducidad, lo que facilita su uso. Sin embargo, los entornos corporativos suelen requerir que el acceso a las URL prefirmadas de Amazon S3 se limite únicamente a una red privada.

Este patrón presenta una solución sin servidor para interactuar de forma segura con los objetos de S3 mediante el uso de URL prefirmadas desde una red privada sin acceso a Internet. En la arquitectura, los usuarios acceden a un Application Load Balancer a través de un nombre de dominio interno. El tráfico se enruta internamente a través de Amazon API Gateway y un punto final de nube privada virtual (VPC) para el bucket de S3. La AWS Lambda función genera URL prefirmadas para la descarga de archivos a través del punto final de la VPC privada, lo que ayuda a mejorar la seguridad y la privacidad de los datos confidenciales.

Requisitos previos y limitaciones

Requisitos previos

- Una VPC que incluye una subred implementada en una Cuenta de AWS que está conectada a la red corporativa (por ejemplo, a través de). AWS Direct Connect

Limitaciones

- El bucket S3 debe tener el mismo nombre que el dominio, por lo que le recomendamos que consulte las reglas de nomenclatura del bucket de Amazon S3.
- Este ejemplo de arquitectura no incluye funciones de monitoreo para la infraestructura implementada. Si su caso de uso requiere supervisión, considere la posibilidad de añadir servicios AWS de supervisión.
- Este ejemplo de arquitectura no incluye la validación de entradas. Si tu caso de uso requiere la validación de las entradas y un mayor nivel de seguridad, considera AWS WAF utilizarla para proteger tu API.
- Esta arquitectura de ejemplo no incluye el registro de acceso con Application Load Balancer. Si tu caso de uso requiere el registro de acceso, considera habilitar los registros de acceso del balanceador de carga.

Versiones

- Python versión 3.11 o posterior
- Terraform versión 1.6 o posterior

Arquitectura

Pila de tecnología de destino

Los siguientes servicios de AWS se utilizan en el conjunto de tecnologías de destino:

- Amazon S3 es el servicio de almacenamiento principal que se utiliza para cargar, descargar y almacenar archivos de forma segura.
- Amazon API Gateway expone los recursos y puntos de enlace para interactuar con el bucket de S3. Este servicio desempeña un papel en la generación de URL prefirmadas para descargar o cargar datos.
- AWS Lambdagenera direcciones URL prefirmadas para descargar archivos de Amazon S3. API Gateway llama a la función Lambda.
- Amazon VPC implementa recursos dentro de una VPC para proporcionar aislamiento de la red. La VPC incluye subredes y tablas de enrutamiento para controlar el flujo de tráfico.
- Application Load Balancer dirige el tráfico entrante a API Gateway o al punto final de VPC del bucket de S3. Permite a los usuarios de la red corporativa acceder a los recursos internamente.

- El punto de conexión de VPC para Amazon S3 permite la comunicación directa y privada entre los recursos de la VPC y Amazon S3 sin tener que atravesar la Internet pública.
- AWS Identity and Access Management (IAM) controla el acceso a los recursos. AWS Los permisos se configuran para garantizar interacciones seguras con la API y otros servicios.

Arquitectura de destino

En el siguiente diagrama se ilustra lo siguiente:

1. Los usuarios de la red corporativa pueden acceder a Application Load Balancer a través de un nombre de dominio interno. Suponemos que existe una conexión entre la red corporativa y la subred de la intranet Cuenta de AWS (por ejemplo, a través de una AWS Direct Connect conexión).
2. El Application Load Balancer dirige el tráfico entrante a API Gateway para generar URL prefirmadas para descargar o cargar datos en Amazon S3, o al punto final de VPC del bucket de S3. En ambos casos, las solicitudes se enrutan internamente y no es necesario que atraviesen Internet.
3. API Gateway expone los recursos y los puntos finales para que interactúen con el bucket de S3. En este ejemplo, proporcionamos un punto final para descargar archivos del depósito de S3, pero esto podría ampliarse para proporcionar también la funcionalidad de carga.
4. La función Lambda genera la URL prefirmada para descargar un archivo de Amazon S3 mediante el nombre de dominio de Application Load Balancer en lugar del dominio público de Amazon S3.
5. El usuario recibe la URL prefirmada y la utiliza para descargar el archivo de Amazon S3 mediante el Application Load Balancer. El balanceador de cargas incluye una ruta predeterminada para enviar el tráfico que no está destinado a la API hacia el punto final de VPC del bucket de S3.
6. El punto final de la VPC enruta la URL prefirmada con el nombre de dominio personalizado al bucket de S3. El bucket de S3 debe tener el mismo nombre que el dominio.

Automatizar y escalar

Este patrón utiliza Terraform para implementar la infraestructura del repositorio de código en un Cuenta de AWS.

Herramientas

Herramientas

- Python es un lenguaje de programación informático de uso general.
- Terraform es una herramienta de infraestructura como código (IaC) HashiCorp que le ayuda a crear y administrar recursos locales y en la nube.
- AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que te ayuda a interactuar con los AWS servicios mediante comandos en tu consola de línea de comandos.

Repositorio de código

El código de este patrón está disponible en un GitHub repositorio en https://github.com/aws-samples/private-s3-vpce.

Prácticas recomendadas

La arquitectura de ejemplo para este patrón utiliza los permisos de IAM para controlar el acceso a la API. Cualquier persona que tenga credenciales de IAM válidas puede llamar a la API. Si su caso de uso requiere un modelo de autorización más complejo, es posible que desee utilizar un mecanismo de control de acceso diferente.

Epics

Implemente la solución en un Cuenta de AWS

Tarea	Descripción	Habilidades requeridas
Obtenga AWS las credencia les.	Revise sus AWS credencia les y el acceso a su cuenta. Para obtener instrucciones, consulte los ajustes de configuración y del archivo de credenciales en la AWS CLI documentación.	AWS DevOps, AWS general

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Clona el GitHub repositor io proporcionado con este patrón: `git clone https://g ithub.com/aws-samp les/private-s3-vpce`	AWS DevOps, AWS general
Configure las variables.	1. En su ordenador, en el GitHub repositorio, abra la `terraform` carpeta: `cd terraform` 2. Abre el `example.tfvars` archivo y personaliza los parámetros según tus necesidades.	AWS DevOps, AWS general
Implemente la solución.	1. En la `terraform` carpeta, ejecuta Terraform y pasa las variables que has personalizado: `terraform apply - var-file="example .tfvars"` 2. Confirme que los recursos que se muestran en el diagrama de arquitectura se implementaron correctam ente.	AWS DevOps, AWS general

Pruebe la solución

Tarea	Descripción	Habilidades requeridas
Cree un archivo de prueba.	Cargue un archivo en Amazon S3 para crear un escenario de prueba para la descarga del archivo. Puede utilizar la consola Amazon S3 o el siguiente AWS CLI comando: `aws s3 cp /path/to/ testfile s3://your-bucket-name/testfile`	AWS DevOps, AWS general
Pruebe la funcionalidad de las URL prefirmadas.	1. Envíe una solicitud al Application Load Balancer para crear una URL prefirmada para el archivo de prueba mediante awscurl: `awscurl https://your-domain-name/api/ get_url?key=testfile` Este paso crea una firma válida a partir de sus credenciales, que será validada por API Gateway. 2. Analice el enlace a partir de la respuesta que reciba en el paso anterior y abra la URL prefirmada para descargar el archivo.	AWS DevOps, AWS general

Tarea	Descripción	Habilidades requeridas
Elimine recursos.	Asegúrese de eliminar los recursos cuando ya no los necesite: `terraform destroy`	AWS DevOps, AWS general

Solución de problemas

Problema	Solución
Los nombres de clave de objetos de S3 con caracteres especiales, como signos numéricos (#), infringen los parámetros de la URL y provocan errores.	Codifique los parámetros de URL correctam ente y asegúrese de que el nombre de la clave del objeto S3 siga las directrices de Amazon S3.

Recursos relacionados

Amazon S3:

- Compartir objetos con direcciones URL prefirmadas
- Controlar el acceso desde los puntos finales de la VPC con políticas de bucket

Amazon API Gateway:

- Usa políticas de puntos de conexión de VPC para las API privadas en API Gateway

Application Load Balancer:

- Alojamiento de sitios web estáticos HTTPS internos con ALB, S3 y PrivateLink (AWS entrada de blog)

Encadene los servicios de AWS mediante un enfoque sin servidor

Creado por Aniket Braganza (AWS)

Entorno: producción	Tecnologías: sin servidor; nativas de la nube; desarrollo y pruebas de software; modernización; infraestructura DevOps	Servicios de AWS: Amazon S3; Amazon SNS; Amazon SQS; AWS Lambda

Resumen

Este patrón muestra un enfoque escalable y sin servidor para procesar un archivo cargado mediante la unión de Amazon Amazon Simple Storage Service (Amazon S3), Amazon Simple Notification Service (Amazon SNS), Amazon Simple Queue Service (Amazon SQS) y Amazon AWS Lambda. El ejemplo del archivo cargado es para fines ilustrativos. Puede utilizar un enfoque sin servidor para completar otras tareas al encadenar la combinación de servicios de AWS necesaria para cumplir sus objetivos empresariales. El enfoque sin servidor emplea un flujo de trabajo asíncrono que se basa en notificaciones basadas en eventos, un almacenamiento flexible y la informática de Función como servicio (FaaS) para procesar las solicitudes. Puede utilizar el enfoque sin servidor para escalar y satisfacer la demanda y, al mismo tiempo, minimizar los costos.

Nota: Existen varias opciones para encadenar los servicios de AWS mediante un enfoque sin servidor. Por ejemplo, puede utilizar un enfoque que combine Lambda con Amazon S3 en lugar de Amazon SNS y Amazon SQS. Sin embargo, este patrón utiliza Amazon SNS y Amazon SQS porque este enfoque permite añadir varios puntos de integración al proceso de invocación de Lambda durante una notificación de eventos y ampliar la implementación para incluir varios oyentes en una orquestación sin servidor y, al mismo tiempo, minimizar la sobrecarga de procesamiento.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Acceso programático a la cuenta de AWS. Para obtener más información, consulte:

  - Requisitos previos de la documentación del AWS Cloud Development Kit (AWS CDK)
  - Requisitos previos de la documentación de la Interfaz de la línea de comandos de AWS (AWS CLI)
- AWS CDK, instalada
- CLI de AWS, instalada y configurada
- Python 3.9

Versiones de producto

- AWS CDK 2.x
- Python 3.9

Arquitectura

En el siguiente diagrama, se muestra cómo los servicios de AWS encadenados pueden permitir a un usuario cargar un archivo a un bucket de S3 para su procesamiento:

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un usuario sube un archivo al bucket S3.
2. La carga inicia un evento de S3 que publica un mensaje en un tema de SNS. El mensaje contiene los detalles del evento de S3.
3. El mensaje publicado en el tema de SNS se inserta en una cola de SQS, que está suscrita y recibe notificaciones sobre ese tema.
4. Una función de Lambda sondea la cola de SQS (como fuente de eventos) y espera a que se procesen los mensajes.
5. Cuando la función de Lambda recibe mensajes de la cola de SQS, los procesa y confirma la recepción de esos mensajes.
6. Si Lambda no procesa un mensaje, ese mensaje se devuelve a la cola de SQS y, finalmente, se transfiere a una cola de mensajes fallidos de SQS.

Pila de tecnología

- Amazon S3
- Amazon SNS
- Amazon SQS
- AWS Lambda

Herramientas

Servicios de AWS

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Amazon Simple Notification Service (Amazon SNS) lo ayuda a coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- Amazon Simple Queue Service (Amazon SQS) ofrece una cola alojada segura, duradera y disponible que le permite integrar y desacoplar sistemas y componentes de software distribuidos.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.

Otras herramientas

- El AWS Cloud Development Kit (AWS CDK) es la herramienta principal para interactuar con su aplicación de AWS CDK. Ejecuta su aplicación, interroga el modelo de aplicación que ha definido y produce e implementa las CloudFormation plantillas de AWS generadas por la CDK de AWS.
- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de la línea de comandos.
- Python es un lenguaje de programación de uso general interpretado de alto nivel.

Código

El código de este patrón está disponible en el repositorio GitHub Chaining S3 to SNS to SQS to Lambda.

Epics

Desarrolle su entorno sin servidores

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Clone el repositorio y navegue hasta la carpeta `python/s3-sns-sqs-lambda-chain` .	Desarrollador de aplicaciones
Configurar un entorno virtual.	1. En la AWS CDK, ejecute el comando `python3 -m venv .venv`. 2. Ejecute el comando `source .venv/bin/activate` en macOS o `.venv\Scripts\activate.bat` en Windows.	Desarrollador de aplicaciones
Instale las dependencias.	Ejecute el comando `pip install -r requirements.txt` .	Desarrollador de aplicaciones

Pruebe la pila CloudFormation

Tarea	Descripción	Habilidades requeridas
Realice pruebas unitarias.	1. Ejecute el comando `pip install -r requirements-dev.txt` . 2. (Opcional) Ejecute el `cdk synth --no-staging > template.yml` comando para generar la CloudFormation	Desarrollador, ingeniero de pruebas

Tarea	Descripción	Habilidades requeridas
	pila. Importante: puede inspeccionar la pila, pero evite generar recursos y artefactos por etapas. 3. Ejecute el comando `pytest` para ejecutar todas las pruebas unitarias. 4. (Opcional) Ejecute el comando `pytest tests/unit/<test_filename>` para ejecutar las pruebas de un archivo específico.	

Implemente la CloudFormation pila

Tarea	Descripción	Habilidades requeridas
Configure el entorno de arranque.	Siga las instrucciones de Bootstrapping de la documentación de AWS para iniciar el entorno para la implementación de la CDK de AWS en cada región de AWS en la que se implementará la CloudFormation pila. Nota: Este paso requiere que disponga de credenciales con acceso programático.	Desarrollador de aplicaciones, ingeniero e ingeniero de datos DevOps
Implemente la CloudFormation pila.	Ejecute el comando `cdk deploy` para crear e	Desarrollador de aplicacio nes, DevOps ingeniero, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	implementar la pila en la cuenta de AWS.	

Limpiar los recursos de su entorno

Tarea	Descripción	Habilidades requeridas
Elimine la CloudFormation pila y elimine los recursos asociados.	Para eliminar la CloudFormation pila que se creó y eliminar todos los recursos asociados, ejecute el comando `run cdk` destroy.	Desarrollador de aplicaciones

Más patrones

- Acceder, consultar y unirse a las tablas de Amazon DynamoDB con Athena
- Agregue datos en Amazon DynamoDB para pronósticos de ML en Athena
- Automatice la evaluación de recursos de AWS
- Automatice la implementación de aplicaciones anidadas mediante SAM de AWS
- Automatice la replicación de las instancias de Amazon RDS en todas las cuentas de AWS
- Archivar automáticamente los elementos en Amazon S3 con DynamoDB TTL
- Detecta automáticamente los cambios e inicia diferentes CodePipeline canalizaciones para un monorepo en CodeCommit
- Cree una arquitectura de acoplamiento flexible con microservicios mediante DevOps prácticas y AWS Cloud9
- Cree una arquitectura sin servidor multiusuario en Amazon Service OpenSearch
- Cree un visor de archivos de unidad central avanzada en la nube de AWS
- Calcule el valor en riesgo (VaR) mediante los servicios de AWS
- Copiar los productos de AWS Service Catalog en diferentes cuentas y regiones de AWS
- Crear automáticamente canalizaciones de CI dinámicas para proyectos de Java y Python
- Descomponga monolitos en microservicios mediante CQRS y abastecimiento de eventos
- Implemente una aplicación de una sola página basada en React en Amazon S3 y CloudFront
- Implemente una API de Amazon API Gateway en un sitio web interno mediante puntos de conexión privados y un Equilibrador de carga de aplicación
- Implementar y depurar clústeres de Amazon EKS
- Implementar y administrar un lago de datos sin servidor en la nube de AWS mediante el uso de la infraestructura como código
- Implementar funciones de Lambda con imágenes de contenedor
- Desarrolle un asistente totalmente automatizado basado en el chat con los agentes y las bases de conocimiento de Amazon Bedrock
- Desarrolle asistentes avanzados de IA generativa basados en chat mediante RAG y solicitudes ReAct
- Genere dinámicamente una política de IAM con IAM Access Analyzer mediante Step Functions
- Asegúrese de que el registro de Amazon EMR en Amazon S3 esté habilitado en el lanzamiento
- Estime el costo de una tabla de DynamoDB para la capacidad bajo demanda

- Genere recomendaciones personalizadas y reclasificadas con Amazon Personalize
- Genere datos de prueba con un trabajo de AWS Glue y Python
- Implementar el patrón saga sin servidor mediante AWS Step Functions
- Mejore el rendimiento operativo al habilitar Amazon DevOps Guru en varias regiones, cuentas y unidades organizativas de AWS con la AWS CDK
- Lance un CodeBuild proyecto en todas las cuentas de AWS mediante Step Functions y una función de proxy Lambda
- Migre las cargas de trabajo de Apache Cassandra a Amazon Keyspaces con AWS Glue
- Supervisar el uso de una imagen de máquina de Amazon compartida en varias cuentas de AWS
- Orqueste un proceso de ETL con validación, transformación y particionamiento mediante AWS Step Functions
- Ejecute cargas de trabajo programadas y basadas en eventos a escala con AWS Fargate.
- Sirva contenido estático en un bucket de Amazon S3 a través de una VPC mediante Amazon CloudFront
- Estructure un proyecto de Python en una arquitectura hexagonal con AWS Lambda
- Cómo desactivar los controles estándar de seguridad en todas las cuentas de los miembros de Security Hub en un entorno de varias cuentas

Desarrollo y pruebas de software

Temas

- Genere automáticamente un modelo de PynamoDB y funciones CRUD para Amazon DynamoDB mediante una aplicación de Python
- Explore el desarrollo completo de aplicaciones web nativas en la nube con Green Boost
- Ejecute pruebas unitarias para una aplicación GitHub de Node.js desde AWS CodeBuild
- Estructure un proyecto de Python en una arquitectura hexagonal con AWS Lambda
- Más patrones

Genere automáticamente un modelo de PynamoDB y funciones CRUD para Amazon DynamoDB mediante una aplicación de Python

Creado por Vijit Vashishtha (AWS), Dheeraj Alimchandani (AWS) y Dhananjay Karanjkar (AWS)

Repositorio de código: amazon-reverse-engineer-dynamodb	Entorno: PoC o piloto	Tecnologías: desarrollo y pruebas de software; bases de datos; DevOps
Carga de trabajo: código abierto	Servicios de AWS: Amazon DynamoDB	

Resumen

Es habitual necesitar entidades y funciones de operaciones de creación, lectura, actualización y eliminación (CRUD) para realizar de forma eficiente las operaciones de base de datos de Amazon DynamoDB. PynamoDB es una interfaz basada en Python que admite Python 3. También proporciona funciones como la compatibilidad con las transacciones de Amazon DynamoDB, la serialización y deserialización automáticas de valores de atributos y la compatibilidad con los marcos de Python más comunes, como Flask y Django. Este patrón ayuda a los desarrolladores a trabajar con Python y DynamoDB al proporcionar una biblioteca que agiliza la creación automática de modelos de PynamoDB y funciones de operación CRUD. Si bien genera funciones CRUD esenciales para las tablas de bases de datos, también puede aplicar ingeniería inversa a los modelos de PynamoDB y a las funciones CRUD de las tablas de Amazon DynamoDB. Este patrón está diseñado para simplificar las operaciones de la base de datos mediante una aplicación basada en Python.

Las características principales de esta solución son las siguientes:

- Esquema JSON a modelo PynamoDB: genere automáticamente modelos PynamoDB en Python importando un archivo de esquema JSON.
- Generación de funciones CRUD: genere automáticamente funciones para realizar operaciones CRUD en tablas de DynamoDB.

- Ingeniería inversa desde DynamoDB: utilice el mapeo relacional de objetos (ORM) de PynamoDB para aplicar ingeniería inversa a los modelos de PynamoDB y a las funciones CRUD de las tablas de Amazon DynamoDB existentes.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Python versión 3.8 o posterior, descargada e instalada
- Jinja2, versión 3.1.2 o posterior, descargada e instalada
- Tablas de Amazon DynamoDB para las que desea generar ORM
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada
- PynamoDB versión 5.4.1 o posterior, instalada

Arquitectura

Pila de tecnología de destino

- Script JSON
- Aplicación Python
- Modelo PynamoDB
- Instancia de base de datos Amazon DynamoDB

Arquitectura de destino

1. Se crea un archivo de esquema JSON de entrada. Este archivo de esquema JSON representa los atributos de las tablas de DynamoDB respectivas a partir de las que desea crear modelos de PyNamoDB y para las que desea crear funciones CRUD. Contiene las tres claves importantes siguientes:
   - `name`: el nombre de la tabla de DynamoDB de destino.
   - `region`— La región de AWS donde está alojada la tabla

- `attributes`— Los atributos que forman parte de la tabla de destino, como la clave de partición (también conocida como atributo hash), la clave de clasificación, los índices secundarios locales, los índices secundarios globales y cualquier atributo que no sea clave. Esta herramienta espera que el esquema de entrada solo proporcione los atributos no clave, ya que la aplicación los obtiene directamente de la tabla de destino. Para ver un ejemplo de cómo especificar los atributos en el archivo de esquema JSON, consulta la sección de información adicional de este patrón.

2. Ejecute la aplicación Python y proporcione el archivo de esquema JSON como entrada.
3. La aplicación Python lee el archivo de esquema JSON.
4. La aplicación Python se conecta a las tablas de DynamoDB para derivar el esquema y los tipos de datos. La aplicación ejecuta la operación describe_table y obtiene los atributos clave y de índice de la tabla.
5. La aplicación Python combina los atributos del archivo de esquema JSON y la tabla de DynamoDB. Utiliza el motor de plantillas Jinja para generar un modelo PynamoDB y las funciones CRUD correspondientes.
6. Puede acceder al modelo PynamoDB para realizar operaciones CRUD en la tabla de DynamoDB.

Herramientas

Servicios de AWS

- Amazon DynamoDB es un servicio de base de datos de NoSQL completamente administrado que ofrece un rendimiento rápido, predecible y escalable.

Otras herramientas

- Jinja es un motor de plantillas extensible que compila plantillas en código Python optimizado. Este patrón usa Jinja para generar contenido dinámico al incrustar marcadores de posición y lógica dentro de las plantillas.
- PynamoDB es una interfaz basada en Python para Amazon DynamoDB.
- Python es un lenguaje de programación informático de uso general.

Repositorio de código

El código de este patrón está disponible en el repositorio de funciones CRUD y modelos de PynamoDB de GitHub generación automática. El repositorio se divide en dos partes principales: el paquete de controladores y las plantillas.

Paquete de controladores

El paquete Python del controlador contiene la lógica de aplicación principal que ayuda a generar el modelo PynamoDB y las funciones CRUD. Contiene lo siguiente:

- `input_json_validator.py`— Este script de Python valida el archivo de esquema JSON de entrada y crea los objetos Python que contienen la lista de tablas de DynamoDB de destino y los atributos necesarios para cada una de ellas.
- `dynamo_connection.py`— Este script establece una conexión con la tabla de DynamoDB y utiliza `describe_table` la operación para extraer los atributos necesarios para crear el modelo de PynamoDB.
- `generate_model.py`— Este script contiene una clase de Python `GenerateModel` que crea el modelo PynamoDB en función del archivo de esquema JSON de entrada y de la operación. `describe_table`
- `generate_crud.py`— Para las tablas de DynamoDB que se definen en el archivo de esquema JSON, este script utiliza `GenerateCrud` la operación para crear las clases de Python.

Plantillas

Este directorio de Python contiene las siguientes plantillas de Jinja:

- `model.jinja`— Esta plantilla de Jinja contiene la expresión de plantilla para generar el script de modelo de PynamoDB.
- `crud.jinja`— Esta plantilla Jinja contiene la expresión de plantilla para generar el script de funciones CRUD.

Epics

Configuración del entorno

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Introduzca el siguiente comando para clonar el repositorio de funciones CRUD y modelos de PynamoDB de generación automática. `git clone https://github.com/aws-samples/amazon-reverse-engineer-dynamodb.git`	Desarrollador de aplicaciones
Configure el entorno Python.	1. Navegue hasta el directorio de nivel superior del repositorio clonado. `cd amazon-reverse-engineer-dynamodb` 2. Introduzca el siguiente comando para instalar las bibliotecas y los paquetes necesarios. `pip install -r requirements.txt`	Desarrollador de aplicaciones

Generar el modelo PynamoDB y las funciones CRUD

Tarea	Descripción	Habilidades requeridas
Modifique el archivo de esquema JSON.	1. Navegue hasta el directorio de nivel superior del repositorio clonado. `cd amazon-reverse-engineer-dynamodb` 2. Abre el `test.json` archivo en el editor que prefieras. Puede usar este archivo como referencia para crear su propio archivo de esquema JSON o puede actualizar los valores de este archivo para que coincidan con su entorno. 3. Modifique los valores de nombre y atributos de las tablas de DynamoDB de destino. Región de AWS Nota: Si define una tabla que no existe en el archivo de esquema JSON, esta solución no genera modelos ni funciones CRUD para esa tabla. 4. Guarde y cierre el archivo `test.json` . Se recomienda guardar este archivo con un nombre nuevo.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Ejecute la aplicación Python.	Introduzca el siguiente comando para generar los modelos de PynamoDB y las funciones CRUD, `<input_schema.json>` donde aparece el nombre del archivo de esquema JSON. `python main.py --file <input_schema.json>`	Desarrollador de aplicaciones

Verificar el modelo PynamoDB y las funciones CRUD

Tarea	Descripción	Habilidades requeridas
Compruebe el modelo PynamoDB generado.	1. En el directorio de nivel superior del repositorio clonado, introduzca el siguiente comando para acceder al repositorio. `models` `cd models` 2. De forma predeterminada, esta solución asigna un nombre al archivo de modelo de PynamoDB. `demo_model.py` Valide que este archivo esté presente.	Desarrollador de aplicaciones
Verifique las funciones CRUD generadas.	1. En el directorio de nivel superior del repositor io clonado, introduce el	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	siguiente comando para acceder al repositorio. `crud` `cd crud` 2. De forma predeterminada, esta solución asigna un nombre al script. `demo_crud.py` Valide que este archivo esté presente. 3. Utilice las clases de Python del `demo_crud.py` archivo para realizar una operación CRUD en la tabla de DynamoDB de destino. Confirme que la operación se ha completado correctamente.	

Recursos relacionados

- Componentes principales de Amazon DynamoDB (documentación de DynamoDB)
- Mejora del acceso a los datos con índices secundarios (documentación de DynamoDB)

Información adicional

Ejemplos de atributos para el archivo de esquema JSON

```
[
{
"name": "test_table",
"region": "ap-south-1",
"attributes": [
```

```
{
"name": "id",
"type": "UnicodeAttribute"
},
{
"name": "name",
"type": "UnicodeAttribute"
},
{
"name": "age",
"type": "NumberAttribute"
}
]
}
]
```

Explore el desarrollo completo de aplicaciones web nativas en la nube con Green Boost

Creado por Ben Stickley (AWS) y Amiin Samatar (AWS)

Entorno: PoC o piloto	Tecnologías: desarrollo y pruebas de software; aplicaciones web y móviles; nativas de la nube	Carga de trabajo: código abierto
Servicios de AWS: Amazon Aurora; AWS CDK; Amazon CloudFront; AWS Lambda; AWS WAF		

Resumen

En respuesta a las necesidades cambiantes de los desarrolladores, Amazon Web Services (AWS) reconoce la demanda crítica de un enfoque eficiente para desarrollar aplicaciones web nativas en la nube. El objetivo de AWS es ayudarlo a superar los obstáculos comunes asociados con la implementación de aplicaciones web en la nube de AWS. Al aprovechar las capacidades de las tecnologías modernas, como el TypeScript AWS Cloud Development Kit (AWS CDK), React y Node.js, este patrón tiene como objetivo agilizar y acelerar el proceso de desarrollo.

Basado en el kit de herramientas Green Boost (GB), el patrón ofrece una guía práctica para crear aplicaciones web que utilicen al máximo las amplias capacidades de AWS. Actúa como una hoja de ruta integral que lo guía a través del proceso de implementación de una aplicación web CRUD (creación, lectura, actualización, eliminación) fundamental integrada con la edición compatible con Amazon Aurora PostgreSQL. Esto se logra mediante el uso de la interfaz de la línea de comandos de Green Boost (CLI de Green Boost) y el establecimiento de un entorno de desarrollo en las instalaciones.

Tras la implementación exitoso de la aplicación, el patrón profundiza en los componentes clave de la aplicación web, como el diseño de la infraestructura, el desarrollo del backend y el front-end, y en herramientas esenciales como cdk-dia para la visualización, lo que facilita la gestión eficiente de los proyectos.

Requisitos previos y limitaciones

Requisitos previos

- Git instalado
- Visual Studio Code (VS Code) instalado
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada
- Kit de herramientas de AWS CDK instalado
- Node.js 18 instalado o Node.js 18 con pnpm activado
- pnpm está instalado, si no forma parte de la instalación de Node.js
- Familiaridad básica con TypeScript AWS CDK, Node.js y React
- Una cuenta de AWS activa
- Una cuenta de AWS iniciada mediante AWS CDK en `us-east-1`. La región de `us-east-1` AWS es necesaria para admitir las funciones de Amazon CloudFront Lambda @Edge.
- Credenciales de seguridad de AWS, incluida `AWS_ACCESS_KEY_ID`, correctamente configuradas en su entorno de terminal
- Para los usuarios de Windows, un terminal en modo administrador (para adaptarse a la forma en que pnpm gestiona los módulos de nodos)

Versiones de producto

- AWS SDK para la JavaScript versión 3
- AWS CDK versión 2
- CLI de AWS versión 2.2
- Node.js versión 18
- React versión 18

Arquitectura

Pila de tecnología de destino

- Edición de Amazon Aurora compatible con PostgreSQL
- Amazon CloudFront
- Amazon CloudWatch

- Amazon Elastic Compute Cloud (Amazon EC2)
- AWS Lambda
- AWS Secrets Manager
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)
- AWS WAF

Arquitectura de destino

El siguiente diagrama muestra que las solicitudes de los usuarios pasan por Amazon CloudFront, AWS WAF y AWS Lambda antes de interactuar con un bucket de S3, una base de datos de Aurora o una instancia de EC2 y, finalmente, llegar a los desarrolladores. Los administradores, por otro lado, utilizan Amazon SNS y Amazon con CloudWatch fines de notificación y supervisión.

Para obtener una visión más profunda de la aplicación tras su implementación, puede crear un diagrama con cdk-dia, como se muestra en el siguiente ejemplo.

Estos diagramas muestran la arquitectura de la aplicación web desde dos ángulos distintos. El diagrama cdk-dia ofrece una vista técnica detallada de la infraestructura de CDK de AWS y destaca servicios específicos de AWS, como Amazon Aurora, compatible con PostgreSQL, y AWS Lambda. Por el contrario, el otro diagrama adopta una perspectiva más amplia y hace hincapié en el flujo lógico de los datos y las interacciones de los usuarios. La diferencia clave reside en el nivel de detalle: el cdk-dia profundiza en las complejidades técnicas, mientras que el primer diagrama ofrece una visión más centrada en el usuario.

La creación del diagrama cdk-dia se describe en la epopeya Comprenda la infraestructura de aplicaciones mediante AWS CDK.

Herramientas

Servicios de AWS

- La edición de Amazon Aurora compatible con PostgreSQL es un motor de base de datos relacional compatible con ACID, completamente administrado que le permite configurar, utilizar y escalar implementaciones de PostgreSQL.

- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura de la nube de AWS en código.
- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante comandos en su intérprete de comandos de línea de comandos.
- Amazon CloudFront acelera la distribución de tu contenido web al distribuirlo a través de una red mundial de centros de datos, lo que reduce la latencia y mejora el rendimiento.
- Amazon le CloudWatch ayuda a monitorizar las métricas de sus recursos de AWS y las aplicaciones que ejecuta en AWS en tiempo real.
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.
- AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Ejecuta el código solo cuando es necesario y amplía la capacidad de manera automática, por lo que solo pagará por el tiempo de procesamiento que utilice.
- AWS Secrets Manager le permite reemplazar las credenciales codificadas en el código, incluidas las contraseñas, con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación.
- AWS Systems Manager le permite administrar las aplicaciones y la infraestructura que se ejecutan en la nube de AWS. Simplifica la administración de aplicaciones y recursos, reduce el tiempo requerido para detectar y resolver problemas operativos y ayuda a utilizar y administrar los recursos de AWS a escala de manera segura. Este patrón utiliza el administrador de sesiones de AWS Systems Manager.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le permite almacenar, proteger y recuperar cualquier cantidad de datos. Amazon Simple Notification Service (Amazon SNS) le permite coordinar y administrar el intercambio de mensajes entre publicadores y clientes, incluidos los servidores web y las direcciones de correo electrónico.
- AWS WAF es un firewall de aplicación web que le permite monitorizar las solicitudes HTTP y HTTPS que se reenvíen a los recursos de su aplicación web protegida

Otras herramientas

- Git es un sistema de control de versiones distribuido y de código abierto.

- Green Boost es un conjunto de herramientas para crear aplicaciones web en AWS.
- Next.js es un marco de React para añadir funciones y optimizaciones.
- Node.js es un entorno de JavaScript ejecución basado en eventos diseñado para crear aplicaciones de red escalables.
- pgAdmin es una herramienta de gestión de código abierto para PostgreSQL. Proporciona una interfaz gráfica que permite crear, mantener y utilizar objetos de bases de datos.
- pnpm es un administrador de paquetes para las dependencias del proyecto Node.js.

Prácticas recomendadas

Consulte la sección Epics para obtener más información sobre las siguientes recomendaciones:

- Supervise la infraestructura mediante Amazon CloudWatch Dashboards y alarmas.
- Aplique las prácticas recomendadas de AWS mediante cdk-nag para ejecutar análisis estáticos de infraestructura como código (IaC).
- Establezca el reenvío de puertos de base de datos a través de túneles SSH (Secure Shell) con Systems Manager Session Manager, que es más seguro que tener una dirección IP expuesta públicamente.
- Gestione las vulnerabilidades ejecutando `pnpm audit`.
- Aplique las mejores prácticas utilizando ESLint para realizar análisis de TypeScript código estático y Prettier para estandarizar el formato del código.

Epics

Implemente una aplicación web CRUD con Aurora compatible con PostgreSQL

Tarea	Descripción	Habilidades requeridas
Instale la CLI de Green Boost.	Para instalar Green Boost CLI, ejecute el siguiente comando. `pnpm add -g gboost`	Desarrollador de aplicaciones
Cree una aplicación GB.	1. Para crear una aplicació n mediante Green Boost,	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	ejecute el comando `gboost create`. 2. Elija la plantilla `CRUD App with Aurora PostgreSQL .`	

Tarea	Descripción	Habilidades requeridas
Instale las dependencias e implemente la aplicación.	1. Desplácese hasta el directorio del proyecto: `cd <your directory>` . 2. Utilice el comando `pnpm i` para instalar las dependencias. 3. Vaya al directorio infra: `cd infra`. 4. Para implementar la aplicación, ejecute el siguiente comando `pnpm deploy:local` . Se trata de un alias para un comando `cdk deploy ...` definido en `infra/package.json` . Espere a que finalice la implementación (aproximadamente 20 minutos). Mientras espera, supervise las CloudFormation pilas de AWS en la CloudFormation consola. Observe cómo las estructuras definidas en el código se corresponden con el recurso implementado. Revise la vista en árbol de CDK Construct en la CloudFormation consola.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Accede a la aplicación.	Después de implementar su aplicación GB de forma local, puede acceder a ella mediante la CloudFront URL. La URL se imprime en la salida del terminal, pero encontrar la puede resultar un poco abrumador. Siga los pasos siguientes para encontrarlo rápidamente: 1. Abra la terminal en la que ejecutó el comando `pnpm deploy:local` . 2. Busque una sección en la salida del terminal que se parezca al texto siguiente. `myapp5stickbui9C39A55A.CloudFrontDomainName = d1q16n5pof924c.cloudfront.net` La URL será exclusiva para la implementación. Como alternativa, puedes encontrar la CloudFront URL accediendo a la CloudFront consola de Amazon: 1. Inicie sesión en la consola de administración de	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	AWS y navegue hasta el CloudFront servicio. 2. Busque la última distribución implementada en la lista. Copie el nombre de dominio asociado a la distribución. Tendrá un aspecto similar a `your-unique-id.cloudfront.net` .	

Supervise mediante Amazon CloudWatch

Tarea	Descripción	Habilidades requeridas
Ver el CloudWatch panel de control.	1. Abre la CloudWatch consola y selecciona Paneles de mandos. 2. Seleccione el panel que tiene el nombre <appId>-<stageName>-dashboard. 3. Revise el panel. ¿Qué recursos se están supervisando? ¿Qué métricas se registran? Este panel es posible gracias a la construcción de código abierto. cdk-monitoring-constructs	Desarrollador de aplicaciones
Habilitar de alertas.	Un CloudWatch panel de control le ayuda a monitorear activamente su aplicación	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	web. Para supervisar de forma pasiva su aplicación web, puede activar las alertas. 1. Navegue hasta `/infra/src/app/stateless/monitor-stack.ts` , que define la pila de monitores. 2. Elimine los comentarios de la siguiente línea y sustituya `admin@example.com` por su dirección de correo electrónico. `onAlarmTopic.addSubscription(new EmailSubscription("admin@example.com"));` 3. Añada la información siguiente sobre las importaciones a la parte superior del archivo. `import { EmailSubscription } from "aws-cdk-lib/aws-sns-subscriptions";` 4. En `infra/`, ejecute el siguiente comando. `cdk deploy "*/monitor" --exclusively.` 5. Para confirmar su suscripción al tema de SNS que se	

Tarea	Descripción	Habilidades requeridas
	inicia cuando se activa una alarma de monitorización, elija el enlace del mensaje de correo electrónico.	

Comprenda la infraestructura de aplicaciones mediante AWS CDK

Tarea	Descripción	Habilidades requeridas
Cree un diagrama de arquitectura.	Genere un diagrama de arquitectura de su aplicación web mediante cdk-dia. La visualización de la arquitectura ayuda a mejorar la comprensión y la comunicación entre los miembros del equipo. Proporciona una visión general clara de los componentes del sistema y sus relaciones. 1. Instale Graphviz. 2. En `infra/`, ejecute el comando `pnpm cdk-dia`. 3. Ver su `infra/diagram.png` .	Desarrollador de aplicaciones
Use cdk-nag para aplicar las prácticas recomendadas.	Utilice cdk-nag para ayudarle a mantener una infraestructura segura y que cumpla con las normas, aplicando las prácticas recomendadas y reduciendo el riesgo de	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	vulnerabilidades de seguridad y errores de configuración. 1. Conozca las prácticas recomendadas de cdk-nag en su sección de reglas, que incluye las comprobaciones del paquete de reglas de la biblioteca de soluciones de AWS. 2. Para ver cómo cdk-nag aplica las reglas, realice un cambio en el código. Por ejemplo, en `infra/src/app/stateful/data-stacks.ts` , cambie `storageEncrypted: true` a `storageEncrypted: false` . 3. En `infra/`, ejecute el comando `cdk synth "*/data"`. Durante la síntesis, se producirá un error de compilación que indica una infracción de la regla. `AwsSolutions-RDS2: The RDS instance or Aurora DB cluster does not have storage encryption enabled.` Este error muestra cómo cdk-nag es un mecanismo	

Tarea	Descripción	Habilidades requeridas
	de seguridad para aplicar las prácticas recomendadas de infraestructura y evitar errores de configuración de seguridad. 4. Si es necesario, también puede suprimir las reglas en diferentes ámbitos. Por ejemplo, para suprimir AwsSolutions -RDS2, añade el siguiente código debajo de la instanciación de. `DbIamCluster` `NagSuppressions.addResourceSuppressions( cluster.node.findChild("Resource"), [ { id: "AwsSolutions-RDS2", reason: "Customer requirement necessitates having unencrypted DB storage", }, ], );` 5. Tras la supresión, vuelva a ejecutar `cdk synth "*/data"`. Su aplicación AWS CDK ahora debería sintetizarse correctamente. Puede encontrar todas	

Tarea	Descripción	Habilidades requeridas
	las reglas suprimidas en `infra/cdk.out/assembly-<appId>-<stageName>/AwsSolutions-<appId>-<stageName>-${stackId}-NagReport.csv` .	

Evalúe la configuración y el esquema de la base de datos

Tarea	Descripción	Habilidades requeridas
Adquiera variables de entorno.	Para obtener las variables de entorno requeridas, siga los siguientes pasos: 1. Para encontrar el `DB_BASTION_ID` , inicie sesión en la consola y navegue hasta la consola EC2. Elija Instancias (en ejecución) y busque la fila que contiene - Nombre. ssm-db-bastion <stageName> El Identificador de instancia comienza por i-. 2. Para buscar `DB_ENDPOINT` , en la consola de Amazon Relational Database Service (Amazon RDS), elija Instancias de base de datos y seleccione el clúster regional que tiene	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	un identificador de base de datos que comience por <appId>-<stageName>-data-. Localice el punto de conexión de la instancia de escritura, que termina en rds.amazonaws.com.	
Establezca el reenvío de puertos.	Para establecer el reenvío de puertos, siga estos pasos: 1. Instale el complemento Administrador de sesiones de AWS Systems Manager. 2. Inicie el reenvío de puertos ejecutando `pnpm db:connect` dentro de `core/` para establecer una conexión segura a través del host bastión. 3. Cuando vea el texto `Waiting for connections...,` en su terminal, significa que se ha establecido correctam ente un túnel SSH entre su máquina local y el servidor Aurora a través del host bastión de EC2.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Ajuste el tiempo de espera del Administrador de sesiones de Systems Manager.	(Opcional) Si el tiempo de espera predeterminado de la sesión de 20 minutos es demasiado corto, puede aumentarlo hasta 60 minutos en la consola de Systems Manager seleccionando Administrador de sesiones, Preferencias, Editar, Tiempo de espera de sesión inactiva.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Visualice la base de datos.	pgAdmin es una herramienta de código abierto fácil de usar para administrar bases de datos PostgreSQL. Simplific a las tareas de las bases de datos, lo que le permite crear, administrar y optimizar las bases de datos de manera eficiente. Esta sección le guía a través de la instalación de pgAdmin y el uso de sus funciones para la administr ación de bases de datos PostgreSQL. 1. En el Explorador de objetos, abra el menú contextual (haga clic con el botón derecho) de Servidores y, a continuac ión, seleccione Registrar, Servidor. 2. En la pestaña General, escriba <appId>-< stageName> para el campo Nombre. 3. Para obtener la contraseñ a de la base de datos, abra la consola de AWS Secrets Manager, seleccione el secreto que contenga la descripción Generated by the CDK for the stack: <appId>-<stageName	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	>-data y elija la tarjeta Valor secreto. Seleccione Recuperar Valor secreto y copie el Valor secreto con una clave o contraseña. 4. En la pestaña Conexión, introduzca 0.0.0 para el campo Nombre/dirección del host e introduzca <appId>_admin para el campo Nombre de usuario. Para el campo Contraseña, use el secreto que obtuvo anteriormente. Seleccione Sí en el campo ¿Guardar contraseña?. 5. Seleccione Guardar. 6. Para ver las tablas, vaya a <appId>-<stageName>, Bases de datos, <appId>_db, Esquemas, <appId>, Tablas. 7. Abra el menú contextual (haga clic con el botón derecho) de la tabla de Elementos y, a continuación, seleccione Ver/editar datos, Todas las filas. 8. Explore la tabla.	

Depuración con Node.js

Tarea	Descripción	Habilidades requeridas
Depura el caso práctico de creación de objetos.	Para depuración del caso práctico de creación de elementos, siga estos pasos: 1. Abra el archivo `core/src/modules/item/create-item.use-case.ts` e inserte el siguiente código. 2. El código agregado en el paso anterior garantiza que se llame a la función de `createItemUseCase` cuando este módulo se ejecute directamente.	Desarrollador de aplicaciones

```
import { fileURLTo
Path } from "node:url
";

// existing create-it
em.use-case.ts code
 here

if (process.argv[1]
 === fileURLTo
Path(import.meta.u
rl)) {
  createItemUseCase(
{
    description:
 "Item 1's Descripti
on",
    name: "Item 1",
  });
}
```

Tarea	Descripción	Habilidades requeridas
	Establezca puntos de interrupción en las líneas de este bloque de código en las que desee iniciar la line-by-line depuración. 1. Abre la terminal de JavaScript depuración de VS Code y, a continuación, ejecuta `pnpm tsx core/src/modules/item/create-item.use-case.ts` para ejecutar el código con la depuración. line-by-line Como alternativa, puede usar sentencias e `console.log` , pero las instrucciones impresas pueden resultar inadecuadas cuando trabajas con una lógica empresarial compleja. La ine-by-line depuración L te da más contexto.	

Desarrolle la interfaz

Tarea	Descripción	Habilidades requeridas
Configure el servidor de desarrollo.	1. Navegue hasta `ui/` y ejecute `pnpm dev` para iniciar el servidor de desarrollo Next.js.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	2. Acceda a su aplicación web de forma local en `http://localhost:3000` . El servidor de desarrollo Next.js está configurado con información instantánea de Fast Refresh sobre las modificaciones realizadas en sus componentes de React. 3. Experimente con la personalización del color de la barra de la aplicación. Abre el archivo `ui/src/components/theme/theme.tsx` y busque la sección que define el tema de la barra de la aplicación. En la sección `colorSchemes.light.palette.primary` , actualice el valor principal de `colors.lagoon` a `colors.carrot` . Tras realizar este cambio, guarde el archivo y observe la actualización en su navegador. 4. Experimente modificando el texto y los componentes y añadiendo nuevas páginas.	

Trabajando con Green Boost

Tarea	Descripción	Habilidades requeridas
Configure monorepo y el administrador de paquetes pnpm.	1. Revise `pnpm-workspace.yaml` en la raíz de su repositorio de GB y observe cómo se definen los espacios de trabajo. Para obtener más información sobre espacios de trabajo, consulte la documentación de pnpm. 2. Revise `ui/package.json` y observe cómo hace referencia al espacio de trabajo `core/` con el nombre de paquete `"<appId>/core": "workspace:^",` . 3. Observe cómo se TypeScript centraliza la configuración de ESLint en los paquetes de utilidades definidos en él. `packages/` Esta configuración es utilizada luego por paquetes de aplicaciones como `core/`, `infra/` y `ui/`. Esto resulta útil cuando la aplicación se escala y se definen más paquetes de aplicaciones, que pueden hacer referencia a los paquetes de utilidades	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	sin duplicar el código de configuración.	
Ejecute scripts pnpm.	Ejecute los siguientes comandos en la raíz de su repositorio: 1. Ejecute `pnpm lint`. Este comando ejecuta un análisis de código estático con ESLint. 2. Ejecute `pnpm typecheck`. Este comando ejecuta el TypeScript compilador para comprobar los tipos de código. 3. Ejecute `pnpm test`. Este comando ejecuta Vitest para ejecutar pruebas unitarias. Observe cómo se ejecutan estos comandos en todos los espacios de trabajo. Los comandos se definen en el campo `package.json#scripts` de cada espacio de trabajo.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Utilice ESLint para el análisis de código estático.	Para probar la capacidad de análisis de código estático de ESLint, haga lo siguiente: 1. Primero, asegúrese de que la extensión ESLint de VS Code (ID: `dbaeumer.vscode-eslint`) esté instalada. También recomendamos instalar VS Code Error Lens (ID: `usernamehw.errorlens`) para ver los errores en línea. 2. Incluya en el código una línea de código que utilice la función `eval()` como se muestra en el siguiente ejemplo. `const userInput = "import("fs").then((fs) => console.log(fs.readFileSync("/etc/passwd", { encoding: "utf8" })))"; eval(userInput);` Importante: esto es solo con fines de prueba. Usar `eval()` se considera potencialmente peligroso y debe evitarse debido a los riesgos de seguridad.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	3. Después de incluir la línea `eval()`, abra su editor de código para confirmar que ESLint indicó el olor del código con garabatos rojos. 4. Revise los complemen tos y la configuración de ESLint en `packages/eslint-config-{node,next}/.eslintrc.cjs` .	
Gestione las dependencias y vulnerabilidades.	1. Para identificar cualquier vulnerabilidad y exposició n común (CVE), ejecute `pnpm audit` en la raíz de su repositorio. Debería ver No se ha encontrado ninguna vulnerabilidad conocida. 2. Instale un paquete intencion almente vulnerable en `core/` al ejecutar `pnpm add minimist@0.2.3` y, a continuación, ejecute `pnpm audit`. Observe cómo se informa de la vulnerabilidad. 3. Desinstale el paquete vulnerable que contiene `core/` `pnpm remove minimist` al ejecutar .	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Precomete los enlaces con Husky.	1. Realiza un par de pequeños cambios en TypeScript los archivos del repositorio. Los cambios pueden ser tan básicos como añadir comentarios. 2. Organice y confirme estos cambios utilizando `git add -A` y, a continuación, `git commit -m "test husky"`. El activador del enlace Husky previo a la confirmación, que se define en `.husky/pre-commit` , ejecuta el comando `pnpm lint-staged` . 3. Observe cómo lint-staged ejecuta los comandos especificados en los archivos `*/.lintstagedrc.js` de todo el repositorio en archivos que Git ha preparado. Estas herramientas son mecanismos que ayudan a evitar que el código incorrecto llegue a su aplicación.	Desarrollador de aplicaciones

Derribe la infraestructura

Tarea	Descripción	Habilidades requeridas
Elimine la implementación de su cuenta.	1. Para destruir la infraestructura que aprovisionó en la primera epopeya, ejecute `pnpm destroy:local` en `infra/`. 2. Espere 15 minutos después de que `pnpm destroy:local` haya finalizado y, a continuación, elimine la función de Lambda @Edge retenida buscando el identificador de su aplicación en la consola de Lambda. Las funciones Lambda @Edge se replican, lo que dificulta su eliminación. Para obtener más información sobre la eliminación de funciones de Lambda @Edge, consulte la CloudFront documentación.	Desarrollador de aplicaciones

Solución de problemas

Problema	Solución
No se pudo establecer el reenvío de puertos	Asegúrese de que sus credenciales de AWS estén configuradas correctamente y tengan los permisos necesarios.

Problema	Solución
	Compruebe que las variables de entorno del identificador de host bastión (`DB_BASTIO N_ID `) y del punto de conexión de la base de datos (`DB_ENDPOINT `) estén configuradas correctamente. Si sigue teniendo problemas, consulte la documentación de AWS para solucionar problemas de conexiones SSH y Administrador de sesiones.
Sitio web no está cargando en `localhost :3000`	Confirme que la salida del terminal indica que el reenvío de puertos se ha realizado correctam ente, incluida la dirección de reenvío. Asegúrese de que no haya procesos conflicti vos al utilizar el puerto 3000 de su máquina en las instalaciones. Compruebe que la aplicación Green Boost esté correctamente configurada y ejecutándose en el puerto esperado (3000). Compruebe en su navegador web si hay extensiones o ajustes de seguridad que puedan bloquear las conexiones en las instalacioneses.
Mensajes de error durante la implementación local (`pnpm deploy:local `)	Revise los mensajes de error detenidamente para identificar la causa del problema. Compruebe que las variables de entorno y los archivos de configuración necesarios estén configurados correctamente.

Recursos relacionados

- Documentación de AWS SDK
- Documentación de Green Boost
- Documentación de Next.js
- Documentación de Node.js
- Documentación de React
- TypeScript documentación

Ejecute pruebas unitarias para una aplicación GitHub de Node.js desde AWS CodeBuild

Creado por Thomas Scott (AWS) y Jean-Baptiste Guillois (AWS)

Repositorio de código: ejemplo de pruebas de Node JS	Entorno: producción	Tecnologías: desarrollo y pruebas de software
Servicios de AWS: AWS CodeBuild		

Resumen

Este patrón proporciona un ejemplo de código fuente y componentes clave de pruebas unitarias para una API de juegos de Node.js. También incluye instrucciones para ejecutar estas pruebas unitarias desde un GitHub repositorio mediante AWS CodeBuild, como parte de su flujo de trabajo de integración y entrega continuas (CI/CD).

Las pruebas unitarias son un proceso de desarrollo de software en el que diferentes partes de una aplicación, llamadas unidades, se prueban de forma individual e independiente para comprobar su correcto funcionamiento. Las pruebas validan la calidad del código y confirman que funciona según lo esperado. Otros desarrolladores también pueden familiarizarse fácilmente con su base de código consultando las pruebas. Las pruebas unitarias reducen el tiempo de refactorización en el futuro, ayudan a los ingenieros a ponerse al día con su base de código con mayor rapidez y proporcionan confianza en el comportamiento esperado.

Las pruebas unitarias implican probar funciones individuales, incluidas las funciones de AWS Lambda. Para crear pruebas unitarias, necesita un marco de pruebas y una forma de validar las pruebas (aserciones). Los ejemplos de código de este patrón utilizan el marco de pruebas Mocha y la biblioteca de aserciones Chai.

Para obtener más información sobre las pruebas unitarias y ejemplos de componentes de las pruebas, consulte la sección de Información adicional.

Requisitos previos y limitaciones

- Una cuenta de AWS activa con CodeBuild los permisos correctos
- Una GitHub cuenta (consulte las instrucciones para registrarse)
- Git (consulte las instrucciones de instalación)
- Un editor de código para realizar cambios e insertar el código GitHub (por ejemplo, puede usar AWS Cloud9)

Arquitectura

Este patrón implementa la arquitectura que se muestra en el siguiente diagrama.

Herramientas

Herramientas

- Git es un sistema de control de versiones que puede utilizar para el desarrollo de código.
- AWS Cloud9 es un entorno de desarrollo integrado (IDE) que ofrece una completa experiencia de edición de código, con soporte para varios lenguajes de programación y depuradores de tiempo de ejecución, además de un terminal integrado. Contiene una colección de herramientas que se utilizan para codificar, compilar, ejecutar, probar y depurar software, y le ayuda a lanzar software en la nube. Es posible acceder al IDE de AWS Cloud9 a través de un navegador web.
- AWS CodeBuild – AWS CodeBuild es un servicio de integración continua totalmente gestionado que compila el código fuente, ejecuta pruebas y produce paquetes de software listos para su implementación. Con CodeBuild esto, no necesita aprovisionar, administrar ni escalar sus propios servidores de compilación. CodeBuild escala de forma continua y procesa varias compilaciones de forma simultánea, para que sus compilaciones no se queden esperando en una cola. Puede comenzar con rapidez usando entornos de compilación preempaquetados, o crear sus propios entornos de compilación personalizados que utilicen sus propias herramientas de compilación. Con CodeBuild, se le cobra por minuto por los recursos de cómputo que utilice.

Código

El código fuente de este patrón está disponible en el GitHub repositorio de aplicaciones de prueba de unidades de juego de muestra. Puedes crear tu propio GitHub repositorio a partir de esta muestra

(opción 1) o utilizar el repositorio de muestras directamente (opción 2) para este patrón. Siga las instrucciones para cada opción que se indican en la siguiente sección. La opción que siga dependerá de su caso de uso.

Epics

Opción 1: Ejecute pruebas unitarias en su GitHub repositorio personal con CodeBuild

Tarea	Descripción	Habilidades requeridas
Cree su propio GitHub repositorio a partir del proyecto de muestra.	1. Inicie sesión en GitHub. 2. Crear un nuevo repositor io. Para obtener instrucci ones, consulte la GitHub documentación. 3. Clone e inserte el repositor io de muestras en el nuevo repositorio de su cuenta.	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps
Cree un CodeBuild proyecto nuevo.	1. Inicie sesión en la consola de administración de AWS y abra la CodeBuild consola en https://console.a ws.amazon.com/codesuite/ codebuild/home. 2. Elija Crear el proyecto de compilación. 3. En la sección Configuración del proyecto, en Nombre del proyecto, escriba aws-tests-sample-node-js. 4. En la sección Fuente, en Proveedor de fuentes, elija GitHub. 5. En Repositorio, seleccion a Repositorio en mi GitHub	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	cuenta y, a continuación, pega la URL en el GitHub repositorio recién creado. 6. En la sección Primary source webhook events (Eventos de webhooks de origen principales), seleccione Rebuild every time a code change is pushed to this repository. (Volver a compilar cada vez que se inserte un cambio de código en este repositor io). 7. Para el tipo de evento, elija PUSH. 8. En la sección Environme nt (Entorno), elija Managed image (Imagen gestionad a), Amazon Linux 2 y la imagen más reciente. 9. Utilice los valores predeterminados para el resto de opciones y, a continuación, elija Create build project (Crear proyecto de compilación).	
Comience la compilación.	En la página Review (Revisar) , elija Start build (Comenzar compilación) para ejecutar la compilación.	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps

Opción 2: Ejecute pruebas unitarias en un repositorio público con CodeBuild

Tarea	Descripción	Habilidades requeridas
Crea un nuevo proyecto de CodeBuild compilación.	1. Inicie sesión en la consola de administración de AWS y abra la CodeBuild consola en https://console.aws.amazon.com/codesuite/codebuild/home. 2. Elija Crear el proyecto de compilación. 3. En la sección Configuración del proyecto, en Nombre del proyecto, escriba aws-tests-sample-node-js. 4. En la sección Fuente, en Proveedor de fuentes, elija GitHub. 5. En Repositorio, seleccion a Repositorio público y, a continuación, pega la URL: https://github.com/aws-samples/ node-js-tests-sample. 6. En la sección Environme nt (Entorno), elija Managed image (Imagen gestionad a), Amazon Linux 2 y la imagen más reciente. 7. Utilice los valores predeterminados para el resto de opciones y, a continuación, elija	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	Create build project (Crear proyecto de compilación).	
Comience la compilación.	En la página Review (Revisar) , elija Start build (Comenzar compilación) para ejecutar la compilación.	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps

Analice las pruebas unitarias

Tarea	Descripción	Habilidades requeridas
Ver resultados de la prueba.	En la CodeBuild consola, revise los resultados de las pruebas unitarias del CodeBuild trabajo. Deben coincidir con los resultados que se muestran en la sección de Additional information (Información adicional). Estos resultados validan la integración del GitHub repositorio con CodeBuild.	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps
Aplique un webhook.	Ahora puede aplicar un webhook para iniciar automáticamente una compilación cada vez que introduzca cambios de código en la rama principal de su repositorio. Para obtener instrucciones, consulte la CodeBuild documentación.	Desarrollador de aplicaciones, administrador de AWS, AWS DevOps

Recursos relacionados

- Ejemplo de aplicación de prueba de unidades de juego (GitHub repositorio con código de muestra)
- CodeBuild Documentación de AWS
- GitHub eventos de webhook (CodeBuild documentación)
- Crear un repositorio nuevo (GitHub documentación)

Información adicional

Ver resultados de la prueba unitaria

En la CodeBuild consola, debería ver los siguientes resultados de las pruebas una vez que el proyecto se haya creado correctamente.

Ejemplo de componentes de una prueba unitaria

Esta sección describe los cuatro tipos de componentes de prueba que se utilizan en las pruebas unitarias: aserciones, espías, stubs y mocks. Incluye una breve explicación y un ejemplo de código de cada componente.

Aserciones

Se utiliza una aserción para verificar un resultado esperado. Este es un componente de prueba importante porque valida la respuesta esperada de una función determinada. El siguiente ejemplo de aserción valida que el identificador devuelto esté entre 0 y 1000 al inicializar un juego nuevo.

```
const { expect }  = require('chai');
const { Game } = require('../src/index');

describe('Game Function Group', () => {
 it('Check that the Game ID is between 0 and 1000', function() {
      const game = new Game();
      expect(game.id).is.above(0).but.below(1000)
 });
});
```

Espías

Un espía se utiliza para observar lo que sucede cuando se ejecuta una función. Por ejemplo, es posible que quiera comprobar que se ha llamado a la función correctamente. El siguiente ejemplo muestra que los métodos de inicio y parada se llaman en un objeto de la clase Juego.

```
const { expect }  = require('chai');
const { spy } = require('sinon');

const { Game } = require('../src/index');

describe('Game Function Group', () => {
   it('should verify that the correct function is called', () => {
      const spyStart = spy(Game.prototype, "start");
      const spyStop = spy(Game.prototype, "stop");

      const game = new Game();
      game.start();
      game.stop();

      expect(spyStart.called).to.be.true
      expect(spyStop.called).to.be.true
    });
});
```

Stubs

Un stub se utiliza para anular la respuesta predeterminada de una función. Esto resulta especialmente útil cuando la función realiza una solicitud externa, ya que se quiere evitar realizar solicitudes externas a partir de pruebas unitarias. (Las solicitudes externas son más adecuadas para las pruebas de integración, que pueden probar físicamente las solicitudes entre diferentes componentes). En el siguiente ejemplo, un stub fuerza un ID de retorno de la función getId.

```
const { expect }  = require('chai');
const {.stub } = require('sinon');

const { Game } = require('../src/index');

describe('Game Function Group', () =>  {
   it('Check that the Game ID is between 0 and 1000', function() {
      let generateIdStub = stub(Game.prototype, 'getId').returns(999999);

      const game = new Game();
```

```
      expect(game.getId).is.equal(999999);

      generateIdStub.restore();
    });
});
```

Mocks

Un mock es un método falso que tiene un comportamiento preprogramado para probar diferentes escenarios. Un mock puede considerarse una forma extendida de un stub y puede llevar a cabo múltiples tareas simultáneamente. En el siguiente ejemplo, se utiliza un mock para validar tres escenarios:

- Se llama a la función
- La función se llama con argumentos
- La función devuelve el entero 9

```
const { expect }  = require('chai');
const {.mock } = require('sinon');

const { Game } = require('../src/index');

describe('Game Function Group', () =>  {
   it('Check that the Game ID is between 0 and 1000', function() {
      let mock = mock(Game.prototype).expects('getId').withArgs().returns(9);

      const game = new Game();
      const id = get.getId();

      mock.verify();
      expect(id).is.equal(9);
    });
});
```

Estructure un proyecto de Python en una arquitectura hexagonal con AWS Lambda

Creado por Furkan Oruc (AWS), Dominik Goby (AWS), Darius Kunce (AWS) y Michal Ploski (AWS)

Entorno: PoC o piloto	Tecnologías: desarrollo y pruebas de software; nativo en la nube; contenedores y microservicios; sin servidor; modernización	Servicios de AWS: Amazon DynamoDB; AWS Lambda; Amazon API Gateway

Resumen

Este patrón muestra cómo estructurar un proyecto de Python en una arquitectura hexagonal mediante AWS Lambda. El patrón utiliza el AWS Cloud Development Kit (AWS CDK) como herramienta de infraestructura como código (IaC), Amazon API Gateway como REST API y Amazon DynamoDB como capa de persistencia. La arquitectura hexagonal sigue los principios de diseño basados en el dominio. En la arquitectura hexagonal, el software consta de tres componentes: dominio, puertos y adaptadores. Para obtener información detallada sobre las arquitecturas hexagonales y sus ventajas, consulte la guía Creación de arquitecturas hexagonales en AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Experiencia en Python
- Familiaridad con AWS Lambda, AWS CDK, Amazon API Gateway y DynamoDB
- Una GitHub cuenta (consulte las instrucciones para registrarse)
- Git (consulte las instrucciones de instalación)
- Un editor de código para realizar cambios y enviar el código a GitHub (por ejemplo, AWS Cloud9, Visual Studio Code o) JetBrains PyCharm
- Docker instalado y el daemon de Docker en funcionamiento

Versiones de producto

- Git versión 2.24.3 o posterior
- Python versión 3.7 o posterior
- AWS CDK v2
- Poetry versión 1.1.13 o posterior
- AWS Lambda Powertools para Python, versión 1.25.6 o posterior
- pytest versión 7.1.1 o posterior
- Moto versión 3.1.9 o posterior
- versión 1.9.0 o posterior de pydantic
- Boto3 versión 1.22.4 o posterior
- mypy-boto3-dynamodb versión 1.24.0 o posterior

Arquitectura

Pila de tecnología de destino

La pila de tecnología de destino consiste en un servicio de Python que utiliza API Gateway, Lambda y DynamoDB. El servicio utiliza un adaptador de DynamoDB para conservar los datos. Proporciona una función que utiliza Lambda como punto de entrada. El servicio usa Amazon API Gateway para exponer una REST API. La API utiliza AWS Identity and Access Management (IAM) para la autenticación de clientes.

Arquitectura de destino

Para ilustrar la implementación, este patrón despliega una arquitectura de destino sin servidor. Los clientes pueden enviar solicitudes a un punto de conexión final de API Gateway. API Gateway reenvía la solicitud a la función de Lambda de destino que implementa el patrón de arquitectura hexagonal. La función de Lambda realiza operaciones de creación, lectura, actualización y eliminación (CRUD) en una tabla de DynamoDB.

> Importante: este patrón se probó en un entorno PoC. Debe realizar una revisión de seguridad para identificar el modelo de amenaza y crear una base de código segura antes de implementar cualquier arquitectura en un entorno de producción.

La API admite cinco operaciones en una entidad de producto:

- `GET /products` devuelve todos los productos.
- `POST /products` crea un nuevo producto.
- `GET /products/{id}` devuelve un producto específico.
- `PUT /products/{id}` actualiza un producto específico.
- `DELETE /products/{id}` elimina un producto específico.

Puede utilizar la siguiente estructura de carpetas para organizar el proyecto de forma que siga el patrón de arquitectura hexagonal:

```
app/  # application code
|--- adapters/  # implementation of the ports defined in the domain
     |--- tests/  # adapter unit tests
|--- entrypoints/  # primary adapters, entry points
     |--- api/  # api entry point
          |--- model/  # api model
          |--- tests/  # end to end api tests
|--- domain/  # domain to implement business logic using hexagonal architecture
     |--- command_handlers/  # handlers used to execute commands on the domain
     |--- commands/  # commands on the domain
     |--- events/  # events triggered via the domain
     |--- exceptions/  # exceptions defined on the domain
     |--- model/  # domain model
     |--- ports/  # abstractions used for external communication
     |--- tests/  # domain tests
|--- libraries/  # List of 3rd party libraries used by the Lambda function
infra/  # infrastructure code
simple-crud-app.py  # AWS CDK v2 app
```

Herramientas

Servicios de AWS

- Amazon API Gateway es un servicio completamente administrado que facilita a los desarrolladores la publicación, el mantenimiento, la supervisión y la protección de las API a cualquier escala.

- Amazon DynamoDB es una base de datos NoSQL de valor clave, sin servidor y totalmente gestionada que está diseñada para ejecutar aplicaciones de alto rendimiento a cualquier escala.
- AWS Lambda es un servicio de computación controlado por eventos sin servidor que permite ejecutar código para prácticamente cualquier tipo de aplicación o servicio backend, sin aprovisionar ni administrar servidores. Puede lanzar funciones de Lambda desde más de 200 aplicaciones de software como servicio (SaaS) y pagar solo por lo que utilice.

Herramientas

- Git se utiliza como sistema de control de versiones para el desarrollo de código en este patrón.
- Python se utiliza como lenguaje de programación para este patrón. Python proporciona estructuras de datos de alto nivel y un enfoque de la programación orientada a objetos. AWS Lambda proporciona un tiempo de ejecución de Python integrado que simplifica el funcionamiento de los servicios de Python.
- Visual Studio Code se utiliza como IDE para desarrollar y probar este patrón. Puede usar cualquier IDE que sea compatible con el desarrollo de Python (por ejemplo, AWS Cloud9 o PyCharm).
- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software de código abierto que le permite definir los recursos de su aplicación en la nube utilizando lenguajes de programación conocidos. Este patrón utiliza la CDK para escribir e implementar la infraestructura de la nube como código.
- Poetry se utiliza para gestionar las dependencias del patrón.
- AWS CDK utiliza Docker para crear el paquete y la capa Lambda.

Código

El código de este patrón está disponible en el repositorio de ejemplos de arquitectura hexagonal GitHub Lambda.

Prácticas recomendadas

Para usar este patrón en un entorno de producción, siga estas prácticas recomendadas:

- Utilice las claves administradas por el cliente en AWS Key Management Service (AWS KMS) para cifrar los grupos de CloudWatch registros de Amazon y las tablas de Amazon DynamoDB.
- Configure AWS WAF para Amazon API Gateway para permitir el acceso únicamente desde la red de su organización.

- Considere otras opciones para la autorización de API Gateway si IAM no satisface sus necesidades. Por ejemplo, puede usar grupos de usuarios de Amazon Cognito o autorizadores de Lambda de API Gateway.
- Utilice Copias de seguridad de DynamoDB.
- Configure las funciones de Lambda con una implementación de nube privada virtual (VPC) para mantener el tráfico de red dentro de la nube.
- Actualice la configuración de origen permitida para la verificación previa del intercambio de recursos entre orígenes (CORS) para restringir el acceso únicamente al dominio de origen solicitante.
- Utilice cdk-nag para comprobar las prácticas recomendadas de seguridad en el código de AWS CDK.
- Considere la posibilidad de utilizar herramientas de escaneo de código para detectar problemas de seguridad comunes en el código. Por ejemplo, Bandit es una herramienta diseñada para detectar problemas de seguridad comunes en el código Python. PIP-audit escanea los entornos de Python en busca de paquetes que tengan vulnerabilidades conocidas.

Este patrón utiliza AWS X-Ray para rastrear las solicitudes a través del punto de entrada, el dominio y los adaptadores de la aplicación. AWS X-Ray ayuda a los desarrolladores a identificar los cuellos de botella y determinar las latencias altas para mejorar el rendimiento de las aplicaciones.

Epics

Inicializar el proyecto

Tarea	Descripción	Habilidades requeridas
Cree su propio repositorio.	1. Inicie sesión en. GitHub 2. Crear un nuevo repositorio. Para obtener instrucciones, consulte la GitHub documentación. 3. Clone e inserte el repositorio de muestras de este patrón en el nuevo repositorio de su cuenta.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Instale las dependencias.	1. Instale Poetry. `pip install poetry` 2. Instale los paquetes desde el directorio raíz. El siguiente comando instala la aplicación y los paquetes de AWS CDK. También instala los paquetes de desarrollo necesarios para ejecutar las pruebas unitarias. Todos los paquetes instalados se colocan en un nuevo entorno virtual. `poetry install` 3. Para ver una represent ación gráfica de los paquetes instalados, ejecute el siguiente comando. `poetry show --tree` 4. Actualice todas las dependencias. `poetry update` 5. Abra un nuevo intérpret e de comandos en el entorno virtual recién	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	creado. Contiene todas las dependencias instaladas. `poetry shell`	

Tarea	Descripción	Habilidades requeridas
Configure su IDE.	Recomendamos Visual Studio Code, pero puede usar cualquier IDE de su elección que sea compatibl e con Python. Los siguientes pasos son para Visual Studio Code. 1. Actualizar el archivo `.vscode/settings` `{ "python.testing.pytestArgs": [ "app/adapters/tests", "app/entrypoints/api/tests", "app/domain/tests" ], "python.testing.unittestEnabled": false, "python.testing.pytestEnabled": true, "python.envFile": "${workspaceFolder}/.env", }` 2. Cree un archivo `.env` en el directorio raíz del proyecto. Esto garantiza que el directorio raíz del proyecto esté incluido en el directori o `PYTHONPATH` para que	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`pytest` pueda encontrarlo y descubrir correctamente todos los paquetes. `PYTHONPATH=.`	
Ejecute pruebas unitarias, opción 1: utilice Visual Studio Code.	1. Elija el intérprete de Python del entorno virtual gestionado por Poetry. 2. Ejecute las pruebas desde Test Explorer.	Desarrollador de aplicaciones
Ejecute pruebas unitarias, opción 2: utilice comandos del intérprete de comandos.	1. Inicie un nuevo intérprete de comandos en el entorno virtual. `poetry shell` 2. Ejecute el comando `pytest` desde el directorio raíz. `python -m pytest` Otra posibilidad es ejecutar el comando directamente desde Poetry. `poetry run python -m pytest`	Desarrollador de aplicaciones

Implementar y probar la aplicación

Tarea	Descripción	Habilidades requeridas
Solicitar credenciales temporales.	Para tener credenciales de AWS en el intérprete de comandos cuando ejecute `cdk deploy`, cree credencia les temporales mediante AWS IAM Identity Center (sucesor de AWS Single Sign-On). Para obtener instrucciones, consulte la entrada del blog How to retrieve short-term credentials for CLI use with AWS IAM Identity Center.	Desarrollador de aplicaciones, AWS DevOps
Implemente la aplicación .	1. Instale la v2 de AWS CDK. `npm install -g aws-cdk` Para obtener más informaci ón, consulte la documenta ción de AWS CDK. 2. Arranque la AWS CDK en su cuenta y región. `cdk bootstrap aws://12345678900/ us-east-1 --profile aws-profile-name` 3. Implemente la aplicación como una CloudFormation pila de AWS mediante un perfil de AWS.	Desarrollador de aplicaciones, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`cdk deploy --profile aws-profile-name`	
Pruebe la API, opción 1: utilice la consola.	Utilice la consola de API Gateway para probar la API. Para obtener más información sobre las operaciones de la API y los mensajes de solicitud/respuesta, consulte la sección de uso de la API del archivo readme del repositorio. GitHub	Desarrollador de aplicaciones, AWS DevOps

Tarea	Descripción	Habilidades requeridas
Pruebe la API, opción 2: utilice Postman.	Si quiere utilizar una herramienta como Postman: 1. Instale Postman como una aplicación independiente o una extensión del navegador. 2. Copie la URL del punto de conexión de la API Gateway. Deberá tener el siguiente formato: `https://{api-id}.execute-api.{region}.amazonaws.com/{stage}/{path}` 3. Configure la firma de AWS en la pestaña de autorización. Para obtener instrucciones, consulte el artículo de AWS Re:post sobre activación de la autenticación de IAM para las REST API de API Gateway. 4. Utilice Postman para enviar solicitudes al punto de conexión de la API.	Desarrollador de aplicaciones, AWS DevOps

Desarrolle el servicio

Tarea	Descripción	Habilidades requeridas
Redacte pruebas unitarias para el dominio empresarial.	1. Cree un archivo de Python en la carpeta `app/domai`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	n/tests con el prefijo del nombre de archivo test_. 2. Cree un nuevo método de prueba para probar la nueva lógica empresari al mediante el siguiente ejemplo. `def test_crea te_product_should_ store_in_repositor y(): # Arrange command = create_product_com mand.CreateProduct Command(name="Test Product", descripti on="Test Descripti on",) # Act create_pr oduct_command_hand ler.handle_create_ product_command(command=c ommand, unit_of_w ork=mock_unit_of_w ork) # Assert` 3. Cree una clase de comando en la carpeta app/domai n/commands .	

Tarea	Descripción	Habilidades requeridas
	4. Si la funcionalidad es nueva, cree un código auxiliar para el controlador de comandos de la carpeta `app/domain/command_handlers` . 5. Ejecute la prueba unitaria para comprobar si falla, ya que todavía no existe una lógica empresarial. `python -m pytest`	

Tarea	Descripción	Habilidades requeridas
Implemente comandos y controladores de comandos.	1. Implemente la lógica empresarial en el archivo de controlador de comandos recién creado. 2. Para cada dependencia que interactúe con sistemas externos, declare una clase abstracta en la carpeta `app/domain/ports` . `class ProductsRepository(ABC):` `  @abstractmethod` `  def add(self, product: product.Product) -> None:` `  ...` `class UnitOfWork(ABC):` `  products: ProductsRepository` `  @abstractmethod` `  def commit(self) -> None:` `  ...` `  @abstractmethod` `  def __enter__(self) -> typing.Any:` `  ...` `  @abstractmethod` `  def __exit__(self, *args) -> None:` `  ...`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	3. Actualice la firma del controlador de comandos para aceptar las dependencias recién declaradas utilizando la clase de puerto abstracta como anotación de tipo. `def handle_create_product_command(` `  command: create_product_command.CreateProductCommand,` `  unit_of_work: unit_of_work.UnitOfWork,` `) -> str:` `  ...` 4. Actualice la prueba unitaria para simular el comportamiento de todas las dependencias declaradas para el controlador de comandos. `  # Arrange` `  mock_unit_of_work = unittest.mock.create_autospec(` `  spec=unit_of_work.UnitOfWork, instance=True` `  )` `  mock_unit_of_work.products = unittest.mock.create_autospec(`	

Tarea	Descripción	Habilidades requeridas
	<pre>spec=unit _of_work.ProductsR epository, instance= True)</pre> 5. Actualice la lógica de aserción en la prueba para comprobar las invocaciones de dependencia esperadas. <pre># Assert mock_unit _of_work.commit.as sert_called_once() product = mock_unit_of_work. products.add.call_ args.args[0] assertpy. assert_that(produc t.name).is_equal_t o("Test Product") assertpy. assert_that(produc t.description).is_ equal_to("Test Description")</pre> 6. Ejecute la prueba unitaria para comprobar que funciona correctamente. <pre>python -m pytest</pre>	

Tarea	Descripción	Habilidades requeridas
Escriba pruebas de integración para los adaptadores secundarios.	1. Cree un archivo de prueba en la carpeta `app/adapters/tests` utilizando `test_` como prefijo de nombre de archivo. 2. Utilice la biblioteca Moto para simular los servicios de AWS. 3. Cree un nuevo método de prueba para una prueba de integración del adaptador.	Desarrollador de aplicaciones

```
@pytest.fixture
def mock_dynamodb():
   with moto.mock
_dynamodb():
    yield boto3.res
ource("dynamodb",
 region_name="eu-ce
ntral-1")
```

```
def test_add_
and_commit_should_
store_product(mock
_dynamodb):
    # Arrange
    unit_of_work =
 dynamodb_unit_of_w
ork.DynamoDBUnitOf
Work(
        table_nam
e=TEST_TABLE_NAME,
 dynamodb_client=mo
ck_dynamodb.meta.c
lient
    )
    current_time =
 datetime.datetime.
```

Tarea	Descripción	Habilidades requeridas
	<pre>now(datetime.timezone.utc).isoformat() new_product_id = str(uuid.uuid4()) new_product = product.Product(id=new_product_id, name="test-name", description="test-description", createDate=current_time, lastUpdateDate=current_time,) # Act with unit_of_work: unit_of_work.products.add(new_product) unit_of_work.commit() # Assert</pre> 4. Cree una clase de adaptador en la carpeta `app/adapters` . Utilice la clase abstracta de la carpeta de puertos como clase base.	

Tarea	Descripción	Habilidades requeridas
	5. Ejecute la prueba unitaria para ver si falla, porque todavía no hay lógica. `python -m pytest`	

Tarea	Descripción	Habilidades requeridas
Implemente adaptadores secundarios.	1. Implemente la lógica en el archivo de adaptador recién creado. 2. Actualice las afirmaciones de las pruebas. `# Assert` `    with unit_of_work_readonly:` `        product_from_db = unit_of_work_readonly.products.get(new_product_id)` `    assertpy.assert_that(product_from_db).is_not_none()` `    assertpy.assert_that(product_from_db.dict()).is_equal_to(` `        {` `            "id": new_product_id,` `            "name": "test-name",` `            "description": "test-description",` `            "createDate": current_time,` `            "lastUpdateDate": current_time,` `        }` `    )`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	3. Ejecute la prueba unitaria para comprobar que funciona correctamente. `python -m pytest`	

Tarea	Descripción	Habilidades requeridas
end-to-end Redacte pruebas.	1. Cree un archivo de prueba en la carpeta `app/entry points/api/tests` utilizando `test_` como prefijo de nombre de archivo. 2. Cree un elemento de contexto de Lambda que la prueba utilizará para llamar a Lambda. `@pytest.fixture def lambda_co ntext(): @dataclass class LambdaCon text: function_ name: str = "test" memory_li mit_in_mb: int = 128 invoked_f unction_arn: str = "arn:aws:lambda:eu -west-1:809313241: function:test" aws_reque st_id: str = "52fdfc07-2182-154 f-163f-5f0f9a621d7 2" return LambdaCon text()` 3. Cree un método de prueba para la invocación de la API.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`def test_crea te_product(lambda_ context):` `    # Arrange` `    name = "TestName"` `    description =  "Test description"` `    request =  api_model.CreatePr oductRequest(name= name, descripti on=description)` `    minimal_event =  api_gateway_proxy_ event.APIGatewayPr oxyEvent(` `        {` `            "path": "/ products",` `            "httpMeth od": "POST",` `            "requestC ontext": {  #  correlation ID` `  "requestId":  "c6af9ac6-7b61-11e 6-9a41-93e8deadbee f"` `            },` `            "body":  json.dumps(request .dict()),` `        }` `    )` `    create_pr oduct_func_mock =  unittest.mock.crea te_autospec(`	

Tarea	Descripción	Habilidades requeridas
	<pre>spec=crea te_product_command _handler.handle_cr eate_product_comma nd) handler.c reate_product_comm and_handler.handle _create_product_co mmand = (create_pr oduct_func_mock) # Act handler.h andler(minimal_eve nt, lambda_context)</pre> 4. Ejecute la prueba unitaria para ver si falla, porque todavía no hay lógica. <pre>python -m pytest</pre>	

Tarea	Descripción	Habilidades requeridas
Implemente los adaptadores principales.	1. Cree una función para la lógica empresarial de la API y declare como un recurso de la API. `@tracer.capture_method` `@app.post("/products")` `@utils.parse_event(model=api_model.CreateProductRequest, app_context=app)` `def create_product(` `request: api_model.CreateProductRequest,` `) -> api_model.CreateProductResponse:` `"""Creates a product."""` `...` Nota: todos los decoradores que ve son características de la biblioteca AWS Lambda Powertools para Python. Para obtener más información, consulte el sitio web de AWS Lambda Powertools para Python. 2. Implemente la lógica de la API. `id=create_product_command_handler.ha`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	ndle_create_produc t_command(command=c reate_product_comm and.CreateProductC ommand(name=requ est.name, descripti on=request.descrip tion,), unit_of_w ork=unit_of_work,) response = api_model.CreatePr oductResponse(id=i d) return response. dict() 3. Ejecute la prueba unitaria para comprobar que funciona correctamente. python -m pytest	

Recursos relacionados

Guía de APG

- Creación de arquitecturas hexagonales en AWS

Referencias de AWS

- Documentación de AWS Lambda
- Documentación de AWS SDK

  - Su primera aplicación de AWS CDK
- Documentación de API Gateway
  - Control del acceso a una API con permisos de IAM
  - Uso de la consola de API Gateway para probar un método de la API de REST
- Documentación de Amazon DynamoDB

Herramientas

- Sitio web git-scm.com
- Instalación de Git
- Crear un GitHub repositorio nuevo
- Sitio web de Python
- AWS Lambda Powertools para Python
- Sitio web de Postman
- Biblioteca de objetos simulados de Python
- Sitio web de Poetry

IDEs

- Sitio web de Visual Studio Code
- Documentación de AWS Cloud9
- PyCharm sitio web

Más patrones

- Automatice la implementación de conjuntos de pilas mediante AWS CodePipeline y AWS CodeBuild
- Adjunte automáticamente una política administrada de AWS para Systems Manager a los perfiles de instancia de EC2 mediante Cloud Custodian y AWS CDK
- Cree una canalización de procesamiento de vídeo con Amazon Kinesis Video Streams y AWS Fargate
- Encadene los servicios de AWS mediante un enfoque sin servidor
- Convierta el tipo de datos VARCHAR2 (1) para Oracle en un tipo de datos booleano para Amazon Aurora PostgreSQL
- Implementar una aplicación agrupada en Amazon ECS con AWS Copilot
- Despliega canarios de CloudWatch Synthetics con Terraform
- Implementar funciones de Lambda con imágenes de contenedor
- Genere una dirección IP saliente estática mediante una función de Lambda, Amazon VPC y una arquitectura sin servidor
- Genere datos de prueba con un trabajo de AWS Glue y Python
- Implementa una estrategia de ramificación de Gitflow para entornos de múltiples cuentas DevOps
- Implemente una estrategia GitHub de ramificación de Flow para entornos de cuentas múltiples DevOps
- Implemente una estrategia de ramificación troncal para entornos de cuentas múltiples DevOps
- Modernizar las aplicaciones de ASP.NET Web Forms en AWS
- Ejecute un contenedor de Docker de la API web de ASP.NET Core en una instancia Linux de Amazon EC2
- Ejecutar pruebas unitarias para trabajos ETL de Python en AWS Glue con el marco pytest
- Transfiera datos de Db2 z/OS a gran escala a Amazon S3 en archivos CSV
- Validar Account Factory para el código Terraform (AFT) localmente

Almacenamiento y copia de seguridad

Temas

- Permitir a las instancias de EC2 el acceso de escritura a los buckets de S3 en las cuentas de AMS
- Automatice la ingesta de flujos de datos en una base de datos de Snowflake mediante Snowflake Snowpipe, Amazon S3, Amazon SNS y Amazon Data Firehose
- Cifrar automáticamente los volúmenes de Amazon EBS nuevos y existentes
- Realice copias de seguridad de los servidores Sun SPARC en el emulador Stromasys Charon-SSP en la nube de AWS
- Realice copias de seguridad y archive datos en Amazon S3 con Veeam Backup & Replication
- Configurar Veritas NetBackup para VMware Cloud on AWS
- Copiar datos de un bucket de S3 a otra cuenta y región mediante la AWS CLI
- Copie datos de un bucket de S3 a otra cuenta y región mediante S3 Batch Replication
- Migre datos de un entorno Hadoop local a Amazon S3 con DistCp AWS PrivateLink para Amazon S3
- Uso CloudEndure para la recuperación ante desastres de una base de datos local
- Más patrones

Permitir a las instancias de EC2 el acceso de escritura a los buckets de S3 en las cuentas de AMS

Documento creado por Mansi Suratwala (AWS)

Entorno: producción	Tecnologías: almacenamiento y copia de seguridad; bases de datos; seguridad, identidad, cumplimiento; operaciones	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon S3; AWS Managed Services		

Resumen

AWS Managed Services (AMS) facilita poder operar la infraestructura de Amazon Web Services (AWS) de forma más eficiente y segura. Las cuentas de AMS tienen barreras de protección de la seguridad para la administración estandarizada de los recursos de AWS. Una barrera de protección es que los perfiles de instancia de Amazon Elastic Compute Cloud (Amazon EC2) predeterminados no permiten el acceso de escritura a los buckets de Amazon Simple Storage Service (Amazon S3). Sin embargo, es posible que su organización tenga varios buckets de S3 y requiera un mayor control sobre el acceso de las instancias de EC2. A modo de ejemplo, es posible que desee almacenar copias de seguridad de bases de datos de instancias de EC2 en un bucket de S3.

Este patrón explica cómo utilizar las solicitudes de cambio (RFC) para permitir que sus instancias de EC2 tengan acceso de escritura a los buckets de S3 de su cuenta de AMS. Una RFC es una solicitud creada por el interesado o por AMS para realizar un cambio en el entorno administrado y que incluye un identificador de tipo de cambio (CT) para una operación concreta.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AMS Advanced. Para obtener más información al respecto, consulte los planes de operaciones de AMS en la documentación de AWS Managed Services.

- Acceso al rol de customer-mc-user-role AWS Identity and Access Management (IAM) para enviar las RFC.
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada con las instancias de EC2 en la cuenta de AMS.
- Conocimiento de cómo crear y enviar las RFC en AMS. Para obtener más información al respecto, consulte What are AMS change types? (¿Qué son los tipos de cambio de AMS?) en la documentación de AWS Managed Services.
- Conocimiento de los tipos de cambios (CT) manuales y automatizados. Para obtener más información al respecto, consulte los Automated and manual CTs (Tipos de cambio automatizados y manuales) en la documentación de AWS Managed Services.

Arquitectura

Pila de tecnología

- AMS
- CLI de AWS
- Amazon EC2
- Amazon S3
- IAM

Herramientas

- La Interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que permite interactuar con los servicios de AWS mediante comandos en el intérprete de comandos de línea de comandos.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- AWS Managed Services (AMS) facilita poder operar la infraestructura de AWS de forma más eficiente y segura.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez.

Epics

Crear un bucket de S3 con una RFC

Tarea	Descripción	Habilidades requeridas
Cree un bucket de S3 mediante una RFC automatizada.	1. Inicie sesión en su cuenta de AMS, seleccione la página Choose change type (Seleccionar tipo de cambio) y, a continuación, RFC y Create RFC (Crear una RFC). 2. Envíe la RFC automatizada Create S3 Bucket. Nota: Asegúrese de registrar el nombre del bucket de S3.	Administrador de sistemas de AWS, desarrollador de AWS

Crear un perfil de instancia de IAM y asócielo a las instancias de EC2

Tarea	Descripción	Habilidades requeridas
Envíe una RFC manual para crear un rol de IAM.	Cuando se incorpora una cuenta de AMS, se crea un perfil de instancia de IAM predeterminado de customer-mc-ec 2 perfiles de instancia y se asocia a cada instancia de EC2 de su cuenta de AMS. Sin embargo, el perfil de	Administrador de sistemas de AWS, desarrollador de AWS

Tarea	Descripción	Habilidades requeridas
	instancia no tiene permisos de escritura en los buckets de S3. Para añadir los permisos de escritura, envíe la RFC manual Create IAM Resource para crear un rol de IAM que tenga las tres políticas siguientes: customer_ ec2_instance_, customer_ deny_policy y customer_ ec2_s3_integration_policy. Importante: Las políticas customer_ec2_instance_ y customer_deny_policy ya existen en la cuenta de AMS. Sin embargo, debe crear la política customer_ec2_s3_in tegration_policy mediante el ejemplo de política siguiente: `{ "Version": "2012-10-17", "Statement": [ { "Sid": "", "Effect": "Allow", "Principal": { "Service": "ec2.amazonaws.com" }, "Action": "sts:AssumeRole" } ]`	

Tarea	Descripción	Habilidades requeridas
	<pre>} Role Permissions: { "Version": "2012-10-17", "Statement": [{ "Action": ["s3:ListBucket", "s3:GetBucketLocat ion"], "Resource ": "arn:aws:s3:::", "Effect": "Allow" }, { "Action": ["s3:GetObject", "s3:PutObject", "s3:ListMultipartU ploadParts", "s3:AbortMultipart Upload"], "Resource ": "arn:aws:s3:::/*", "Effect": "Allow" }] }</pre>	

Tarea	Descripción	Habilidades requeridas
Envíe una RFC manual para reemplazar el perfil de instancia de IAM.	Envíe una RFC manual para asociar las instancias de EC2 de destino al nuevo perfil de instancias de IAM.	Administrador de sistemas de AWS, desarrollador de AWS
Pruebe una operación de copia en el bucket de S3.	Pruebe una operación de copia en el bucket de S3; para ello, ejecute el comando siguiente en la AWS CLI: `aws s3 cp test.txt s3://<S3 Bucket>/test2.txt`	Administrador de sistemas de AWS, desarrollador de AWS

Recursos relacionados

- Create an IAM instance profile for your Amazon EC2 instances (Crear un perfil de instancia de IAM para las instancias Amazon EC2)
- Creating an S3 bucket (using the Amazon S3 console, AWS SDKs, or AWS CLI) (Crear un bucket de S3 [mediante la consola de Amazon S3, los SDK de AWS o la CLI de AWS])

Automatice la ingesta de flujos de datos en una base de datos de Snowflake mediante Snowflake Snowpipe, Amazon S3, Amazon SNS y Amazon Data Firehose

Creado por Bikash Chandra Rout (AWS)

Entorno: PoC o piloto	Tecnologías: almacenamiento y copia de seguridad

Resumen

Este patrón describe cómo puede utilizar los servicios de la nube de Amazon Web Services (AWS) para procesar un flujo continuo de datos y cargarlo en una base de datos de Snowflake. El patrón utiliza Amazon Data Firehose para entregar los datos a Amazon Simple Storage Service (Amazon S3), Amazon Simple Notification Service (Amazon SNS) para enviar notificaciones cuando se reciben nuevos datos y Snowflake Snowpipe para cargar los datos en una base de datos de Snowflake.

Si sigue este patrón, podrá disponer de datos generados de forma continua para analizarlos en cuestión de segundos, evitando así múltiples comandos de copia manuales. También podrá conseguir un soporte completo para datos semiestructurados al cargarlos.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Una fuente de datos que envía datos de forma continua a un flujo de entrega de Firehose.
- Un depósito de S3 existente que recibe los datos del flujo de entrega de Firehose.
- Una cuenta de Snowflake activa.

Limitaciones

- Snowflake Snowpipe no se conecta directamente a Firehose.

Arquitectura

Pila de tecnología

- Amazon Data Firehose
- Amazon SNS
- Amazon S3
- Snowflake Snowpipe
- Base de datos de Snowflake

Herramientas

- Firehose: Amazon Data Firehose es un servicio totalmente gestionado para entregar datos de streaming en tiempo real a destinos como Amazon S3, Amazon Redshift, Amazon OpenSearch Service, Splunk y cualquier punto de enlace HTTP personalizado o punto de enlace HTTP propiedad de proveedores de servicios externos compatibles.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet.
- Amazon SNS: Amazon Simple Notification Service (Amazon SNS) coordina y administra la entrega o el envío de mensajes a los puntos de enlace o clientes suscritos.
- Snowflake: Snowflake es un almacén de datos analíticos que se proporciona como oftware-as-a S-Service (SaaS).
- Snowflake Snowpipe: Snowpipe carga los datos de los archivos tan pronto como están disponibles en una etapa de Snowflake.

Epics

Configure Snowflake Snowpipe

Tarea	Descripción	Habilidades requeridas
Cree un archivo CSV en Snowflake.	Inicie sesión en Snowflake y ejecute el comando “CREAR	Desarrollador

Tarea	Descripción	Habilidades requeridas
	FORMATO DE ARCHIVO” para crear un archivo CSV con un delimitador de campo específico. Para obtener más información sobre este y otros comandos de Snowflake, consulte la sección “Informac ión adicional”.	
Cree una etapa de Snowflake externa.	Ejecute el comando “CREAR ETAPA” para crear una etapa de Snowflake externa que haga referencia al archivo CSV que creó anteriormente. Importante: Necesitará la URL del bucket de S3, la clave de acceso de AWS y la clave de acceso secreta de AWS. Ejecute el comando “MOSTRAR ETAPAS” para comprobar que se haya creado la etapa de Snowflake.	Desarrollador
Cree la tabla de destino de Snowflake.	Ejecute el comando “CREAR TABLA” para crear la tabla de Snowflake.	Desarrollador

Tarea	Descripción	Habilidades requeridas
Cree una canalización.	Ejecute el comando “CREAR CANALIZACIÓN” y asegúrese de incluir “auto_ingest=true” en el comando. Ejecute el comando “MOSTRAR CANALIZACIONES” para comprobar que se haya creado la canalización. Copie y guarde el valor de la columna “notification_channel”. Este valor se utilizará para configurar las notificaciones de eventos de Amazon S3.	Desarrollador

Configure el bucket de S3

Tarea	Descripción	Habilidades requeridas
Cree una política de ciclo de vida de 30 días para el bucket de S3.	Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3. Elige el depósito S3 que contiene los datos de Firehose. A continuación, seleccione la pestaña “Administración” en el bucket de S3 y elija “Agregar regla de ciclo de vida”. Introduzca un nombre para la regla en el cuadro de diálogo “Regla del ciclo de vida” y configure una regla de ciclo de vida de 30 días para el bucket.	Administrador de sistemas, desarrollador

Tarea	Descripción	Habilidades requeridas
	Para obtener más informaci ón sobre esta y otras explicaci ones, consulte la sección “Recursos relacionados”.	
Cree una política de IAM para el bucket de S3.	Abra la consola de AWS Identity and Access Management (IAM) y seleccione “Políticas”. Elija “Crear política” y, a continuac ión, elija la pestaña “JSON”. Copie y pegue la política de la sección “Información adicional ” en el campo JSON. Esta política otorgará los permisos «PutObjectDeleteObject» y «», así como los permisos «GetObject GetObject Version,» y «ListBucket». Elija “Revisar política”, escriba un nombre para la política y después elija “Crear política”.	Administrador de sistemas, desarrollador

Tarea	Descripción	Habilidades requeridas
Asigne la política a un rol de IAM.	Abra la consola de IAM, elija “Roles” y, a continuación, elija “Crear rol”. Elija “Otra cuenta de AWS” como entidad de confianza. Introduzca el ID de su cuenta de AWS y elija “Requerir ID externo”. Introduzca un marcador de posición de ID que podrá cambiar más adelante. Elija “Siguiente” y asigne la política de IAM que creó anteriorm ente. Luego, cree el rol de IAM.	Administrador de sistemas, desarrollador
Copie el nombre de recurso de Amazon (ARN) para el rol de IAM.	Abra la consola de IAM y seleccione “Roles”. Elija el rol de IAM que creó anteriorm ente y, a continuación, copie y almacene el “ARN del rol”.	Administrador de sistemas, desarrollador

Configure una integración de almacenamiento en Snowflake

Tarea	Descripción	Habilidades requeridas
Cree una integración de almacenamiento en Snowflake .	Inicie sesión en Snowflake y ejecute el comando “CREAR INTEGRACIÓN DE ALMACENAMIENTO”. Esto modificará la relación de confianza, concederá acceso a Snowflake y proporcionará el ID externo de su etapa de Snowflake.	Administrador de sistemas, desarrollador

Tarea	Descripción	Habilidades requeridas
Recupere el rol de IAM para su cuenta de Snowflake.	Ejecute el comando “INTEGRACIÓN DESC” para recuperar el ARN del rol de IAM. Importante: <integration_ name> es el nombre de la integración de almacenamiento de Snowflake que creó anteriormente.	Administrador de sistemas, desarrollador
Registre los valores de dos columnas.	Copie y guarde los valores de las columnas “storage_aws_iam_user_arn” y “storage_aws_external_id”.	Administrador de sistemas, desarrollador

Permita que Snowflake Snowpipe acceda al bucket de S3

Tarea	Descripción	Habilidades requeridas
Modifique la política del rol de IAM.	Abra la consola de IAM y seleccione “Roles”. Elija el rol de IAM que creó anteriormente y seleccione la pestaña “Relaciones de confianza”. Elija “Editar relación de confianza”. Sustituya “snowflake_external_id” por el valor “storage_aws_external_id” que copió anteriormente. Sustituya “snowflake_user_arn” por el valor “storage_aws_iam_user_arn” que copió anteriormente. Elija “Actualizar política de confianza”.	Administrador de sistemas, desarrollador

Active y configure las notificaciones de SNS para el bucket de S3

Tarea	Descripción	Habilidades requeridas
Active las notificaciones de eventos para el bucket de S3.	Abra la consola de Amazon S3 y elija un bucket. Seleccione “Propiedades” y, en “Configuración avanzada”, seleccione “Eventos”. Seleccione “Añadir notificación” e especifique un nombre para este evento. Si no introduce un nombre, se generará un identificador único global (GUID) y se utilizará para el nombre.	Administrador de sistemas, desarrollador
Configure las notificaciones de Amazon SNS para el bucket de S3.	En «Eventos», elija «ObjectCreate (Todos)» y, a continuación, elija «SQS Queue» en la lista desplegable «Enviar a». En la lista “SNS”, seleccione “Añadir ARN de cola de SQS” y pegue el valor “notification_channel” que copió anteriormente. A continuación, elija “Guardar”.	Administrador de sistemas, desarrollador
Suscriba la cola de SQS de Snowflake al tema de SNS.	Suscriba la cola de SQS de Snowflake al tema de SNS que ha creado. Para obtener más información sobre este paso, consulte la sección “Recursos relacionados”.	Administrador de sistemas, desarrollador

Compruebe la integración de la etapa de Snowflake

Tarea	Descripción	Habilidades requeridas
Revise y pruebe Snowpipe.	Inicie sesión en Snowflake y abra la etapa de Snowflake . Coloque los archivos en su bucket de S3 y compruebe si la tabla Snowflake los carga. Amazon S3 enviará notificaciones de SNS a Snowpipe cuando aparezcan nuevos objetos en el bucket de S3.	Administrador de sistemas, desarrollador

Recursos relacionados

- Cree una política de ciclo de vida para un bucket de S3
- Suscriba la cola de SQS de Snowflake al tema de Amazon SNS

Información adicional

Crear un formato de archivo:

```
CREATE FILE FORMAT <name>
TYPE = 'CSV'
FIELD_DELIMITER = '|'
SKIP_HEADER = 1;
```

Crear una etapa externa:

```
externalStageParams (for Amazon S3) ::=
  URL = 's3://[//]'

  [ { STORAGE_INTEGRATION =  } | { CREDENTIALS = ( {  { AWS_KEY_ID = `` AWS_SECRET_KEY
 = `` [ AWS_TOKEN = `` ] } | AWS_ROLE = ``  } ) ) }` ]
  [ ENCRYPTION = ( [ TYPE = 'AWS_CSE' ] [ MASTER_KEY = '' ] |
                   [ TYPE = 'AWS_SSE_S3' ] |
```

```
                    [ TYPE = 'AWS_SSE_KMS' [ KMS_KEY_ID = '' ] |
                    [ TYPE = NONE ] )
```

Creación de una tabla:

```
CREATE [ OR REPLACE ] [ { [ LOCAL | GLOBAL ] TEMP[ORARY] | VOLATILE } | TRANSIENT ]
 TABLE [ IF NOT EXISTS ]
  <table_name>
    ( <col_name> <col_type> [ { DEFAULT <expr>
                                | { AUTOINCREMENT | IDENTITY } [ ( <start_num> ,
 <step_num> ) | START <num> INCREMENT <num> ] } ]
                                 /* AUTOINCREMENT / IDENTITY supported only for numeric
 data types (NUMBER, INT, etc.) */
                             [ inlineConstraint ]
      [ , <col_name> <col_type> ... ]
      [ , outoflineConstraint ]
      [ , ... ] )
  [ CLUSTER BY ( <expr> [ , <expr> , ... ] ) ]
  [ STAGE_FILE_FORMAT = ( { FORMAT_NAME = '<file_format_name>'
                           | TYPE = { CSV | JSON | AVRO | ORC | PARQUET | XML }
 [ formatTypeOptions ] } ) ]
  [ STAGE_COPY_OPTIONS = ( copyOptions ) ]
  [ DATA_RETENTION_TIME_IN_DAYS = <num> ]
  [ COPY GRANTS ]
  [ COMMENT = '<string_literal>' ]
```

Mostrar etapas:

```
SHOW STAGES;
```

Creación de una canalización:

```
CREATE [ OR REPLACE ] PIPE [ IF NOT EXISTS ]
  [ AUTO_INGEST = [ TRUE | FALSE ] ]
  [ AWS_SNS_TOPIC =  ]
  [ INTEGRATION = '' ]
  [ COMMENT = '' ]
  AS
```

Mostrar canalizaciones:

```
SHOW PIPES [ LIKE '<pattern>' ]
```

```
            [ IN { ACCOUNT | [ DATABASE ] <db_name> | [ SCHEMA ] <schema_name> } ]
```

Crear una integración de almacenamiento:

```
CREATE STORAGE INTEGRATION <integration_name>
  TYPE = EXTERNAL_STAGE
  STORAGE_PROVIDER = S3
  ENABLED = TRUE
  STORAGE_AWS_ROLE_ARN = '<iam_role>'
  STORAGE_ALLOWED_LOCATIONS = ('s3://<bucket>/<path>/', 's3://<bucket>/<path>/')
  [ STORAGE_BLOCKED_LOCATIONS = ('s3://<bucket>/<path>/', 's3://<bucket>/<path>/') ]
```

Ejemplo:

```
create storage integration s3_int
  type = external_stage
  storage_provider = s3
  enabled = true
  storage_aws_role_arn = 'arn:aws:iam::001234567890:role/myrole'
  storage_allowed_locations = ('s3://mybucket1/mypath1/', 's3://mybucket2/mypath2/')
  storage_blocked_locations = ('s3://mybucket1/mypath1/sensitivedata/', 's3://
mybucket2/mypath2/sensitivedata/');
```

Para obtener más información sobre este paso, consulte Configuración de una integración de almacenamiento de Snowflake para acceder a Amazon S3 en la documentación de Snowflake.

Describir una integración:

```
DESC INTEGRATION <integration_name>;
```

Política de bucket de S3:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
              "s3:PutObject",
              "s3:GetObject",
              "s3:GetObjectVersion",
```

```
                "s3:DeleteObject",
                "s3:DeleteObjectVersion"
            ],
            "Resource": "arn:aws:s3:::/*"
        },
        {
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::",
            "Condition": {
                "StringLike": {
                    "s3:prefix": [
                        "/*"
                    ]
                }
            }
        }
    ]
}
```

Cifrar automáticamente los volúmenes de Amazon EBS nuevos y existentes

Creado por Tony DeMarco (AWS) y Josh Joy (AWS)

Repositorio de código: https://github.com/aws-samples/ aws-system-manager-automation - unencrypted-to-encrypted-resources /tree/main/ebs	Entorno: producción	Tecnologías: almacenamiento y respaldo; seguridad, identidad y cumplimiento; administración y gobierno
Servicios de AWS: AWS Config; Amazon EBS; AWS KMS; AWS Organizations; AWS Systems Manager		

Resumen

El cifrado de volúmenes de Amazon Elastic Block Store (Amazon EBS) es importante para la estrategia de protección de datos de una organización. Es un paso importante para establecer un entorno bien diseñado. Aunque no hay forma directa de cifrar un volumen o una instantánea existente sin cifrar, puede cifrarlos mediante la creación de un volumen o una instantánea. Para obtener más información, consulte Cifrar recursos de EBS en la documentación de Amazon EC2. Este patrón proporciona controles preventivos y de detección para cifrar los volúmenes de EBS, tanto nuevos como existentes. En este patrón, configura los ajustes de la cuenta, crea procesos de corrección automatizados e implementa controles de acceso.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de Amazon Web Services (AWS) activa
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada en macOS, Linux o Windows.
- jq instalado y configurado en macOS, Linux o Windows.

- Los permisos de AWS Identity and Access Management (IAM) se proporcionan para tener acceso de lectura y escritura a AWS, CloudFormation Amazon Elastic Compute Cloud (Amazon EC2), AWS Systems Manager, AWS Config y AWS Key Management Service (AWS KMS)
- AWS Organizations está configurado con todas las características habilitadas, un requisito para las políticas de control de servicios.
- AWS Config está habilitado en las cuentas de destino.

Limitaciones

- En su cuenta de AWS de destino, no debe haber reglas de AWS Config denominadas encrypted-volumes. Esta solución implementa una regla con este nombre. Las reglas preexistentes con este nombre pueden provocar un error en la implementación y generar cargos innecesarios relacionados con el procesamiento de la misma regla más de una vez.
- Esta solución cifra todos los volúmenes de EBS con la misma clave de AWS KMS.
- Si habilita el cifrado de los volúmenes de EBS de la cuenta, esta configuración es específica de la región. Si lo habilita para una región de AWS, puede deshabilitarlo para volúmenes o instantáneas individuales en esa región. Para obtener más información, consulte Cifrado de forma predeterminada en la documentación de Amazon EC2.
- Cuando corrija los volúmenes de EBS no cifrados existentes, asegúrese de que la instancia de EC2 no esté en uso. Esta automatización cierra la instancia para separar el volumen no cifrado y adjuntar el cifrado. Se produce un tiempo de inactividad mientras se lleva a cabo la corrección. Si se trata de una parte fundamental de la infraestructura para su organización, asegúrese de contar con configuraciones manuales o automáticas de alta disponibilidad para no afectar la disponibilidad de las aplicaciones que se estén ejecutando en la instancia. Le recomendamos que corrija los recursos críticos solo durante los períodos de mantenimiento estándar.

Arquitectura

Flujo de trabajo de automatización

1. AWS Config detecta un volumen de EBS sin cifrar.
2. Un administrador usa AWS Config para enviar un comando de corrección a Systems Manager.
3. La automatización de Systems Manager toma una instantánea del volumen de EBS no cifrado.

4. La automatización de Systems Manager utiliza AWS KMS para crear una copia cifrada de la instantánea.
5. La automatización de Systems Manager hace lo siguiente:
   a. Detiene la instancia de EC2 afectada si se está ejecutando.
   b. Adjunta la nueva copia cifrada del volumen a la instancia de EC2.
   c. Regresa la instancia de EC2 a su estado original.

Herramientas

Servicios de AWS

- AWS CLI: la interfaz de la línea de comandos de AWS (AWS CLI) proporciona acceso directo a las interfaces de programación de aplicaciones (API) públicas de los servicios de AWS. Puede explorar las capacidades de un servicio con la CLI de AWS y desarrollar scripts de shell para administrar los recursos. Además de los comandos equivalentes de la API de bajo nivel, varios servicios de AWS ofrecen personalizaciones para la CLI de AWS. Las personalizaciones pueden incluir comandos de un nivel superior que simplifican el uso de un servicio con una API compleja.
- AWS CloudFormation: AWS CloudFormation es un servicio que le ayuda a modelar y configurar sus recursos de AWS. Crea una plantilla que describe todos los recursos de AWS que desea (como las instancias de Amazon EC2) y CloudFormation aprovisiona y configura esos recursos por usted.
- AWS Config: AWS Config proporciona una visión detallada de la configuración de los recursos de AWS de su cuenta de AWS. Esto incluye cómo se relacionan los recursos entre sí y cómo se han configurado en el pasado, para que pueda ver cómo las configuraciones y las relaciones cambian a lo largo del tiempo.
- Amazon EC2: Amazon Elastic Compute Cloud (Amazon EC2) es un servicio web que proporciona una capacidad de computación redimensionable para que pueda crear y alojar sus sistemas de software.
- AWS KMS: AWS Key Management Service (AWS KMS) es un servicio de cifrado y administración de claves escalado para la nube. Otros servicios de AWS utilizan las claves y la funcionalidad de AWS KMS, y usted puede utilizarlas para proteger los datos de su entorno de AWS.
- AWS Organizations: AWS Organizations es un servicio de administración de cuentas que le permite unificar varias cuentas de AWS en una organización que crea y administra de forma centralizada.

- Automatización de AWS Systems Manager: la automatización de Systems Manager simplifica las tareas comunes de mantenimiento e implementación de instancias de Amazon EC2 y de otros recursos de AWS.

Otros servicios

- jq: jq es un procesador JSON de línea de comandos ligero y flexible. Esta herramienta se utiliza para extraer información clave de la salida de la CLI de AWS.

Código

- El código de este patrón está disponible en el repositorio Cómo corregir GitHub automáticamente los volúmenes de EBS no cifrados mediante claves de KMS del cliente.

Epics

Automatizar la corrección de volúmenes no cifrados

Tarea	Descripción	Habilidades requeridas
Descargue scripts y plantillas. CloudFormation	Descargue el script de shell, el archivo JSON y CloudFormation las plantillas del repositorio Remediar GitHub automáticamente volúmenes de EBS no cifrados mediante claves KMS del cliente.	Administrador de AWS, AWS general
Identifique al administrador de la clave de AWS KMS.	1. Inicie sesión en la consola de administración de AWS y abra la consola de IAM en https://console.aws.amazon.com/iam/. 2. Identifique un usuario o rol que será el administrador de clave de AWS KMS. Si es necesario	Administrador de AWS, AWS general

Tarea	Descripción	Habilidades requeridas
	crear un nuevo usuario o rol para este propósito, créelo ahora. Para obtener más información, consulte Identidades de IAM en la documentación de IAM. Esta automatización crea una nueva clave de AWS KMS. 3. Una vez identificado, copie el nombre de recurso de Amazon (ARN) del usuario o rol. Para obtener más información, consulte ARN de IAM en la documentación de IAM. Utilizará este ARN en el siguiente paso.	

Tarea	Descripción	Habilidades requeridas
Implemente la plantilla Stack1. CloudFormation	1. Abra la CloudFormation consola de AWS en https://console.aws.amazon.com/cloudformation/. 2. En CloudFormation, implemente la `Stack1.yaml` plantilla. Tenga en cuenta los siguientes detalles de implementación: • Proporcione a la pila un nombre claro y descriptivo. Tenga en cuenta el nombre de pila porque necesita este valor en el siguiente paso. • Pegue el ARN del administrador de clave en el único campo de parámetro de Stack1. Este usuario o rol se convierte en el administrador de la clave de AWS KMS creada por la pila. Para obtener más información sobre la implementación de una CloudFormation plantilla, consulte Trabajar con CloudFormation plantillas de AWS en la CloudFormation documentación.	Administrador de AWS, AWS general

Tarea	Descripción	Habilidades requeridas
Implemente la plantilla Stack2 CloudFormation .	En CloudFormation, despliega la `Stack2.yaml` plantilla. Tenga en cuenta los siguientes detalles de implementación: • Proporcione a la pila un nombre claro y descriptivo. • Para el único parámetro de Stack2, introduzca el nombre de la pila que creó en el paso anterior. Esto permite a Stack2 hacer referencia a la nueva clave y rol de AWS KMS implementados por la pila en el paso anterior.	Administrador de AWS, AWS general
Cree un volumen sin cifrar para realizar pruebas.	Cree una instancia de EC2 con un volumen de EBS sin cifrar. Para obtener instrucciones, consulte Creación de un volumen de Amazon EBS en la documentación de Amazon EC2. El tipo de instancia no importa y no es necesario acceder a la instancia. Puede crear una instancia t2.micro para permanecer en el nivel gratuito y no necesita crear un par de claves.	Administrador de AWS, AWS general

Tarea	Descripción	Habilidades requeridas
Pruebe la regla de AWS Config.	1. Abra la consola de AWS Config en https://console.aws.amazon.com/config/. En la página Reglas, seleccione la regla encrypted-volumes. 2. Confirme que la nueva instancia de prueba sin cifrar aparezca en la lista de recursos no conformes. Si el volumen no aparece inmediatamente, espere unos minutos y actualice los resultados. La regla AWS Config detecta los cambios en los recursos poco después de crear la instancia y el volumen. 3. Seleccione el recurso y, a continuación, seleccione Corregir. Puede ver el progreso y el estado de la corrección en Systems Manager de la siguiente manera: 1. Abra la consola de AWS Systems Manager en https://console.aws.amazon.com/systems-manager/. 2. En el panel de navegación, elija automatización.	Administrador de AWS, AWS general

Tarea	Descripción	Habilidades requeridas
	3. Seleccione el enlace ID de ejecución para ver los pasos y el estado.	
Configure cuentas o regiones de AWS adicionales.	Según sea necesario para su caso de uso, repita esta epopeya para cualquier otra cuenta o región de AWS.	Administrador de AWS, AWS general

Habilitar el cifrado a nivel de cuenta de los volúmenes de EBS

Tarea	Descripción	Habilidades requeridas
Ejecute el script de habilitación.	1. En un shell de bash, use el comando `cd` para navegar hasta el repositorio clonado. 2. Ingrese el comando siguiente para ejecutar el script `enable-ebs-encryption-for-account` . `./Bash/enable-ebs-encryption-for-account.sh`	Administrador de AWS, AWS general, bash
Confirme si la configuración está actualizada.	1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/. 2. En la parte derecha de la pantalla, en Configuración, selecciona Protección y seguridad de datos.	Administrador de AWS, AWS general

Tarea	Descripción	Habilidades requeridas
	3. En la sección de cifrado de EBS, confirme que la opción Encriptar siempre los nuevos volúmenes de EBS esté activada y que la clave de cifrado predeterminada esté establecida en el ARN que especificó anteriormente. Nota: Si la configuración Encriptar siempre los nuevos volúmenes de EBS está desactivada o la clave sigue configurada en alias/aws/ebs, confirme que ha iniciado sesión en la misma cuenta y región de AWS en la que ejecutó el script de shell y compruebe si hay mensajes de error en el shell.	
Configure cuentas o regiones de AWS adicionales.	Según sea necesario para su caso de uso, repita esta epopeya para cualquier otra cuenta o región de AWS.	Administrador de AWS, AWS general

Impedir la creación de instancias no cifradas

Tarea	Descripción	Habilidades requeridas
Cree una política de control de servicios.	1. Abra la consola de AWS Organizations en https://c	Administrador de AWS, AWS general

Tarea	Descripción	Habilidades requeridas
	onsole.aws.amazon.com/organizations/v2/. 2. Cree una nueva política de control de servicios. Para obtener más información, consulte Creación, actualización y eliminación de políticas de control de servicios en la documentación de AWS Organizations. 3. Añada el contenido de `DenyUnencryptedEC2.json` a la política y guárdelo. En la primera epopeya, descargó este archivo JSON del repositorio. GitHub 4. Adjunte esta política a la raíz de la organización o a cualquier unidad organizativa (OU) necesaria. Para obtener más información, consulte Asociar y desasociar políticas de control de servicios en la documentación de AWS Organizations.	

Recursos relacionados

Documentación de servicio de AWS

- CLI de AWS
- AWS Config

- AWS CloudFormation
- Amazon EC2
- AWS KMS
- AWS Organizations
- Automatización de AWS Systems Manager

Otros recursos

- jq manual (sitio web de jq)
- descarga jq () GitHub

Realice copias de seguridad de los servidores Sun SPARC en el emulador Stromasys Charon-SSP en la nube de AWS

Creado por Kevin Yung (AWS), Luis Ramos (Stromasys) y Rohit Darji (AWS)

Entorno: producción	Tecnologías: almacenamiento y respaldo; sistemas operativos; DevOps	Carga de trabajo: Oracle
Servicios de AWS: Amazon EFS; Amazon S3; AWS Storage Gateway; AWS Systems Manager; Amazon EC2		

Resumen

Este patrón ofrece cuatro opciones para realizar copias de seguridad de los servidores SPARC de Sun Microsystems tras una migración de un entorno en las instalaciones a la nube de Amazon Web Services (AWS). Estas opciones de copia de seguridad lo ayudan a implementar un plan de copia de seguridad que cumpla con el objetivo de punto de recuperación (RPO) y el objetivo de tiempo de recuperación (RTO) de su organización, utilice enfoques automatizados y reduzca sus costos operativos generales. El patrón proporciona una descripción general de las cuatro opciones de copia de seguridad y los pasos para implementarlas.

Si utiliza un servidor Sun SPARC alojado como huésped en un emulador Charon-SSP de Stromasys, puede utilizar una de las tres opciones de copia de seguridad siguientes:

- Opción de copia de seguridad 1: cinta virtual Stromasys: utilice la función de cinta virtual Charon-SSP para configurar una instalación de copia de seguridad en el servidor Sun SPARC y archivar los archivos de copia de seguridad en Amazon Simple Storage Service (Amazon S3) y Amazon Simple Storage Service Glacier mediante la Automatización de AWS Systems Manager.
- Opción de copia de seguridad 2: instantánea de Stromasys: utilice la característica de instantáneas de Charon-SSP para configurar una función de copia de seguridad para los servidores invitados Sun SPARC en Charon-SSP.

- Opción de copia de seguridad 3: instantánea de volumen de Amazon Elastic Block Store (Amazon EBS): si aloja el emulador Charon-SSP en Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2), puede usar una instantánea de volumen de Amazon EBS para crear copias de seguridad para un sistema de archivos Sun SPARC.

Si utiliza un servidor Sun SPARC alojado como huésped en un emulador Charon-SSP de EC2, puede utilizar la opción de copia de seguridad siguiente:

- Opción de copia de seguridad 4: biblioteca de cintas virtuales (VTL) AWS Storage Gateway: utilice una aplicación de copia de seguridad con una puerta de enlace de cinta Storage Gateway VTL para realizar copias de seguridad de los servidores Sun SPARC.

Si utiliza un servidor Sun SPARC alojado como una zona de marca en un servidor Sun SPARC, puede utilizar las opciones de copia de seguridad 1, 2 y 4.

Stromasys proporciona software y servicios para emular los sistemas críticos antiguos SPARC, Alpha, VAX y PA-RISC. Para obtener más información sobre la migración a la nube de AWS mediante la emulación de Stromasys, consulte Realojar SPARC, Alpha u otros sistemas heredados en AWS con Stromasys en el blog de AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Servidores Sun SPARC existentes.
- Licencias para Charon-SSP existentes. Las licencias para Charon-SSP están disponibles en AWS Marketplace y las licencias para Stromasys Virtual Environment (VE) están disponibles en Stromasys. Para obtener más información, póngase en contacto con el departamento de ventas de Stromasys.
- Familiaridad con los servidores Sun SPARC y las copias de seguridad de Linux.
- Familiaridad con la tecnología de emulación Charon-SSP. Para obtener más información al respecto, consulte la emulación de servidores antiguos de Stromasys en la documentación de Stromasys.
- Si desea utilizar la función de cinta virtual o las aplicaciones de copia de seguridad para los sistemas de archivos de sus servidores Sun SPARC, debe crear y configurar las instalaciones de copia de seguridad para el sistema de archivos del servidor Sun SPARC.

- Comprensión del RPO y el RTO. Para obtener más información al respecto, consulte los objetivos de recuperación de desastres del documento técnico sobre el pilar de la fiabilidad en la documentación del Marco de AWS Well-Architected.
- Para usar la opción 4 de copia de seguridad, debe tener lo siguiente:
  - Aplicación de backup basada en software que admite una Puerta de enlace de cinta Storage Gateway VTL. Para obtener más información, consulte Trabajar con dispositivos VTL en la documentación de AWS Storage Gateway.
  - Bacula Director o una aplicación de copia de seguridad similar, instalada y configurada. Para obtener información, consulte la documentación de Bacula Director.

En la siguiente tabla se proporciona información sobre las cuatro opciones de copia de seguridad de este patrón.

Opciones de copia de seguridad	¿Es coherente ante bloqueos?	¿Es coherente en cuanto a las aplicaciones?	¿Solución de dispositivo de copia de seguridad virtual?	Casos de uso típicos
Opción 1: cinta virtual Stromasys	Sí Puede automatizar las instantáneas del sistema de archivos Sun SPARC para hacer copias de seguridad de los datos en una cinta virtual. Por ejemplo, puede utilizar instantáneas de UFS o ZFS.	Sí Esta opción de copia de seguridad requiere un script automatizado para vaciar las transacciones en curso, configurar un modo sin conexión temporal o de solo lectura durante la instantánea del sistema	Sí	Realice copias de seguridad de los sistemas de archivos del servidor Sun SPARC con archivos .tar o .zip Copia de seguridad de los datos de la aplicación

	de archivos o realizar un volcado de datos de la aplicació n. Es posible que también necesite tiempo de inactividad de la aplicación o modo de solo lectura.

Opción 2: instantánea de Stromasys	Sí Debe configurar el Administrador Charon-SSP o utilizar un argumento de startup desde la línea de comandos para habilitar esta característica. También debe ejecutar un comando de Linux para solicitar al emulador Charon-SSP que guarde el estado del servidor invitado Sun SPARC en un archivo de instantánea. Importante: debe apagar el servidor invitado Sun SPARC.	Sí Esta opción de copia de seguridad crea una instantánea del servidor invitado emulado, incluidos sus discos virtuales y su volcado de memoria. Importante: debe apagar el servidor invitado Sun SPARC durante la instantánea.	No	Instantánea del servidor Sun SPARC Copia de seguridad de los datos de la aplicación

Opción 3: instantánea de volumen de Amazon EBS	Sí Puede usar AWS Backup para automatizar la instantánea de Amazon EBS.	Sí Esta opción de copia de seguridad requiere un script automatizado para vaciar las transacciones en curso y configurar una parada temporal o de solo lectura de la instancia EC2 durante la instantánea del volumen de Amazon EBS. Importante: esta opción de copia de seguridad puede requerir un tiempo de inactividad de la aplicación o un modo de solo lectura para lograr la coherencia de la aplicación.	No	Instantánea de los sistemas de archivos del servidor Sun SPARC Copia de seguridad de los datos de la aplicación

Opción 4: AWS Storage Gateway VTL	Sí Puede realizar automáticamente una copia de seguridad de los datos de copia de seguridad del sistema de archivos Sun SPARC en la VTL mediante un agente de copia de seguridad.	Sí Esta opción de copia de seguridad requiere un script automatizado para vaciar las transacciones en curso, configura r un modo sin conexión temporal o de solo lectura durante la instantánea del sistema de archivos o realizar un volcado de datos de la aplicación. Importante: esta opción de copia de seguridad puede requerir un tiempo de inactividad de la aplicación o un modo de solo lectura.	Sí	Una amplia flota de copias de seguridad del sistema de archivos del servidor Sun SPARC Copia de seguridad de los datos de la aplicación

Limitaciones

- Puede utilizar los enfoques de este patrón para hacer copias de seguridad de servidores Sun SPARC individuales, pero también puede utilizar estas opciones de copia de seguridad para datos compartidos si tiene aplicaciones que se ejecutan en un clúster.

Herramientas

Opción de copia de seguridad 1: cinta virtual Stromasys

- Emulador Charon-SSP de Stromasys: el emulador de Charon-SSP crea la réplica virtual del hardware SPARC original dentro de un sistema informático estándar compatible con x86 de 64 bits. Ejecuta el código binario SPARC original, incluidos sistemas operativos como SunOS o Solaris, sus productos en capas y sus aplicaciones.
- Amazon EC2: Amazon Elastic Compute Cloud (Amazon EC2) es un servicio web que proporciona una capacidad de computación redimensionable para que pueda crear y alojar sus sistemas de software.
- Amazon EFS: Amazon Elastic File System (Amazon EFS) proporciona un sistema de archivos simple, set-and-forget elástico y sin servidor para su uso con los servicios en la nube y los recursos locales de AWS.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet.
- Amazon S3 Glacier: Amazon S3 Glacier es un servicio de almacenamiento seguro, duradero y de bajo costo para archivo de datos y copias de seguridad a largo plazo.
- Automatización de AWS Systems Manager: la automatización, una capacidad de AWS Systems Manager, simplifica las tareas comunes de mantenimiento e implementación de las instancias de EC2 y otros recursos de AWS.

Opción de copia de seguridad 2: instantánea de Stromasys

- Emulador Charon-SSP de Stromasys: el emulador de Charon-SSP crea la réplica virtual del hardware SPARC original dentro de un sistema informático estándar compatible con x86 de 64 bits. Ejecuta el código binario SPARC original, incluidos sistemas operativos como SunOS o Solaris, sus productos en capas y sus aplicaciones.

- Amazon EC2: Amazon Elastic Compute Cloud (Amazon EC2) es un servicio web que proporciona una capacidad de computación redimensionable para que pueda crear y alojar sus sistemas de software.
- Amazon EFS: Amazon Elastic File System (Amazon EFS) proporciona un sistema de archivos simple, set-and-forget elástico y sin servidor para su uso con los servicios en la nube y los recursos locales de AWS.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet.
- Amazon S3 Glacier: Amazon S3 Glacier es un servicio de almacenamiento seguro, duradero y de bajo costo para archivo de datos y copias de seguridad a largo plazo.
- Automatización de AWS Systems Manager: la automatización, una capacidad de AWS Systems Manager, simplifica las tareas comunes de mantenimiento e implementación de las instancias de EC2 y otros recursos de AWS.

Opción de copia de seguridad 3: instantánea de volumen de Amazon EBS

- Emulador Charon-SSP de Stromasys: el emulador de Charon-SSP crea la réplica virtual del hardware SPARC original dentro de un sistema informático estándar compatible con x86 de 64 bits. Ejecuta el código binario SPARC original, incluidos sistemas operativos como SunOS o Solaris, sus productos en capas y sus aplicaciones.
- AWS Backup es un servicio totalmente administrado que facilita la centralización y automatización de la protección de datos en todos los servicios de AWS, en la nube y en las instalaciones.
- Amazon EBS: Amazon Elastic Block Store (Amazon EBS) proporciona volúmenes de almacenamiento por bloques para su uso con instancias de EC2.
- Amazon EC2: Amazon Elastic Compute Cloud (Amazon EC2) es un servicio web que proporciona una capacidad de computación redimensionable para que pueda crear y alojar sus sistemas de software.

Opción de copia de seguridad 4: AWS Storage Gateway VTL

- Emulador Charon-SSP de Stromasys: el emulador de Charon-SSP crea la réplica virtual del hardware SPARC original dentro de un sistema informático estándar compatible con x86 de 64

bits. Ejecuta el código binario SPARC original, incluidos sistemas operativos como SunOS o Solaris, sus productos en capas y sus aplicaciones.

- Bacula es un sistema de copia de seguridad informática de código abierto y de nivel empresarial. Para obtener más información sobre si su aplicación de copia de seguridad existente es compatible con Tape Gateway, consulte Aplicaciones de copia de seguridad de terceros compatibles para una puerta de enlace de cinta en la documentación de AWS Storage Gateway.
- Amazon EC2: Amazon Elastic Compute Cloud (Amazon EC2) es un servicio web que proporciona una capacidad de computación redimensionable para que pueda crear y alojar sus sistemas de software.
- Amazon RDS para MySQL: Amazon Relational Database Service (Amazon RDS) admite instancias de bases de datos en las que se ejecutan varias versiones de MySQL.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet.
- Amazon S3 Glacier: Amazon S3 Glacier es un servicio de almacenamiento seguro, duradero y de bajo costo para archivo de datos y copias de seguridad a largo plazo.
- AWS Storage Gateway conecta un dispositivo de software en las instalaciones con el almacenamiento basado en la nube para ofrecer una integración fluida con características de seguridad de datos entre el entorno de TI local y la infraestructura de almacenamiento de AWS.

Epics

Opción de copia de seguridad 1: crear una copia de seguridad en cinta virtual de Stromasys

Tarea	Descripción	Habilidades requeridas
Cree un sistema de archivos compartidos Amazon EFS para el almacenamiento de archivos en cinta virtual.	Inicie sesión en la consola de administración de AWS o utilice CLI de AWS para crear un sistema de archivos de Amazon EFS. Para obtener más información, consulte Crear un sistema de archivos de Amazon EFS en	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	la documentación de Amazon EFS.	
Configure el host Linux para montar el sistema de archivos compartidos.	Instale el controlador Amazon EFS en la instancia Linux Amazon EC2 y configure el sistema operativo Linux para montar el sistema de archivos compartidos Amazon EFS durante el startup. Para obtener más información al respecto, consulte Montaje de sistemas de archivos mediante el asistente de montaje EFS en la documentación de Amazon EFS.	DevOps ingeniero
Instale el emulador Charon-SSP.	Instale el emulador Charon-SSP en la instancia Linux de Amazon EC2. Para obtener más información al respecto, consulte Configuración de una instancia de nube de AWS para Charon-SSP en la documentación de Stromasys.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Cree un contenedor de archivos de cinta virtual en el sistema de archivos compartido para cada servidor huésped Sun SPARC.	Ejecute el comando `touch <vtape-container-name>` para crear un contenedor de archivos de cinta virtual en el sistema de archivos compartido para cada servidor huésped Sun SPARC implementado en el emulador Charon-SSP.	DevOps ingeniero
Configure Charon-SSP Manager para crear dispositivos de cinta virtuales para los servidores invitados SPARC de Sun.	Inicie sesión en Charon-SSP Manager, cree dispositivos de cinta virtuales y configúrelos para que utilicen los archivos contenedores de cintas virtuales de cada servidor huésped Sun SPARC. Para obtener más información al respecto, consulte la guía del usuario de Charon-SSP 5.2 para Linux en la documentación de Stromasys.	DevOps ingeniero
Valide que el dispositivo de cinta virtual esté disponible en los servidores invitados Sun SPARC.	Inicie sesión en cada servidor huésped Sun SPARC y ejecute el comando `mt -f /dev/rmt/1` para validar que el dispositivo de cinta virtual esté configurado en el sistema operativo.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Cree un manual de procedimientos de Systems Manager Automation.	Desarrolle el manual de procedimientos de automatización de Systems Manager y configure ventanas y asociaciones de mantenimiento en Systems Manager para programar el proceso de copia de seguridad. Para obtener más información, consulte Un recorrido por la automatización y Configurar las ventanas de mantenimiento en la documentación de AWS Systems Manager.	Arquitecto de la nube
Configure Systems Manager Automation para archivar los archivos de contenedores de cintas virtuales rotados.	Utilice el ejemplo de código de la Opción de copia de seguridad 1 de la sección Información adicional para desarrollar un manual de procedimientos de automatización de Systems Manager para archivar archivos contenedores de cintas virtuales rotados en Amazon S3 y Amazon S3 Glacier.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Implemente el manual de procedimientos de automatización de Systems Manager para archivar y programar.	Implemente el manual de procedimientos de automatización de Systems Manager y prográmelo para que se ejecute automáticamente en Systems Manager. Para obtener más información, consulte Configuración de la automatización en la documentación de Systems Manager.	Arquitecto de la nube

Opción de copia de seguridad 2: crear una instantánea de Stromasys

Tarea	Descripción	Habilidades requeridas
Cree un sistema de archivos compartidos Amazon EFS para el almacenamiento de archivos en cinta virtual.	Inicie sesión en la consola de administración de AWS o utilice CLI de AWS para crear un sistema de archivos de Amazon EFS. Para obtener más información, consulte Crear un sistema de archivos de Amazon EFS en la documentación de Amazon EFS.	Arquitecto de la nube
Configure el host Linux para montar el sistema de archivos compartidos.	Instale el controlador Amazon EFS en la instancia Linux Amazon EC2 y configure el sistema operativo Linux para montar el sistema de archivos	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
	compartidos Amazon EFS durante el inicio. Para obtener más información al respecto, consulte Montaje de sistemas de archivos mediante el asistente de montaje EFS en la documentación de Amazon EFS.	
Instale el emulador Charon-SSP.	Instale el emulador Charon-SSP en la instancia Linux de Amazon EC2. Para obtener más información al respecto, consulte Configuración de una instancia de nube de AWS para Charon-SSP en la documentación de Stromasys.	DevOps ingeniero
Configure los servidores invitados SPARC de Sun para que se inicien con la opción de instantánea.	Utilice el administrador Charon-SSP para configurar la opción de instantáneas para cada servidor huésped Sun SPARC. Para obtener más información al respecto, consulte la guía del usuario de Charon-SSP 5.2 para Linux en la documentación de Stromasys.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Cree un manual de procedimientos de Systems Manager Automation.	Utilice el ejemplo de código de la Opción de copia de seguridad 2 de la sección Información adicional para desarrollar un manual de procedimientos de automatización de Systems Manager para ejecutar de forma remota el comando snapshot en un servidor huésped Sun SPARC durante un período de mantenimiento.	Arquitecto de la nube
Implemente el manual de procedimientos de automatización de Systems Manager y configure la asociación a los hosts Linux de Amazon EC2.	Desarrolle el manual de procedimientos de automatización de Systems Manager y configure ventanas y asociaciones de mantenimiento en Systems Manager para programar el proceso de copia de seguridad. Para obtener más información, consulte Un recorrido por la automatización y Configurar las ventanas de mantenimiento en la documentación de AWS Systems Manager.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
Archive las instantáneas en un almacenamiento a largo plazo.	Utilice el ejemplo de código del manual de procedimientos de la sección Additional information (Información adicional) para desarrollar un manual de procedimientos de Systems Manager para archivar archivos de instantáneas en Amazon S3 y Amazon S3 Glacier.	Arquitecto de la nube

Opción de copia de seguridad 3: crear una instantánea de volumen de Amazon EBS

Tarea	Descripción	Habilidades requeridas
Instale el emulador Charon-SSP.	Instale el emulador Charon-SSP en la instancia Linux de Amazon EC2. Para obtener más información al respecto, consulte Configuración de una instancia de nube de AWS para Charon-SSP en la documentación de Stromasys.	DevOps ingeniero
Cree volúmenes de EBS para los servidores invitados del Sun SPRAC.	Inicie sesión en la consola de administración de AWS, abra la consola de Amazon EBS y, a continuación, cree volúmenes de EBS para los servidores invitados de Sun SPRAC.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	Para obtener más información al respecto, consulte Configuración de una instancia de nube de AWS para Charon-SSP en la documentación de Stromasys.	
Adjunte los volúmenes de Amazon EBS a la instancia Linux de Amazon EC2.	En la consola de Amazon EC2, adjunte los volúmenes de EBS a la instancia Linux de Amazon EC2. Para obtener más información, consulte Adjuntar un volumen de Amazon EBS a una instancia en la documentación de Amazon EC2.	AWS DevOps
Mapee los volúmenes de EBS como unidades SCSI en el emulador Charon-SSP.	Configure el administrador Charon-SSP para mapear los volúmenes de EBS como unidades SCSI en los servidores invitados Sun SPARC. Para obtener más información al respecto, consulte la sección Configuración del almacenamiento SCSI en la guía de Charon-SSP 5.2 para Linux en la documentación de Stromasys.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Configure el programa de AWS Backup para realizar instantáneas de los volúmenes de EBS.	Configure la política y los cronogramas de AWS Backup para realizar instantáneas de los volúmenes de EBS. Para obtener más información al respecto, consulte el tutorial sobre Copia de seguridad y restauración de Amazon EBS mediante AWS Backup en la documentación del Centro de desarrolladores de AWS.	AWS DevOps

Opción de copia de seguridad 4: creación de una VTL de AWS Storage Gateway

Tarea	Descripción	Habilidades requeridas
Cree un dispositivo de Puerta de enlace de cinta.	Inicie sesión en la consola de administración de AWS, abra la consola AWS Storage Gateway y, a continuación, cree un dispositivo de Puerta de enlace de cinta en una VPC. Para obtener más información al respecto, consulte Creación de una puerta de enlace en la documentación de AWS Storage Gateway.	Arquitecto de la nube
Creación de una instancia de base de datos de Amazon RDS para el catálogo de Bacula.	Abra la consola de Amazon RDS y cree una instancia de base de datos de Amazon RDS para MySQL.	Arquitecto de la nube

Tarea	Descripción	Habilidades requeridas
	Para obtener más información al respecto, consulte Creación de una instancia de base de datos MySQL y conexión a una base de datos en una instancia de base de datos MySQL en la documentación de Amazon RDS.	
Implemente el controlador de aplicaciones de copia de seguridad en la VPC.	Instale Bacula en la instancia EC2, implemente el controlador de aplicaciones de copia de seguridad y, a continuación, configure el almacenamiento de copia de seguridad para que se conecte al dispositivo de Puerta de enlace de cinta. Puede usar el ejemplo de configuración del daemon de almacenamiento de Bacula Director que se encuentra en el archivo `Bacula-storage-daemon-config.txt` (adjunto). Para obtener más información, consulte la documentación de Bacula.	AWS DevOps

Tarea	Descripción	Habilidades requeridas
Configure la aplicación de copia de seguridad en los servidores invitados Sun SPARC.	Configure un segundo cliente para instalar y configurar la aplicación de copia de seguridad en los servidore s invitados de Sun SPARC utilizando el ejemplo de configuración de Bacula que se incluye en el archivo `SUN-SPARC-Guest-Bacula-Config.txt` (adjunto).	DevOps ingeniero
Configure la configuración y la programación de la copia de seguridad.	Configure la configuración y los horarios de las copias de seguridad en el controlador de la aplicación de copia de seguridad mediante el ejemplo de configuración de Bacula Director que se encuentra en el archivo `Bacula-Di rectory-Config.txt` (adjunto). Para obtener más información, consulte la documentación de Bacula.	DevOps ingeniero

Tarea	Descripción	Habilidades requeridas
Valide que la configuración y los programas de copia de seguridad sean correctos.	Siga las instrucciones de la documentación de Bacula para realizar las pruebas de validación y copia de seguridad de su configuración en los servidores invitados Sun SPARC. Por ejemplo, puede utilizar los siguientes comandos para validar los archivos de configuración: • `bacula-dir -t -c bacula-dir.conf` • `bacula-fd -t -c bacula-fd.conf` • `bacula-sd -t -c bacula-sd.conf`	DevOps ingeniero

Recursos relacionados

- SPARC virtual de Charon con licencia VE
- SPARC virtual de Charon
- Uso de servicios en la nube y almacenamiento de objetos con Bacula Enterprise Edition
- Objetivos de recuperación de desastres (DR)
- Soluciones de emulación de sistemas heredados de Charon

Información adicional

Opción de copia de seguridad 1: crear una cinta virtual de Stromasys

Puede utilizar el siguiente código de ejemplo del manual de procedimientos de automatización de Systems Manager para iniciar automáticamente la copia de seguridad y, a continuación, cambiar las cintas:

```
...
# example backup script saved in SUN SPARC Server
 #!/usr/bin/bash
 mt -f  rewind
 tar -cvf
 mt -f  offline
...
         mainSteps:
         - action: aws:runShellScript
           name:
           inputs:
             onFailure: Abort
             timeoutSeconds: "1200"
             runCommand:
             - |
               # Validate tape backup container file exists
               if [ ! -f {{TapeBackupContainerFile}} ]; then
                 logger -s -p local3.warning "Tape backup container file is not exists
 - {{TapeBackupContainerFile}}, create a new one"
                 touch {{TapeBackupContainerFile}}
               fi
         - action: aws:runShellScript
           name: startBackup
           inputs:
             onFailure: Abort
             timeoutSeconds: "1200"
             runCommand:
             - |
               user={{BACKUP_USER}}
               keypair={{KEYPAIR_PATH}}
               server={{SUN_SPARC_IP}}
               backup_script={{BACKUP_SCRIPT}}
               ssh -i $keypair $user@$server -c "/usr/bin/bash $backup_script"
         - action: aws:runShellScript
           name: swapVirtualDiskContainer
           inputs:
             onFailure: Abort
             timeoutSeconds: "1200"
             runCommand:
```

```
            - |
              mv {{TapeBackupContainerFile}} {{TapeBackupContainerFile}}.$(date +%s)
              touch {{TapeBackupContainerFile}}
        - action: aws:runShellScript
          name: uploadBackupArchiveToS3
          inputs:
            onFailure: Abort
            timeoutSeconds: "1200"
            runCommand:
            - |
              aws s3 cp {{TapeBackupContainerFile}} s3://{{BACKUP_BUCKET}}/
{{SUN_SPARC_IP}}/$(date '+%Y-%m-%d')/
 ...
```

Opción de copia de seguridad 2: crear una instantánea de Stromasys

Puede utilizar el siguiente código de ejemplo del manual de procedimientos de automatización de Systems Manager para iniciar automáticamente la copia de seguridad.

```
     ...

        mainSteps:
        - action: aws:runShellScript
          name: startSnapshot
          inputs:
            onFailure: Abort
            timeoutSeconds: "1200"
            runCommand:
            - |
              # You may consider some graceful stop of the application before taking a
 snapshot
              # Query SSP PID by configuration file
              # Example: ps ax | grep ssp-4 | grep Solaris10.cfg | awk '{print $1"
"$5}' | grep ssp4 | cut -f1 -d" "
              pid=`ps ax | grep ssp-4 | grep {{SSP_GUEST_CONFIG_FILE}} | awk '{print
$1" "$5}' | grep ssp4 | cut -f1 -d" "`
              if [ -n "${pid}" ]; then
                kill -SIGTSTP ${pid}
              else
                echo "No PID found for SPARC guest with config
 {{SSP_GUEST_CONFIG_FILE}}"
                exit 1
              fi
```

```
         - action: aws:runShellScript
           name: startBackup
           inputs:
             onFailure: Abort
             timeoutSeconds: "1200"
             runCommand:
             - |
               # upload snapshot and virtual disk files into S3
               aws s3 sync {{SNAPSHOT_FOLDER}} s3://{{BACKUP_BUCKET}}/$(date '+%Y-%m-
%d')/
               aws s3 cp {{VIRTUAL_DISK_FILE}} s3://{{BACKUP_BUCKET}}/$(date '+%Y-%m-
%d')/
         - action: aws:runShellScript
           name: restratSPARCGuest
           inputs:
             onFailure: Abort
             timeoutSeconds: "1200"
             runCommand:
             - |
               /opt/charon-ssp/ssp-4u/ssp4u -f {{SSP_GUEST_CONFIG_FILE}} -d -a
 {{SPARC_GUEST_NAME}} --snapshot {{SNAPSHOT_FOLDER}}
 ...
```

Opción de copia de seguridad 4: AWS Storage Gateway VTL

Si utiliza zonas no globales de Solaris para ejecutar servidores Sun SPARC antiguos virtualizados, el enfoque de la aplicación de copia de seguridad se puede aplicar a las zonas no globales que se ejecutan en los servidores Sun SPARC (por ejemplo, el cliente de copia de seguridad puede ejecutarse dentro de las zonas no globales). Sin embargo, el cliente de copia de seguridad también se puede ejecutar en el host de Solaris y tomar instantáneas de las zonas no globales. A continuación, se puede hacer una copia de seguridad de las instantáneas en una cinta.

El siguiente ejemplo de configuración añade el sistema de archivos que aloja las zonas no globales de Solaris a la configuración de copia de seguridad del host de Solaris:

```
FileSet {
   Name = "Branded Zones"
   Include {
     Options {
       signature = MD5
     }
```

```
    File = /zones
  }
}
```

Conexiones

Para acceder al contenido adicional asociado a este documento, descomprima el archivo: attachment.zip

Realice copias de seguridad y archive datos en Amazon S3 con Veeam Backup & Replication

Creado por Jeanna James, Anthony Fiore (AWS) (AWS) y William Quigley

Entorno: producción	Tecnologías: Almacenamiento y copia de seguridad	Servicios de AWS: Amazon EC2; Amazon S3; Amazon S3 Glacier

Resumen

Este patrón detalla el proceso de envío de copias de seguridad creadas por Veeam Backup & Replication a las clases de almacenamiento de objetos compatibles con Amazon Simple Storage Service (Amazon S3) mediante la capacidad de repositorio de copias de seguridad escalable de Veeam.

Veeam admite múltiples clases de almacenamiento de Amazon S3 para adaptarse mejor a sus necesidades específicas. Puede elegir el tipo de almacenamiento en función del acceso a los datos, la resiliencia y los requisitos de costo de sus datos de copia de seguridad o archivado. Por ejemplo, puede almacenar los datos que no planea usar durante 30 días o más en Amazon S3 de acceso poco frecuente (IA) a un menor costo. Si planea archivar datos durante 90 días o más, puede utilizar Amazon Simple Storage Service Glacier (Amazon S3 Glacier) Flexible Retrieval o S3 Glacier Deep Archive con el nivel de archivado de Veeam. También puede usar el Bloqueo de objetos de S3 para hacer que las copias de seguridad sean inmutables en Amazon S3.

Este patrón no describe cómo configurar Veeam Backup & Replication con una puerta de enlace de cinta en AWS Storage Gateway. Para obtener información sobre este tema, consulte Veeam Backup & Replication using AWS VTL Gateway - Deployment Guide en el sitio web de Veeam.

> Advertencia: este escenario requiere que los usuarios de IAM tengan acceso programático y credenciales a largo plazo, lo que supone un riesgo para la seguridad. Para ayudar a mitigar este riesgo, le recomendamos que proporcione a estos usuarios únicamente los permisos que necesitan para realizar la tarea y que los elimine cuando ya no los necesiten. Las claves de acceso se pueden actualizar si es necesario. Para obtener más información, consulte Actualización de las claves de acceso en la Guía del usuario de IAM.

Requisitos previos y limitaciones

Requisitos previos

- Veeam Backup & Replication, que incluye Veeam Availability Suite o Veeam Backup Essentials, instalado (puede registrarse para obtener una prueba gratuita)
- Licencia Veeam Backup & Replication con funcionalidad Enterprise o Enterprise Plus, que incluye Veeam Universal License (VUL)
- Un usuario activo de AWS Identity and Access Management (IAM) con acceso a un bucket de Amazon S3
- Un usuario de IAM activo con acceso a Amazon Elastic Compute Cloud (Amazon EC2) y Amazon Virtual Private Cloud (Amazon VPC) (si utiliza el nivel de archivado)
- Conectividad de red desde las instalaciones a los servicios de AWS con ancho de banda disponible para realizar copias de seguridad y restaurar el tráfico a través de una conexión pública a Internet o una interfaz virtual pública (VIF) de AWS Direct Connect
- Se abrieron los siguientes puertos de red y puntos de conexión para garantizar una comunicación adecuada con los repositorios de almacenamiento de objetos:
  - Almacenamiento Amazon S3 — TCP — puerto 443: se utiliza para comunicarse con el almacenamiento de Amazon S3.
  - Almacenamiento de Amazon S3 (puntos de enlace en la nube): *.amazonaws.com para las regiones de AWS y las regiones de GovCloud AWS (EE. UU.), o *.amazonaws.com.cn para las regiones de China: se utiliza para comunicarse con el almacenamiento de Amazon S3. Para obtener una lista completa de los puntos de conexión de Amazon S3 en la documentación de AWS.
  - Almacenamiento en Amazon S3 — TCP HTTP — puerto 80: se utiliza para verificar el estado del certificado. Tenga en cuenta que los puntos de conexión de verificación de certificados: las URL de la lista de revocación de certificados (CRL) y los servidores del protocolo de estado de certificados en línea (OCSP) están sujetos a cambios. Encontrará la lista real de direcciones en el propio certificado.
  - Almacenamiento en Amazon S3: puntos de conexión de verificación de certificados: *.amazontrust.com: se utiliza para verificar el estado del certificado. Tenga en cuenta que los puntos de conexión de verificación de certificados (direcciones URL de CRL y servidores OCSP) están sujetos a cambios. Encontrará la lista real de direcciones en el propio certificado.

Limitaciones

- Veeam no admite las políticas de ciclo de vida de S3 en ningún bucket de S3 que se utilice como repositorio de almacenamiento de objetos de Veeam. Estas incluyen políticas con transiciones de clases de almacenamiento de Amazon S3 y reglas de caducidad del ciclo de vida de S3. Veeam debe ser la única entidad que administre estos objetos. La activación de las políticas de ciclo de vida de S3 puede tener resultados inesperados, incluida la pérdida de datos.

Versiones de producto

- Veeam Backup & Replication v9.5 Update 4 o posterior (solo nivel de copia de seguridad o de capacidad)
- Veeam Backup & Replication v10 o posterior (solo nivel de copia de seguridad o de capacidad y Bloqueo de objetos de S3)
- Veeam Backup & Replication v11 o posterior (copia de seguridad o nivel de capacidad, archivo o nivel de archivo y Bloqueo de objetos de S3)
- Veeam Backup & Replication v12 o posterior (nivel de rendimiento, copia de seguridad o nivel de capacidad, archivo o nivel de archivo y Bloqueo de objetos de S3)
- S3 Standard
- S3 Standard-IA
- S3 One Zone-IA
- S3 Glacier Flexible Retrieval (solo v11 y versiones posteriores)
- S3 Glacier Deep Archive (solo v11 y versiones posteriores)
- S3 Glacier Instant Retrieval (solo v12 y versiones posteriores)

Arquitectura

Pila de tecnología de origen

- Instalación en las instalaciones de Veeam Backup & Replication con conectividad desde un servidor de copia de seguridad de Veeam o un servidor gateway de Veeam a Amazon S3

Pila de tecnología de destino

- Amazon S3
- Amazon VPC y Amazon EC2 (si utiliza el nivel de archivado)

Arquitectura de destino: SOBR

El siguiente diagrama muestra la arquitectura del repositorio de copias de seguridad escalable horizontalmente (SOBR).

El software Veeam Backup and Replication protege los datos de errores lógicos, como fallas del sistema, errores de aplicaciones o eliminaciones accidentales. En este diagrama, las copias de seguridad se ejecutan primero en las instalaciones y una copia secundaria se envía directamente a Amazon S3. Una copia de seguridad representa una copia de los datos. point-in-time

El flujo de trabajo consta de tres componentes principales necesarios para organizar o copiar las copias de seguridad en Amazon S3 y un componente opcional:

- Veeam Backup & Replication (1): el servidor de copia de seguridad responsable de coordinar, controlar y administrar la infraestructura de respaldo, la configuración, los trabajos, las tareas de recuperación y otros procesos.
- Servidor de puerta de enlace Veeam (no se muestra en el diagrama): un servidor de puerta de enlace en las instalaciones opcional que se requiere si el servidor de respaldo de Veeam no tiene conectividad saliente con Amazon S3.
- Repositorio de copia de seguridad escalable horizontalmente (2): sistema de repositorio con soporte de escalado horizontal para el almacenamiento de datos en varios niveles. El repositorio de copias de seguridad escalable horizontalmente consta de uno o más repositorios de copias de seguridad que proporcionan un acceso rápido a los datos y se pueden ampliar con los repositorios de almacenamiento de objetos de Amazon S3 para el almacenamiento a largo plazo (nivel de capacidad) y el archivado (nivel de archivo). Veeam utiliza el repositorio de copia de seguridad escalable horizontalmente para organizar los datos automáticamente entre el almacenamiento de objetos local (nivel de rendimiento) y el almacenamiento de objetos de Amazon S3 (niveles de capacidad y archivo).
- Amazon S3 (3): servicio de almacenamiento de objetos de AWS que ofrece escalabilidad, disponibilidad de datos, seguridad y rendimiento.

Arquitectura de destino: DTO

El siguiente diagrama muestra la arquitectura direct-to-object (DTO).

En este diagrama, los datos de las copias de seguridad van directamente a Amazon S3 sin almacenarse primero en las instalaciones. Las copias secundarias se pueden almacenar en S3 Glacier.

Automatizar y escalar

Puede automatizar la creación de recursos de IAM y buckets de S3 mediante las CloudFormation plantillas de AWS que se proporcionan en el VeeamHub GitHub repositorio. Las plantillas incluyen opciones estándar e inmutables.

Herramientas

Herramientas y servicios de AWS

- Veeam Backup & Replication es una solución de Veeam para proteger, hacer copias de seguridad, replicar y restaurar sus cargas de trabajo físicas y virtuales.
- AWS le CloudFormation ayuda a modelar y configurar sus recursos de AWS, a aprovisionarlos de forma rápida y coherente y a gestionarlos durante todo su ciclo de vida. Facilita poder usar una plantilla para describir los recursos y sus dependencias, y lanzarlos y configurarlos juntos como una pila, en lugar de administrarlos de forma individual. Puede administrar y aprovisionar pilas en varias cuentas y regiones de AWS.
- Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable en la nube de AWS. Puede utilizar Amazon EC2 para lanzar tantos servidores virtuales como necesite, y puede escalar horizontalmente o reducir horizontalmente.
- AWS Identity and Access Management (IAM) es un servicio web para controlar el acceso seguro a los recursos de AWS. Con IAM, puede administrar de forma centralizada los usuarios, las credenciales de seguridad (como las claves de acceso) y los permisos que controlan a qué recursos y aplicaciones de AWS pueden obtener acceso los usuarios.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos. Puede utilizar Amazon S3 para almacenar y recuperar cualquier cantidad de datos en cualquier momento y desde cualquier parte de la web.
- Amazon S3 Glacier (S3 Glacier) es un servicio seguro y duradero para archivar datos a bajo costo y realizar copias de seguridad a largo plazo.
- Amazon Virtual Private Cloud (Amazon VPC) le permite aprovisionar una sección aislada de forma lógica de la nube de AWS donde puede lanzar recursos de AWS en una red virtual que haya definido. Dicha red virtual es prácticamente idéntica a las redes tradicionales que se utilizan en

sus propios centros de datos, con los beneficios que supone utilizar la infraestructura escalable de AWS.

Código

Utilice las CloudFormation plantillas incluidas en el VeeamHub GitHub repositorio para crear automáticamente los recursos de IAM y los depósitos de S3 para este patrón. Si prefiere crear estos recursos manualmente, siga los pasos de la sección Epics.

Prácticas recomendadas

- De acuerdo con las mejores prácticas de IAM, le recomendamos encarecidamente que cambie periódicamente las credenciales de usuario de IAM a largo plazo, como el usuario de IAM que utiliza para escribir copias de seguridad de Veeam Backup & Replication en Amazon S3. Para obtener más información, consulte Prácticas recomendadas de seguridad en la documentación de IAM.

Epics

Configurar el almacenamiento de Amazon S3 en su cuenta

Tarea	Descripción	Habilidades requeridas
Cree un usuario de IAM.	Siga las instrucciones de la documentación de IAM para crear un usuario de IAM. Este usuario no debe tener acceso a la consola de AWS y tendrá que crear una clave de acceso para este usuario. Veeam usa esta entidad para autenticarse con AWS para leer y escribir en sus buckets de S3. Debe conceder el privilegio mínimo (es decir, conceder solo los permisos necesarios para realizar una	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	tarea) para que el usuario no tenga más autoridad de la que necesita. Para ver, por ejemplo, las políticas de IAM que debe adjuntar a su usuario de Veeam IAM, consulte la sección Información adicional. Nota: Como alternativa, puede usar las CloudFormation plantillas proporcionadas en el VeeamHub GitHub repositorio para crear un usuario de IAM y un bucket de S3 para este patrón.	

Tarea	Descripción	Habilidades requeridas
Crear un bucket de S3.	1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/. 2. Si aún no tiene un bucket de S3 existente para usarlo como almacenamiento de destino, elija Crear bucket y especifique el nombre del bucket, la región de AWS y la configuración del bucket. • Le recomendamos que habilite la opción Bloquear el acceso público para el bucket de S3 y que configure las políticas de acceso y permisos de usuario para cumplir con los requisitos de su organización. Para ver un ejemplo, consulte la documentación de Amazon S3. • Le recomendamos que habilite Bloqueo de objetos de S3, incluso si no tiene intención de usarlo de inmediato. Esta configuración solo se puede habilitar en el momento de crear el bucket de S3.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	Para más información, consulte Crear un bucket en la documentación de Amazon S3.	

Añada Amazon S3 y S3 Glacier Flexible Retrieval (o S3 Glacier Deep Archive) a Veeam Backup & Replication

Tarea	Descripción	Habilidades requeridas
Inicie el asistente para el nuevo repositorio de objetos.	Antes de configurar el almacenamiento de objetos y los repositorios de copia de seguridad escalables horizontalmente en Veeam, debe añadir los repositorios de almacenamiento Amazon S3 y Amazon S3 Glacier que desee utilizar para los niveles de capacidad y archivo. En la próxima épica, conectará estos repositorios de almacenamiento a su repositorio copia de seguridad escalable horizontalmente. 1. En la consola de Veeam, abra la vista Infraestructura de copia de seguridad. 2. En el panel de inventario, elija el nodo Repositorios de copia de seguridad y, a continuación, elija Añadir repositorio.	Administrador de AWS, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	3. En el cuadro de diálogo Añadir repositorio de copia de seguridad, elija Almacenamiento de objetos, Amazon S3.	

Tarea	Descripción	Habilidades requeridas
Añada almacenamiento de Amazon S3 al nivel de capacidad.	1. En el cuadro de diálogo Amazon Cloud Storage Services, elija Amazon S3. 2. En el paso Nombre del asistente, especifique el nombre del almacenamiento del objeto y una breve descripción, como el creador y la fecha de creación. 3. En el paso Cuenta del asistente, especifique la cuenta de almacenamiento de objetos. • En Credenciales, elija el usuario de IAM que creó en la primera epopeya para acceder a su almacenamiento de objetos de Amazon S3. • Para Región de AWS, elija la región de AWS donde se encuentra el bucket de Amazon S3. 4. En el paso Bucket del asistente, especifique la configuración de almacenamiento de objetos. • En Región del centro de datos, elija la región de AWS donde está ubicado el bucket de Amazon S3.	Administrador de AWS, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	• Para Bucket, elija el bucket S3 que creó en la primera épica. • En Carpeta, cree o seleccione una carpeta en la nube a la que asignar su repositorio de almacenamiento de objetos. • Si quiere activar la inmutabilidad, seleccion e Hacer que las copias de seguridad recientes sean inmutables durante X días y establezca el período de tiempo durante el cual deben estar bloqueadas las copias de seguridad. Tenga en cuenta que habilitar la inmutabil idad se traduce en un aumento de los costos debido al aumento del número de llamadas a la API a Amazon S3 desde Veeam. 5. En el paso de resumen del asistente, revise la información de configura ción y, a continuación, seleccione Finalizar.	

Tarea	Descripción	Habilidades requeridas
Añada el almacenamiento de S3 Glacier al nivel de archivo.	Si desea crear un nivel de archivo, utilice los permisos de IAM que se detallan en la sección Información adicional. 1. Inicie el asistente para el nuevo repositorio de objetos tal y como se describió anteriormente. 2. En el cuadro de diálogo Amazon Cloud Storage Services, elija Amazon S3 Glacier. 3. En el paso Nombre del asistente, especifique el nombre del almacenam iento del objeto y una breve descripción, como el creador y la fecha de creación. 4. En el paso Cuenta del asistente, especifique la cuenta de almacenamiento de objetos. • En Credenciales, elija el usuario de IAM que creó en la primera épica para acceder a su almacenam iento de objetos de Amazon S3 Glacier. • Para Región de AWS, elija la región de AWS donde se encuentra el bucket de Amazon S3.	Administrador de AWS, propietario de la aplicación

Tarea	Descripción	Habilidades requeridas
	5. En el paso Bucket del asistente, especifiq ue la configuración de almacenamiento de objetos. • En Región del centro de datos, elija la región de AWS. • En Bucket, elija un bucket S3 para almacenar los datos de copia de seguridad. Puede ser el mismo bucket que utilizó para el nivel de capacidad. • En Carpeta, cree o seleccione una carpeta en la nube a la que asignar su repositorio de almacenamiento de objetos. • Si quiere habilitar la inmutabilidad, seleccione Hacer que las copias de seguridad recientes sean inmutables durante toda su política de retención . Tenga en cuenta que habilitar la inmutabil idad se traduce en un aumento de los costos debido al aumento del número de llamadas a la API a Amazon S3 desde Veeam.	

Tarea	Descripción	Habilidades requeridas
	• Si quiere usar S3 Glacier Deep Archive como clase de almacenamiento de archivos, elija Usar la clase de almacenamiento Deep Archive. 6. En el paso Dispositivo proxy del asistente, configure la instancia auxiliar que se utiliza para transferir los datos de Amazon S3 a Amazon S3 Glacier. Puede usar la configuración predeterminada o configurar cada configuración manualmente. Para configurar los ajustes manualmente: • Elija Personalizar. • En Tipo de instancia EC2, elija el tipo de instancia para el dispositivo proxy en función de sus requisitos de velocidad y coste para transferir los archivos de copia de seguridad al nivel de archivado de su repositorio de copia de seguridad escalable horizontalmente. • En Amazon VPC, elija la VPC de la instancia de destino.	

Tarea	Descripción	Habilidades requeridas
	• En Subredes, elija la subred del dispositivo proxy. • Para Grupos de seguridad, elija el grupo de seguridad que desea asociar al dispositivo proxy. • En Puerto redirector, especifique el puerto TCP para enrutar las solicitud es entre el dispositivo proxy y los componentes de la infraestructura de copia de seguridad. • Elija Aceptar para confirmar la configura ción. 7. En el paso de resumen del asistente, revise la información de configura ción y, a continuación, seleccione Finalizar.	

Añadir repositorios de copia de seguridad escalables horizontalmente

Tarea	Descripción	Habilidades requeridas
Inicie el asistente de nuevo repositorio de copia de seguridad escalable horizonta lmente.	1. En la consola de Veeam, abra la vista Infraestructura de copia de seguridad. 2. En el panel de inventario, seleccione Repositorios	Propietario de la aplicación, administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	de escalado horizontal y, a continuación, seleccione Añadir repositorio de escalado horizontal.	

Tarea	Descripción	Habilidades requeridas
Añada un repositorio de copias de seguridad escalable horizontalmente y configure los niveles de capacidad y archivo.	1. En el paso Nombre del asistente, especifique el nombre y una breve descripción del repositor io de copias de seguridad escalable horizontalmente. 2. Si es necesario, añada extensiones de rendimien to. También puede utilizar su repositorio de backup local de Veeam existente como nivel de rendimiento. A partir de la versión 12 de Veeam, puede añadir un bucket de S3 como medida de rendimiento para los backups direct-to-object (DTO), sin tener en cuenta el nivel de rendimiento local. 3. Elija Avanzado y especifiq ue opciones adicional es para el repositorio de copias de seguridad escalable horizontalmente. • Seleccione Utilizar archivos de copia de seguridad por máquina para crear un archivo de copia de seguridad independiente para cada máquina y escribir estos archivos en el repositorio de copias	Propietario de la aplicación, administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	de seguridad en varios flujos de forma simultáne a. Se recomienda esta opción para una mejor utilización de los recursos de almacenamiento y procesamiento. • Seleccione Realizar una copia de seguridad completa cuando la extensión requerida esté desconectada para crear un archivo de copia de seguridad completo en caso de que una extensión que contiene puntos de restaurac ión para una copia de seguridad incremental quede sin conexión. Esta opción requiere espacio libre en el repositorio de copias de seguridad ampliable para alojar un archivo de copia de seguridad completo. 4. En el paso de políticas del asistente, especifique la política de ubicación de las copias de seguridad para el repositorio. • Elija la localidad de datos para almacenar juntos los archivos de copia	

Tarea	Descripción	Habilidades requeridas
	de seguridad completos e incrementales que pertenezcan a la misma cadena y con el mismo grado de rendimiento. Puede almacenar los archivos que pertenece n a una nueva cadena de copia de seguridad en el mismo nivel de rendimiento o en otro (a menos que utilice un dispositivo de almacenam iento deduplicado como medida de rendimiento). • Elija Rendimiento para almacenar archivos de copia de seguridad completos e increment ales con distintos niveles de rendimiento. Esta opción requiere una conexión de red rápida y fiable. Si elige Rendimien to, puede restringir los tipos de archivos de copia de seguridad que desea almacenar en cada nivel de rendimien to. Por ejemplo, puede almacenar archivos de copia de seguridad completos en una extensión y archivos de copia de seguridad	

Tarea	Descripción	Habilidades requeridas
	incrementales en otras extensiones. Para elegir los tipos de archivos: • Elija Personalizar. • En el cuadro de diálogo Configuración de ubicación de copias de seguridad, elija una extensión de rendimien to y, a continuación, elija Editar. • Elija el tipo de archivos de copia de seguridad que desee almacenar en la extensión. 5. En el paso Nivel de capacidad del asistente , configure el nivel de almacenamiento a largo plazo que desea adjuntar al repositorio de copias de seguridad escalable horizontalmente. • Elija Ampliar la capacidad del repositorio de copias de seguridad escalable horizontalmente con almacenamiento de objetos. Para el repositor io de almacenamiento de objetos, elija el almacenamiento de Amazon S3 para el nivel	

Tarea	Descripción	Habilidades requeridas
	de capacidad que agregó en la épica anterior. • Elija Ventana para seleccionar una ventana de tiempo para mover o copiar datos. • Seleccione Copiar las copias de seguridad en el almacenamiento de objetos tan pronto como se creen para copiar todos los archivos de copia de seguridad creados recientemente o solo en la medida de su capacidad. • Seleccione Mover las copias de seguridad al almacenamiento de objetos a medida que pasen del período de restauraciones operativa s para transferir las cadenas de copias de seguridad inactivas en la medida de su capacidad. En el campo Mover archivos de copia de seguridad con una antigüedad superior a X días, especifique la duración a partir de la cual deben descargar se los archivos de copia	

Tarea	Descripción	Habilidades requeridas
	de seguridad. (Para eliminar las cadenas de copia de seguridad inactivas el día en que se crearon, especifique 0 días). También puede elegir Anular para mover los archivos de copia de seguridad antes, si el repositorio de copias de seguridad escalable horizontalmente ha alcanzado el umbral que ha especificado. • Elija Cifrar los datos cargados en el almacenamiento de objetos y especifique una contraseña para cifrar todos los datos y sus metadatos para su descarga. Elija Agregar o Gestionar contraseñ as para especificar una nueva contraseña 6. En el paso Nivel de capacidad del asistente , configure el nivel de almacenamiento a largo plazo que desea adjuntar al repositorio de copias de seguridad escalable horizontalmente. (Este paso no aparece si omitió	

Tarea	Descripción	Habilidades requeridas
	añadir almacenamiento en Amazon S3 Glacier). • Elija Archivar las copias de seguridad completas de GFS en el almacenamiento de objetos. Para el repositorio de almacenamiento de objetos, elija el almacenamiento de Amazon S3 Glacier que añadió en la épica anterior. • En Copias de seguridad de Archive GFS que tengan más de N días, elija un intervalo de tiempo para mover los archivos a la extensión de archivado. (Para archivar las cadenas de copias de seguridad inactivas el día en que se crearon, especifique 0 días). 7. En el paso de Resumen del asistente, revise la configuración del repositorio de copias de seguridad escalable horizontalmente y, a continuación, seleccione Finalizar.	

Recursos relacionados

- Crear un usuario de IAM en la cuenta de AWS (documentación de IAM)
- Creación de un bucket (documentación de Amazon S3)
- Bloquear el acceso público al almacenamiento de Amazon S3 (documentación de Amazon S3)
- Uso del Bloqueo de objetos de S3 (documentación de Amazon S3)
- Documentación técnica de Veeam
- Cómo crear una política de IAM segura para la conexión a S3 Object Storage (documentación de Veeam)

Información adicional

Las siguientes secciones proporcionan ejemplos de políticas de IAM que puede utilizar al crear un usuario de IAM en la sección Epics de este patrón.

Política de IAM para el nivel de capacidad

Nota: cambie el nombre de los depósitos de S3 en la política de ejemplo por el nombre del `<yourbucketname>` depósito de S3 que desee utilizar para los respaldos de los niveles de capacidad de Veeam.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:GetObjectVersion",
                "s3:ListBucketVersions",
                "s3:ListBucket",
                "s3:PutObjectLegalHold",
                "s3:GetBucketVersioning",
                "s3:GetObjectLegalHold",
                "s3:GetBucketObjectLockConfiguration",
                "s3:PutObject*",
                "s3:GetObject*",
                "s3:GetEncryptionConfiguration",
                "s3:PutObjectRetention",
```

```
                "s3:PutBucketObjectLockConfiguration",
                "s3:DeleteObject*",
                "s3:DeleteObjectVersion",
                "s3:GetBucketLocation"

            ],
            "Resource": [
                "arn:aws:s3:::/*",
                "arn:aws:s3:::"
            ]
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:ListBucket"
            ],
            "Resource": "*"
        }
    ]
}
```

Política de IAM para el nivel de archivo

Nota: cambie el nombre de los buckets de S3 en la política de ejemplo de `<yourbucketname>` al nombre del bucket de S3 que desee utilizar para las copias de seguridad del nivel de archivo de Veeam.

Para usar su VPC, subred y grupos de seguridad existentes:

```
  {
    "Version": "2012-10-17",
    "Statement": [
      {
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": [
          "s3:DeleteObject",
          "s3:PutObject",
          "s3:GetObject",
          "s3:RestoreObject",
          "s3:ListBucket",
```

```
        "s3:AbortMultipartUpload",
        "s3:GetBucketVersioning",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation",
        "s3:GetBucketObjectLockConfiguration",
        "s3:PutObjectRetention",
        "s3:GetObjectVersion",
        "s3:PutObjectLegalHold",
        "s3:GetObjectRetention",
        "s3:DeleteObjectVersion",
        "s3:ListBucketVersions",
        "ec2:DescribeInstances",
        "ec2:CreateKeyPair",
        "ec2:DescribeKeyPairs",
        "ec2:RunInstances",
        "ec2:DeleteKeyPair",
        "ec2:DescribeVpcAttribute",
        "ec2:CreateTags",
        "ec2:DescribeSubnets",
        "ec2:TerminateInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeVpcs"
      ],
      "Resource": "*"
    }
  ]
}
```

Para crear nuevos grupos de VPC, subred y grupos de seguridad:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteObject",
        "s3:PutObject",
        "s3:GetObject",
        "s3:RestoreObject",
        "s3:ListBucket",
```

```
          "s3:AbortMultipartUpload",
          "s3:GetBucketVersioning",
          "s3:ListAllMyBuckets",
          "s3:GetBucketLocation",
          "s3:GetBucketObjectLockConfiguration",
          "s3:PutObjectRetention",
          "s3:GetObjectVersion",
          "s3:PutObjectLegalHold",
          "s3:GetObjectRetention",
          "s3:DeleteObjectVersion",
          "s3:ListBucketVersions",
          "ec2:DescribeInstances",
          "ec2:CreateKeyPair",
          "ec2:DescribeKeyPairs",
          "ec2:RunInstances",
          "ec2:DeleteKeyPair",
          "ec2:DescribeVpcAttribute",
          "ec2:CreateTags",
          "ec2:DescribeSubnets",
          "ec2:TerminateInstances",
          "ec2:DescribeSecurityGroups",
          "ec2:DescribeImages",
          "ec2:DescribeVpcs",
          "ec2:CreateVpc",
          "ec2:CreateSubnet",
          "ec2:DescribeAvailabilityZones",
          "ec2:CreateRoute",
          "ec2:CreateInternetGateway",
          "ec2:AttachInternetGateway",
          "ec2:ModifyVpcAttribute",
          "ec2:CreateSecurityGroup",
          "ec2:DeleteSecurityGroup",
          "ec2:AuthorizeSecurityGroupIngress",
          "ec2:AuthorizeSecurityGroupEgress",
          "ec2:DescribeRouteTables",
          "ec2:DescribeInstanceTypes"
        ],
        "Resource": "*"
      }
    ]
}
```

Configurar Veritas NetBackup para VMware Cloud on AWS

Creado por Shubham Salani (AWS)

Entorno: producción	Tecnologías: almacenamiento y copia de seguridad; nativas en la nube	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: Amazon S3; AWS Transit Gateway; Amazon VPC; Amazon EBS		

Resumen

> Aviso: A partir del 30 de abril de 2024, AWS o sus socios de canal ya no revenden VMware Cloud on AWS. El servicio seguirá estando disponible a través de Broadcom. Le recomendamos que se ponga en contacto con su representante de AWS para obtener más información.

Muchas empresas utilizan Veritas NetBackup como solución de respaldo y recuperación para sus cargas de trabajo locales basadas en VMware vSphere. Una vez que las empresas migran sus cargas de trabajo a centros de datos definidos por software (SDDC) en la infraestructura de VMware Cloud on Amazon Web Services (AWS), no existe un procedimiento claro de integración. lift-and-shift NetBackup Este patrón describe cómo puede configurar Veritas NetBackup en su cuenta de AWS y configurarla para hacer copias de seguridad de las cargas de trabajo en sus SDDC de VMware.

Este patrón no incluye instrucciones para migrar las cargas de trabajo. Para mayor información, consulte migre VMware SDDC a VMware Cloud en AWS mediante VMware HCX. Al configurar sus cargas de trabajo en VMware Cloud en AWS, use un clúster ampliado (documentación de VMware). En esta configuración, el clúster abarca dos zonas de disponibilidad de AWS en una única región. Esto proporciona una alta disponibilidad y resiliencia en caso de que una de las zonas de disponibilidad se interrumpa. Elastic DRS y un host testigo de vSAN (documentación de VMware) copian los datos con fluidez a una tercera zona de disponibilidad, conocida como dominio de errores. Esta solución de paridad puede ayudarle a recuperar los datos si se produce un fallo. Como este enfoque requiere tres zonas de disponibilidad, al seleccionar una región de AWS para su entorno

de VMware Cloud, asegúrese de tener tres o más zonas de disponibilidad. Para obtener más información, consulte Regiones y zonas de disponibilidad.

En este patrón, cada SDDC tiene un servidor proxy como host de respaldo. Con las instancias de Amazon Elastic Compute Cloud (Amazon EC2), se configuran NetBackup los servidores principal y multimedia en una nube privada virtual (VPC) independiente, una para cada SDDC. Como las interfaces de red elásticas proporcionan un gran ancho de banda y una baja latencia, se utilizan para configurar la conectividad entre los hosts de respaldo y sus servidores principales y multimedia correspondientes NetBackup . Las instancias de EC2 dirigen las copias de seguridad a los volúmenes de Amazon Elastic Block Store (Amazon EBS), que es el primer punto de copia de seguridad. Puede usar AWS DataSync para mantener sincronizados los volúmenes de EBS para los SDDC.

También puede usar AWS Transit Gateway y un punto de conexión de VPC para conectar los volúmenes de EBS a otro servicio de almacenamiento, como Amazon Simple Storage Service (Amazon S3). Según su política de retención, puede usar las clases de almacenamiento S3 Glacier de S3 Intelligent-Tiering para optimizar sus costos de almacenamiento. Para obtener más información, consulte Uso de clases de almacenamiento de Amazon S3 (documentación de Amazon S3).

Requisitos previos y limitaciones

Requisitos previos

- Su entorno de VMware Cloud en AWS usa un clúster ampliado que abarca dos zonas de disponibilidad.
- El host de respaldo debe residir en el SDDC de VMware Cloud en AWS, con acceso al almacén de datos donde se implementan los archivos de VMware Virtual Machine Disk File (VMDK).
- HotAdd El modo de transporte debe estar habilitado en el NetBackup cliente para realizar copias de seguridad y restaurar las máquinas virtuales (VM), y debe permitir la restauración desde archivos y carpetas dirigidos por el usuario.

Limitaciones

- El servidor NetBackup maestro debe usar la resolución de DNS en una dirección IP privada para el host de respaldo de vCenter en el SDDC.
- Los archivos de hosts del servidor NetBackup maestro y del host de respaldo deben contener lo siguiente:

  - La dirección IP privada y el nombre de DNS privado del servidor maestro
  - La dirección IP privada y el nombre de DNS privado del host de respaldo
- Si está configurando los puntos de conexión de VPC de la interfaz en un bucket de S3, el firewall Compute Gateway del SDDC debe configurarse para permitir HTTPS desde un origen de bloques de enrutamiento entre dominios sin clases (CIDR). Para obtener más información, consulte Acceder a un bucket de S3 mediante un punto de conexión de S3 (documentación de VMware).
- VMware Cloud on AWS no admite las siguientes funciones de NetBackup:
  - Realizar copias de seguridad o restaurar plantillas de máquinas virtuales
  - Uso de NetBackup vSphere Client (complemento HTML5)
  - Bloquear y desbloquear máquinas virtuales para realizar copias de seguridad o restauraciones
  - Las copias de seguridad no se pueden almacenar en un almacén de datos de vSAN
  - Modos de transporte de dispositivo de bloques de red (NBD), NBDSSL y SAN

Versiones de producto

- SDDC de VMware Cloud en AWS versión 1.0 o posterior
- Veritas, NetBackup versión 8.1.2 o posterior
- Versión 6.8 o posterior de Linux
- VMware vSphere versión 6.0 o posterior

Arquitectura

En el siguiente diagrama se muestra la configuración NetBackup de VMware Cloud on AWS. El servidor NetBackup principal y el servidor multimedia se implementan en una VPC independiente y se conectan a los hosts de respaldo de los SDDC mediante interfaces de red elásticas. El servidor NetBackup principal y el servidor multimedia almacenan las copias de seguridad en los volúmenes de Amazon EBS. Si lo desea, puede configurar almacenamiento adicional en los buckets de Amazon S3 mediante AWS Transit Gateway y un punto de enlace de VPC con PrivateLink interfaz de AWS.

Herramientas

Servicios y herramientas de AWS

- Amazon Elastic Block Store (Amazon EBS) proporciona volúmenes de almacenamiento por bloques para su uso con instancias de Amazon Elastic Compute Cloud (Amazon EC2).
- AWS le PrivateLink ayuda a crear conexiones unidireccionales y privadas desde sus nubes privadas virtuales (VPC) a servicios externos a la VPC.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esta red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Otros servicios

- VMware Cloud en AWS es una oferta de nube integrada desarrollada conjuntamente por Amazon Web Services (AWS) y VMware.
- NetBackup para VMware, realiza copias de seguridad y restaura las máquinas virtuales de VMware que se ejecutan en los hosts ESXi de VMware.

Epics

Configure los servidores NetBackup

Tarea	Descripción	Habilidades requeridas
Actualice las reglas del firewall.	Actualice las reglas del firewall para establecer la conectividad entre el SDDC de VMware Cloud on AWS y los servidores NetBackup principales y multimedia. Haga lo siguiente: 1. Inicie sesión en VMware Cloud en AWS en https://vmc.vmware.com/	Administrador de red, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	2. En la pestaña Redes y seguridad, seleccione Gateway Firewall. 3. En la página Gateway Firewall, seleccione Compute Gateway. 4. Seleccione AGREGAR regla y, a continuación, cree una nueva regla con la configuración de puerto de firewall necesaria. Para obtener más información, consulte los requisitos de los puertos del NetBackup firewall (documentación de Veritas).	

Tarea	Descripción	Habilidades requeridas
Inicie el servidor NetBackup principal y el servidor multimedia.	1. Inicie sesión en la consola de administración de AWS y abra la consola EC2 en https://console.aws.amazon.com/ec2/ 2. Lance una instancia EC2 (documentación de Amazon EC2) e introduzca los siguientes detalles de configuración: a. Para los servidores NetBackup maestro y multimedia, seleccione `NBU-Linux-GA-8-1-2-Setup-f032d23e-881b-4dee-ba70-b9ca3e915910-ami-072509a7ffc156938.4` Amazon Machine Image (AMI). Esta AMI preconfigurada está disponible en AWS Marketplace. b. Seleccione un tipo de instancia. NetBackup recomendado `m5.2xlarge` para el servidor principal y el servidor multimedia.	Administrador de la nube, administrador de copia de seguridad

Tarea	Descripción	Habilidades requeridas
Configure el host de respaldo para NetBackup.	1. Inicie sesión en VMware Cloud en AWS en https://vmc.vmware.com/ 2. Seleccione el SDDC. 3. Seleccione la pestaña Abrir VCENTER. Se abrirá el vCenter del SDDC. 4. Anote el nombre completo del dominio (FQDN) del host de respaldo. 5. Inicie sesión en la consola NetBackup de administración. Para obtener más información, consulte Inicio de sesión en la consola de NetBackup administración (documentación de Veritas). 6. Seleccione el servidor principal y el servidor multimedia y, a continuación, elija Hosts de acceso de VMware. 7. Agregue el FQDN del host de respaldo. 8. Seleccione Aplicar y, después, Aceptar.	Administrador de la nube, administrador de copia de seguridad

(opcional) Configure el almacenamiento de Amazon S3

Tarea	Descripción	Habilidades requeridas
Configure el almacenamiento en Amazon S3.	1. Revise las Opciones de almacenamiento en	Administrador de la nube, General AWS

Tarea	Descripción	Habilidades requeridas
	la nube de Amazon S3 (documentación de Veritas) y seleccione la clase de almacenamiento adecuada según sus necesidades. 2. Configure NetBackup para usar Amazon S3 para el almacenamiento en la nube según las instrucciones de Configuración del almacenamiento en la nube en NetBackup (documentación de Veritas).	

Recursos relacionados

Documentación de AWS

- Creación de un punto final de VPC de interfaz (documentación de AWS PrivateLink)

Documentación de Veritas

- NetBackup requisitos de puerto de firewall

Documentación de VMware

- Implemente una máquina virtual a partir de una plantilla de OVF en una biblioteca de contenido
- Cargos por transferencia de datos de VMware Cloud en AWS: ¿cómo funcionan? (publicación del blog de VMware)
- VMware Cloud en AWS: clústeres ampliados

Copiar datos de un bucket de S3 a otra cuenta y región mediante la AWS CLI

Creado por Appasaheb Bagali (AWS) y Purushotham G K (AWS)

Entorno: producción	Tecnologías: almacenamiento y copia de seguridad; nativas en la nube	Servicios de AWS: AWS CLI; AWS Identity and Access Management; Amazon S3

Resumen

Este patrón describe cómo migrar datos de un depósito de Amazon Simple Storage Service (Amazon S3) de una cuenta de origen de AWS a un depósito de S3 de destino de otra cuenta de AWS, ya sea en la misma región de AWS o en una región diferente.

El bucket de S3 de origen permite el acceso de AWS Identity and Access Management (IAM) mediante una política de recursos adjunta. Un usuario de la cuenta de destino debe asumir un rol que tenga permisos `PutObject` y `GetObject`para el bucket de origen. Por último, se ejecutan comandos `copy` y `sync` para transferir los datos del depósito de S3 de origen al depósito de S3 de destino.

Las cuentas son propietarias de los objetos que cargan en los buckets de S3. Si copia objetos entre cuentas y regiones, otorga a la cuenta de destino la propiedad de los objetos copiados. Para cambiar la propiedad de un objeto, cambie su lista de control de acceso (ACL) a `bucket-owner-full-control`. Sin embargo, le recomendamos que conceda permisos programáticos para varias cuentas a la cuenta de destino, ya que las ACL pueden ser difíciles de administrar para varios objetos.

Advertencia: este escenario requiere que los usuarios de IAM dispongan de acceso programát ico y credenciales de larga duración, lo que supone un riesgo para la seguridad. Para ayudar a mitigar este riesgo, le recomendamos que brinde a estos usuarios únicamente los permisos que necesitan para realizar la tarea y que los elimine cuando ya no los necesiten. Las claves de acceso se pueden actualizar si es necesario. Para obtener más información, consulte Actualiza ción de claves de acceso en la Guía de usuario de IAM.

Este patrón cubre la migración única. Para los escenarios que requieren una migración continua y automática de nuevos objetos de un bucket de origen a un bucket de destino, puede utilizar la replicación por lotes de S3 en su lugar, tal como se describe en el patrón Copiar datos de un bucket de S3 a otra cuenta y región mediante la replicación por lotes de S3.

Requisitos previos y limitaciones

- Dos cuentas de AWS activas en las mismas o diferentes regiones de AWS.
- Un bucket de S3 existente en la cuenta de origen.
- Si el bucket de Amazon S3 de origen o destino tiene activo el cifrado por defecto, debe modificar los permisos de clave de AWS Key Management Service (AWS KMS). Para obtener más información, consulte el artículo de AWS Re:post sobre este tema.
- Familiaridad con los permisos entre cuentas.

Arquitectura

Herramientas

- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta de código abierto que permite interactuar con los servicios de AWS mediante comandos en el intérprete de comandos de línea de comandos.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.

Prácticas recomendadas

- Prácticas recomendadas de seguridad en IAM (documentación de IAM)
- Aplicar permisos con privilegios mínimos (documentación de IAM)

Epics

Cree un usuario y un rol de IAM en la cuenta de AWS de destino

Tarea	Descripción	Habilidades requeridas
Crear un usuario de IAM para conseguir la clave de acceso.	1. Inicie sesión en la consola de administración de AWS y cree un usuario de IAM que tenga acceso mediante programación. Para ver los pasos detallados, consulte Crear usuarios de IAM en la documentación de IAM. No es necesario adjuntar ninguna política para este usuario. 2. Genere una clave de acceso y una clave secreta para este usuario. Para obtener instrucciones, consulte la cuenta y las claves de acceso de AWS en la documentación de AWS.	AWS DevOps
Crear una política de IAM basada en identidades.	Cree una política basada en la identidad de IAM denominada `S3MigrationPolicy` mediante los siguientes permisos. Para obtener más información, consulte Creación de políticas de IAM en la documentación de IAM. `{`	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	"Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["s3:ListBucket", "s3:GetObject", "s3:GetObjectTagging", "s3:GetObjectVersion", "s3:GetObjectVersionTagging"], "Resource": ["arn:aws:s3:::awsexamplesourcebucket", "arn:aws:s3:::awsexamplesourcebucket/*"] }, { "Effect": "Allow", "Action": ["s3:ListBucket", "s3:PutObject", "s3:PutObjectAcl",	

Tarea	Descripción	Habilidades requeridas
	<pre>"s3:PutObjectTaggi ng", "s3:GetObjectTaggi ng", "s3:GetObjectVersi on", "s3:GetObjectVersi onTagging"], "Resource": ["arn:aws:s3:::awse xampledestinationb ucket", "arn:aws:s3:::awse xampledestinationb ucket/*"] }] }</pre> Nota: Modifique los nombres de los buckets de origen y destino según su caso de uso. Esta política basada en la identidad permite al usuario que asume esta función acceder al depósito de origen y al depósito de destino.	

Tarea	Descripción	Habilidades requeridas
Crear un rol de IAM.	Cree un rol de IAM denominado `S3MigrationRole` mediante la siguiente política de confianza y luego adjunte la creada anteriormente `S3MigrationPolicy` . Para conocer los pasos detallados, consulte Crear una función para delegar permisos a un usuario de IAM en la documentación de IAM. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": "arn:aws:iam::<destination_account>:user/<user_name>" }, "Action": "sts:AssumeRole", "Condition": {} } ] }` Nota: Modifique el nombre de recurso de Amazon (ARN) del nombre de usuario o rol de IAM de destino en la política	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	de confianza según su caso de uso. Esta política de confianza permite que el recién creado usuario de IAM asuma `S3MigrationRole` .	

Crear y adjuntar la política de bucket de S3 en la cuenta de origen

Tarea	Descripción	Habilidades requeridas
Crear y adjuntar una política de bucket de S3.	Inicie sesión en la Consola de administración de AWS de su organización y abra la consola de Amazon S3. Seleccione su bucket de S3 de origen y luego, Permisos. En Política de bucket, seleccione Editar y luego pegue la siguiente política de bucket. Seleccione Guardar. `{ "Version": "2012-10-17", "Statement": [ { "Sid": "DelegateS3Access", "Effect": "Allow", "Principal": {"AWS": "arn:aws:iam::<destination_account>:role/<RoleName>"},`	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	<pre>"Action": ["s3:ListBucket", "s3:GetObject", "s3:GetObjectTagging", "s3:GetObjectVersion", "s3:GetObjectVersionTagging"], "Resource": ["arn:aws:s3:::awsexamplesourcebucket/*", "arn:aws:s3:::awsexamplesourcebucket"] }] }</pre> Nota: Asegúrese de incluir el ID de cuenta de AWS de la cuenta de destino y configure la plantilla de política de bucket de acuerdo con sus requisitos. Esta política basada en recursos permite que el rol de destino `S3MigrationRole`	

Tarea	Descripción	Habilidades requeridas
	acceda a los objetos de S3 de la cuenta de origen.	

Configure el bucket de S3 de destino

Tarea	Descripción	Habilidades requeridas
Crear el bucket de S3 de destino.	Inicie sesión en la consola de administración de AWS de su cuenta de destino, abra la consola de Amazon S3 y, a continuación, elija Crear bucket. Cree un bucket de S3 según sus necesidades. Para obtener más información, consulte Crear un bucket en la documentación de Amazon S3.	Administrador de la nube

Copiar los datos al bucket de S3 de destino

Tarea	Descripción	Habilidades requeridas
Configure la AWS CLI con las credenciales de usuario recién creadas.	1. Instale la versión más reciente de AWS CLI. Para obtener instrucciones, consulte Instalación o actualización de la última versión de AWS CLI en la documentación de la CLI de AWS. 2. Ejecute `$ aws configure` y actualice	AWS DevOps

Tarea	Descripción	Habilidades requeridas
	la CLI con la clave de acceso de AWS del usuario que creó. Para obtener más información, consulte Configuración y ajustes de archivos de credenciales en la documentación de la CLI de AWS.	

Tarea	Descripción	Habilidades requeridas
Asuma la función de migración a S3.	1. Utilice la CLI de AWS para asumir `S3MigrationRole` : `aws sts assume-role \ --role-arn "arn:aws:iam::<destination_account>:role/S3MigrationRole" \ --role-session-name AWSCLI-Session` Este comando genera varios datos. Dentro del bloque de credenciales, necesita las `AccessKeyId` , `SecretAccessKey` , y `SessionToken` . En este ejemplo se utilizan las variables de entorno `RoleAccessKeyID` , `RoleSecretKey` , y `RoleSessionToken` . Tenga en cuenta que la marca de tiempo del campo de caducidad está en la zona horaria UTC. La marca de tiempo indica cuándo caducan las credenciales temporales del rol de IAM. Si las credencia les temporales caducan, debes volver a llamar a	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	la API de `sts:AssumeRole` . 2. Cree tres variables de entorno para asumir el rol de IAM. Estas variables de entorno se rellenan con el siguiente resultado: `# Linux` `export AWS_ACCESS_KEY_ID=RoleAccessKeyID` `export AWS_SECRET_ACCESS_KEY=RoleSecretKey` `export AWS_SESSION_TOKEN=RoleSessionToken` `# Windows` `set AWS_ACCESS_KEY_ID=RoleAccessKeyID` `set AWS_SECRET_ACCESS_KEY=RoleSecretKey` `set AWS_SESSION_TOKEN=RoleSessionToken` 3. Verifique que ha asumido el rol de IAM mediante la ejecución del siguiente comando: `aws sts get-caller-identity`	

Tarea	Descripción	Habilidades requeridas
	Para obtener más información, consulte el Centro de conocimientos de AWS.	

Tarea	Descripción	Habilidades requeridas
Copie y sincronice los datos del bucket de S3 de origen al bucket de S3 de destino.	Cuando haya asumido el rol `S3MigrationRole` , podrá copiar los datos mediante el comando copiar (cp) o sincronizar (sync). Copiar (consulte la referencia de comandos de AWS CLI para obtener más detalles): `aws s3 cp s3:// DOC-EXAMPLE-BUCKET-SOURCE / \` `    s3:// DOC-EXAMPLE-BUCKET-TARGET / \` `    --recursive --source-region SOURCE-REGION-NAME --region  DESTINATION-REGION-NAME` Sincronizar (consulte la referencia de comandos de AWS CLI para obtener más detalles): `aws s3 sync s3://  DOC-EXAMPLE-BUCKET-SOURCE / \` `    s3:// DOC-EXAMPLE-BUCKET-TARGET / \` `    --source-region  SOURCE-REGION-NAME  --region DESTINATION-REGION-NAME`	Administrador de la nube

Resolución de problemas

Problema	Solución
Se ha producido un error (`AccessDenied `) al llamar a la operación `ListObjects` : Acceso denegado	• Asegúrese de haber asumido el rol `S3MigrationRole` . • Ejecute `aws sts get-caller-identit` y para comprobar el rol utilizado. Si el resultado no muestra el ARN de `S3Migrati onRole` , vuelva a asumir la función y vuelva a intentarlo.

Recursos relacionados

- Creación de un bucket de S3 (documentación de Amazon S3)
- Políticas de bucket y políticas de usuario de Amazon S3 (documentación de Amazon S3)
- Identidades de IAM (usuarios, grupos y roles) (documentación de IAM)
- comando cp (documentación de la AWS CLI)
- comando sync (documentación de la AWS CLI)

Copie datos de un bucket de S3 a otra cuenta y región mediante S3 Batch Replication

Creado por Appasaheb Bagali (AWS), Lakshmikanth B D (AWS), Purushotham G K (AWS), Shubham Harsora (AWS) y Suman Rajotia (AWS)

Entorno: PoC o piloto	Tecnologías: almacenamiento y copia de seguridad; nativas en la nube	Servicios de AWS: Amazon S3; AWS Identity and Access Management

Resumen

Este patrón explica cómo puede utilizar la replicación por lotes de Amazon Simple Storage Service (Amazon S3) para copiar el contenido de un bucket de S3 a otro bucket de S3 automáticamente, sin ninguna intervención manual, después de configurar los cubos. Los depósitos de origen y destino pueden estar en la misma región o en regiones diferentes Cuentas de AWS .

La replicación por lotes de S3 le permite replicar objetos de Amazon S3 que existían antes de que se implementara una configuración de replicación, objetos que se replicaron anteriormente y objetos que no se pudieron replicar. Este método utiliza un trabajo de S3 Batch Operations. Cuando finalice el trabajo, recibirá un informe de finalización.

Puede usar S3 Batch Replication en escenarios que requieran una migración continua y automática de nuevos objetos de un bucket de origen a un bucket de destino. Si se trata de una migración única, puede utilizar AWS Command Line Interface (AWS CLI) en su lugar, tal y como se describe en el patrón Copie los datos de un bucket de S3 a otra cuenta o región mediante el AWS CLI.

Requisitos previos y limitaciones

- Una fuente Cuenta de AWS.
- Un destino Cuenta de AWS.
- Un depósito de S3 en la cuenta de origen con algunos objetos (archivos o carpetas).
- Uno o más cubos de S3 en la cuenta de destino.
- El control de versiones de S3 está habilitado en los depósitos de origen y destino.

- AWS Identity and Access Management (IAM) para crear una política de IAM, una función de IAM y una política de bucket de S3 en las cuentas de origen y destino.
- Las reglas del ciclo de vida de Amazon S3 están deshabilitadas mientras el trabajo de replicación por lotes de S3 está activo. Esto garantiza la paridad entre los buckets de origen y destino. De lo contrario, es posible que el depósito de destino no sea una réplica exacta del depósito de origen.

Arquitectura

Herramientas

AWS servicios

- AWS Identity and Access Management (IAM) le ayuda a administrar de forma segura el acceso a sus AWS recursos al controlar quién está autenticado y autorizado a usarlos.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Prácticas recomendadas

El siguiente vídeo de AWS re:Invent 2022 analiza las mejores prácticas para utilizar la replicación de Amazon S3 para cumplir con las normas, proteger los datos y aumentar el rendimiento de las aplicaciones.

Epics

Cree una política y una función de IAM para la replicación entre cuentas en la cuenta de origen

Tarea	Descripción	Habilidades requeridas
Cree una política de IAM para la replicación entre cuentas.	En la cuenta de AWS origen: 1. Abra la consola de IAM. 2. Cree una nueva política de IAM.	Administrador de la nube, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	3. En la sección del editor de políticas, elige JSON y pega el siguiente código. `{ "Version": "2012-10-17", "Statement": [{ "Sid": "GetSourceBucketConfiguration", "Effect": "Allow", "Action": ["s3:ListBucket", "s3:GetBucketLocation", "s3:GetBucketAcl", "s3:GetReplicationConfiguration", "s3:GetObjectVersionForReplication", "s3:GetObjectVersionAcl", "s3:GetObjectVersionTagging"], "Resource": ["arn:aws:s3:::source-bucket-name",`	

Tarea	Descripción	Habilidades requeridas
	<pre>"arn:aws:s3:::source-bucket-name/*"] }, { "Sid": "ReplicateToDestinationBuckets", "Effect": "Allow", "Action": ["s3:List*", "s3:*Object", "s3:ReplicateObject", "s3:ReplicateDelete", "s3:ReplicateTags"], "Resource": ["arn:aws:s3:::destination-bucket-name/*", "arn:aws:s3:::destination-bucket-name/*"] }, { "Sid": "PermissionToOverrideBucketOwner",</pre>	

Tarea	Descripción	Habilidades requeridas
	<pre>"Effect": "Allow", "Action": ["s3:ObjectOwnerOverrideToBucketOwner"], "Resource": ["arn:aws:s3:::destination-bucket-name/*", "arn:aws:s3:::destination-bucket-name/*"] }] }</pre> Esta política incluye tres declaraciones: • `GetSourceBucketConfiguration` proporciona acceso a la configuración de la replicación y a la versión del objeto para la replicación en el bucket de origen. • `ReplicateToDestinationBuckets` proporciona acceso para replicar en el depósito de destino.	

Tarea	Descripción	Habilidades requeridas
	Puede especificar varios cubos de destino en la matriz. • `PermissionToOverrideBucketOwner` proporciona acceso para `ObjectOwnerOverrideToBucketOwner` que el depósito de destino pueda ser propietario de los objetos de la cuenta de destino que se replicaron desde la cuenta de origen. 4. Elija Siguiente, proporcione un nombre de política, por ejemplo `cross-account-bucket-replication-policy` , y, a continuación, elija Crear política. Para obtener más información, consulte Creación de políticas de IAM en la documentación de IAM.	

Tarea	Descripción	Habilidades requeridas
Cree un rol de IAM para la replicación entre cuentas.	En la cuenta de AWS origen: 1. En la consola de IAM, cree un rol de IAM con la siguiente información: a. En Trusted entity type (Tipo de entidad de confianza), seleccione AWS service. b. Para el servicio, elija S3. c. Para el caso de uso, elija S3 Batch Operations. d. Elija la política que creó en el paso anterior. 2. Proporcione un nombre de rol como cross-account-bucket-replication -role y, a continuación, elija Crear rol. Para obtener más informaci ón, consulte Creación de funciones de IAM en la documentación de IAM.	Administrador de la nube, administrador de AWS

Cree una regla de replicación en la cuenta de origen

Tarea	Descripción	Habilidades requeridas
Cree una regla de replicación para el depósito de origen de la cuenta de origen.	En la cuenta AWS de origen: 1. Abra la consola de Amazon S3.	Administrador de la nube, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	2. Navegue hasta el depósito de origen y elija la pestaña Administración. 3. Cree una regla de replicación con la siguiente configuración: a. Proporcione un nombre de regla como `s3-replication-rule` . b. En Status (Estado), elija Enabled (Habilitado). c. Para ver el ámbito de la regla, selecciona Se aplica a todos los objetos del depósito. d. En Destino, selecciona Especificar un depósito en otra cuenta y, a continuación, introduce el Cuenta de AWS número de destino y el nombre del depósito. e. Elige la opción para cambiar la propiedad del objeto al propietario del depósito de destino. f. Para el rol de IAM, elige el rol que creaste anteriormente en la cuenta de origen. g. Para ver opciones de replicación adicionales, seleccione todas las	

Tarea	Descripción	Habilidades requeridas
	opciones disponibles. Estas proporcionan la capacidad de replicar contenido rápidamente, monitorear el progreso de la replicación a través de CloudWatch las métricas de Amazon, replicar marcadore s de eliminación y replicar cambios en los metadatos. h. Seleccione Guardar. 4. Si tiene varios buckets de destino, cree reglas de replicación adicionales. Para obtener más información, consulte Configuración de la replicación cuando los buckets de origen y destino pertenece n a cuentas diferentes en la documentación de Amazon S3.	

Aplique una política de bucket al bucket de destino

Tarea	Descripción	Habilidades requeridas
Aplica una política de bucket al bucket de destino.	Este paso debe realizarse para cada grupo de destino de forma individual en las cuentas de AWS destino.	Administrador de AWS, administrador de sistemas de AWS, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	En la cuenta de AWS destino: 1. Abre la consola de IAM, navega hasta el depósito de destino y selecciona la pestaña Permisos. 2. Edite la política de bucket proporcionando el siguiente código JSON y guarde la política: `{ "Version": "2012-10-17", "Id": "PolicyFo rDestinationBucket", "Statement": [{ "Sid": "Permissions on objects and buckets", "Effect": "Allow", "Principa l": { "AWS": "arn:aws:iam::Sour ceAWSAccountNumber :role/IAM-Role-cre ated-in-step1-in-s ource-account" }, "Action": ["s3:List*", "s3:GetBucketVersi oning",`	

Tarea	Descripción	Habilidades requeridas
	"s3:PutBucketVersioning", "s3:ReplicateDelete", "s3:ReplicateObject"], "Resource": ["arn:aws:s3:::destination-bucket", "arn:aws:s3:::destination-bucket/*"] }, { "Sid": "Permission to override bucket owner", "Effect": "Allow", "Principal": { "AWS": "arn:aws:iam::SourceAWSAccountNumber:role/IAM-Role-created-in-step1-in-source-account" }, "Action": "s3:ObjectOwnerOverrideToBucketOwner", "Resource": "arn:aws:s3:::destination-bucket/*" }]	

Tarea	Descripción	Habilidades requeridas
	`}` Esta política incluye dos declaraciones: • `Permissions on objects and buckets`indica que el depósito de destino puede replicar el contenido en función de la función definida en la cuenta de origen. El rol proporciona permisos al depósito de origen. • `Permission to override bucket owner`indica que el depósito de destino tiene permisos para anular la propiedad de la cuenta de origen.	

Pruebe la replicación multicuenta de Amazon S3

Tarea	Descripción	Habilidades requeridas
Compruebe que la replicación funciona correctamente.	1. Añada un objeto al depósito de origen. 2. Compruebe que el nuevo objeto aparezca en los depósitos de S3 de las cuentas de destino. 3. Ver las CloudWatch métricas:	Administrador de la nube, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	a. En el segmento de origen, selecciona la pestaña Métricas. b. En la sección Métricas de replicación, seleccione una regla de replicación. c. Elija Display charts (Mostrar gráficos). Los gráficos reflejan el estado de la replicación al mostrar las operaciones pendientes de replicación, la latencia de la replicación y los bytes pendientes de replicación. Para obtener más información, consulte Monitorización de métricas con Amazon CloudWatch en la documentación de Amazon S3.	

Recursos relacionados

- ¿Cuándo uso IAM? (documentación de IAM)
- Cómo funciona la IAM (documentación de IAM)
- Creación de funciones de IAM (documentación de IAM)
- Creación de políticas de IAM (documentación de IAM)
- Descripción general de la administración de acceso: permisos y políticas (documentación de IAM)
- Crear, configurar y trabajar con buckets de Amazon S3 (documentación de Amazon S3)

- Carga, descarga y trabajo con objetos en Amazon S3 (documentación de Amazon S3)
- Replicación de objetos (documentación de Amazon S3)

Migre datos de un entorno Hadoop local a Amazon S3 con DistCp AWS PrivateLink para Amazon S3

Creado por Jason Owens (AWS), Andres Cantor (AWS), Jeff Klopfenstein (AWS), Bruno Rocha Oliveira y Samuel Schmidt (AWS)

Entorno: Producción	Origen: Hadoop	Destino: cualquiera
Tipo R: redefinir la plataforma	Carga de trabajo: código abierto	Tecnologías: almacenamiento y respaldo; análisis
Servicios de AWS: Amazon S3; Amazon EMR		

Resumen

Este patrón demuestra cómo migrar prácticamente cualquier cantidad de datos desde un entorno Apache Hadoop local a la nube de Amazon Web Services (AWS) mediante la herramienta de código abierto Apache con DistCpAWS for PrivateLink Amazon Simple Storage Service (Amazon S3). En lugar de utilizar la Internet pública o una solución proxy para migrar los datos, puede utilizar AWS PrivateLink para Amazon S3 para migrar los datos a Amazon S3 a través de una conexión de red privada entre su centro de datos local y una Amazon Virtual Private Cloud (Amazon VPC). Si usa entradas de DNS en Amazon Route 53 o añade entradas en el archivo /etc/hosts en todos los nodos del clúster de Hadoop en las instalaciones, se le redirigirá automáticamente al punto de conexión de interfaz correcto.

Esta guía proporciona instrucciones de uso DistCp para migrar datos a la nube de AWS. DistCp es la herramienta más utilizada, pero hay otras herramientas de migración disponibles. Por ejemplo, puede usar herramientas de AWS sin conexión, como AWS Snowball o AWS Snowmobile, o herramientas de AWS en línea, como AWS Storage Gateway o AWS. DataSync Además, puede utilizar otras herramientas de código abierto, como Apache. NiFi

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa con una conexión de red privada entre el centro de datos en las instalaciones y la nube de AWS
- Hadoop, instalado in situ con DistCp
- Un usuario de Hadoop con acceso a los datos de migración en el sistema de archivos distribuido de Hadoop (HDFS)
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada
- Permisos para colocar objetos en un bucket de S3

Limitaciones

Las limitaciones de la nube privada virtual (VPC) se aplican a AWS PrivateLink para Amazon S3. Para obtener más información, consulte las propiedades y limitaciones de los puntos de conexión de la interfaz y PrivateLink las cuotas de AWS (PrivateLink documentación de AWS).

AWS PrivateLink para Amazon S3 no admite lo siguiente:

- Puntos de conexión del estándar federal de procesamiento de información (FIPS)
- Puntos de conexión del sitio web
- Puntos de enlace global heredado

Arquitectura

Pila de tecnología de origen

- Clúster de Hadoop con instalado DistCp

Pila de tecnología de destino

- Amazon S3
- Amazon VPC

Arquitectura de destino

El diagrama muestra cómo el administrador de Hadoop copia datos desde un entorno local DistCp a través de una conexión de red privada, como AWS Direct Connect, a Amazon S3 a través de un punto de enlace de la interfaz Amazon S3.

Herramientas

Servicios de AWS

- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- Amazon Virtual Private Cloud (Amazon VPC) permite lanzar recursos de AWS en una red virtual que se haya definido. Esa red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de usar la infraestructura escalable de AWS.

Otras herramientas

- Apache Hadoop DistCp (copia distribuida) es una herramienta que se utiliza para copiar grandes clústeres e intracústeres. DistCp utiliza Apache MapReduce para la distribución, la gestión y recuperación de errores y la elaboración de informes.

Epics

Migre los datos a la nube de AWS

Tarea	Descripción	Habilidades requeridas
Cree un punto de conexión para AWS PrivateLink para Amazon S3.	1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon VPC. 2. En el panel de navegación, elija Endpoints (puntos de conexión) y, a continuación, elija Create Endpoint (Crear punto de enlace).	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	3. En Service category, seleccione AWS services. 4. En el campo de búsqueda, escriba s3 y, a continuación, pulse Intro. 5. En los resultados de la búsqueda, elija com.amazonaws. Nombre del servicio < your-aws-region >.s3 donde el valor de la columna Tipo es Interfaz. 6. En VPC, elija su VPC. En Subredes, elija sus subredes. 7. En Grupo de seguridad , elija o cree un grupo de seguridad que permita TCP 443. 8. Añada etiquetas en función de sus necesidades y, a continuación, seleccione Crear punto de conexión.	

Tarea	Descripción	Habilidades requeridas
Compruebe los puntos de conexión y busque las entradas de DNS.	1. Abra la consola de Amazon VPC, elija Puntos de conexión y, a continuación, seleccione el punto de conexión que creó anteriormente. 2. En la pestaña Detalles, busque la primera entrada de DNS en nombres de DNS. Esta es la entrada de DNS regional. Al usar este nombre de DNS, las solicitudes alternan entre las entradas de DNS específicas de las zonas de disponibilidad. 3. Seleccione la pestaña Subredes. Puede encontrar la dirección de la interfaz de red elástica del punto de conexión en cada zona de disponibilidad.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Compruebe las reglas del firewall y las configuraciones de enrutamiento.	Para confirmar que las reglas del firewall están abiertas y que la red está configurada correctamente, use Telnet para probar el punto de conexión en el puerto 443. Por ejemplo: `$ telnet vpce-<your-VPC-endpoint-ID>.s3.us-east-2.vpce.amazonaws.com 443` `Trying 10.104.88.6...` `Connected to vpce-<your-VPC-endpoint-ID>.s3.us-east-2.vpce.amazonaws.com.` `...` `$ telnet vpce-<your-VPC-endpoint-ID>.s3.us-east-2.vpce.amazonaws.com 443` `Trying 10.104.71.141...` `Connected to vpce-<your-VPC-endpoint-ID>.s3.us-east-2.vpce.amazonaws.com.` Nota: si usa la entrada regional, una prueba satisfactoria mostrará que el DNS alterna entre las dos direccion	Administrador de red, administrador de AWS

Tarea	Descripción	Habilidades requeridas
	es IP que puede ver en la pestaña Subredes del punto de conexión seleccionado en la consola de Amazon VPC.	

Tarea	Descripción	Habilidades requeridas
Configure la resolución de nombres.	Debe configurar la resolución de nombres para permitir que Hadoop acceda al punto de conexión de la interfaz Amazon S3. No puede usar el nombre del punto de conexión como tal. En su lugar, debe resolver `<your-bucket-name>.s3.<your-aws-region>.amazonaws.com` o `*.s3.<your-aws-region>.amazonaws.com`. Para obtener más información sobre esta limitación de nombres, consulte Presentación del cliente Hadoop S3A (sitio web de Hadoop). Elija una de las siguientes opciones de configuración: • Use el DNS en las instalaciones para resolver la dirección IP privada del punto de conexión. Puede anular el comportamiento de todos los buckets o de algunos de ellos. Para obtener más información, consulte «Opción 2: acceder a Amazon S3 mediante zonas de política de respuesta del sistema de nombres de dominio	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	(DNS RPZ)» en Acceso híbrido seguro a Amazon S3 mediante AWS PrivateLink (entrada del blog de AWS). • Configure el DNS en las instalaciones para reenviar el tráfico de forma condicional a los puntos de conexión entrantes de la resolución en la VPC. El tráfico se reenvía a Route 53. Para obtener más información, consulte la sección «Opción 3: reenviar solicitudes de DNS desde locales mediante los puntos de enlace entrantes de Amazon Route 53 Resolver» en Acceso híbrido seguro a Amazon S3 mediante AWS (entrada del blog de PrivateLink AWS). • Edite el archivo /etc/hosts en todos los nodos de su clúster de Hadoop. Esta es una solución temporal para realizar pruebas, y no se recomienda su uso en producción. Para editar el archivo /etc/hosts, añada una entrada para `<your-bucket-name>.s3.<your-aws-region>.amazonaws.com`	

Tarea	Descripción	Habilidades requeridas
	o `s3.<your-aws-region>.amazonaws.com` . El archivo /etc/hosts no puede tener varias direcciones IP para una entrada. Debe elegir una única dirección IP de una de las zonas de disponibilidad, que luego se convertirá en un único punto de error.	

Tarea	Descripción	Habilidades requeridas
Configure la autenticación para Amazon S3.	Para autenticarse en Amazon S3 a través de Hadoop, le recomendamos que exporte las credenciales de rol temporales al entorno de Hadoop. Para obtener más información, consulte Autenticación con S3 (sitio web de Hadoop). En trabajos de larga duración, puede crear un usuario y asignar una política con permisos para colocar datos únicament e en un bucket de S3. La clave de acceso y la clave secreta se pueden almacenar en Hadoop, y solo pueden acceder a ellas el propio DistCp trabajo y el administr ador de Hadoop. Para obtener más información sobre el almacenamiento de secretos, consulte Almacenamiento de secretos con los proveedores de credenciales de Hadoop (sitio web de Hadoop). Para obtener más información sobre otros métodos de autenticación, consulte Cómo obtener credenciales de un rol de IAM para su uso con acceso de CLI a una cuenta de AWS en la documentación de AWS IAM Identity Center	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	(sucesor de AWS Single Sign-On). Para usar credenciales temporales, añada las credenciales temporales a su archivo de credencia les o ejecute los siguientes comandos para exportar las credenciales a su entorno: `export AWS_SESSI ON_TOKEN=SECRET-SE SSION-TOKEN` `export AWS_ACCES S_KEY_ID=SESSION-A CCESS-KEY` `export AWS_SECRE T_ACCESS_KEY=SESSION- SECRET-KEY` Si tiene una combinación de clave de acceso y clave secreta tradicional, ejecute los siguientes comandos: `export AWS_ACCES S_KEY_ID=my.aws.key` `export AWS_SECRE T_ACCESS_KEY=my.se cret.key` Nota: Si utiliza una combinaci ón de clave de acceso y clave secreta, cambie el proveedor de credenciales en los DistCp comandos de a. `"org.apac`	

Tarea	Descripción	Habilidades requeridas
	he.hadoop.fs.s3a.T emporaryAWSCredent ialsProvider" "org.apache.hadoop .fs.s3a.SimpleAWSC redentialsProvider"	

Tarea	Descripción	Habilidades requeridas
Transfiera datos mediante DistCp.	Para usarlo DistCp para transferir datos, ejecute los siguientes comandos: `hadoop distcp -Dfs.s3a.aws.credentials.provider=\"org.apache.hadoop.fs.s3a.TemporaryAWSCredentialsProvider" \ -Dfs.s3a.access.key="${AWS_ACCESS_KEY_ID}" \ -Dfs.s3a.secret.key="${AWS_SECRET_ACCESS_KEY}" \ -Dfs.s3a.session.token="${AWS_SESSION_TOKEN}" \ -Dfs.s3a.path.style.access=true \ -Dfs.s3a.connection.ssl.enabled=true \ -Dfs.s3a.endpoint=s3.<your-aws-region>.amazonaws.com \ hdfs:///user/root/ s3a://<your-bucket-name>` Nota: La región de AWS del punto de conexión no se descubre automáticamente cuando se utiliza el DistCp comando con AWS PrivateLink para Amazon S3. Hadoop 3.3.2 y las versiones posterior	Ingeniero de migraciones; administrador de AWS

Tarea	Descripción	Habilidades requeridas
	es resuelven este problema habilitando la opción de establecer de forma explícita la región de AWS del bucket de S3. Para obtener más información, consulte S3A para añadir la opción fs.s3a.endpoint.region y establecer la región de AWS (sitio web de Hadoop). Para obtener más informaci ón sobre otros proveedores de S3A, consulte Configuración general de cliente S3A (sitio web de Hadoop). Por ejemplo, si usa el cifrado, puede añadir la siguiente opción a la serie de comandos anteriores en función del tipo de cifrado: `-Dfs.s3a.server-si de-encryption-algo rithm=AES-256 [or SSE- C or SSE-KMS]` Nota: para usar el punto de conexión de la interfaz con el S3A, debe crear una entrada de alias de DNS para el nombre regional de S3 (por ejemplo, `s3.<your- aws-region>.amazon aws.com`) en el punto de conexión de la interfaz. Consulte la sección Configura	

Tarea	Descripción	Habilidades requeridas
	r autenticación para Amazon S3 para obtener más instrucciones. Esta solución alternativa es necesaria para Hadoop 3.3.2 y versiones anteriores. Las versiones futuras de S3A no requieren de esta solución alternativa. Si tiene problemas de firma con Amazon S3, añada una opción para usar Signature Version 4 (SigV4): `-Dmapreduce.map.java.opts="-Dcom.amazonaws.services.s3.enableV4=true"`	

Uso CloudEndure para la recuperación ante desastres de una base de datos local

Creado por Nishant Jain (AWS) y Anuraag Deekonda (AWS)

Entorno: PoC o piloto	Tecnologías: almacenamiento y respaldo; modernización; bases de datos

Resumen

> Advertencia: los usuarios de IAM tienen credenciales de larga duración, lo que supone un riesgo para la seguridad. Para ayudar a mitigar este riesgo, le recomendamos que proporcione a estos usuarios únicamente los permisos que necesitan para realizar la tarea y que los elimine cuando ya no los necesiten.

Este patrón utiliza CloudEndure Disaster Recovery y el CloudEndure Failback Client para la recuperación ante desastres (DR). Configura la DR para un host de centro de datos en las instalaciones mediante una instancia de Amazon Elastic Compute Cloud (Amazon EC2).

Debe usar el CloudEndure Failback Client para replicar desde una infraestructura que no sea de nube u otra infraestructura de nube a la nube de Amazon Web Services (AWS). Una vez que haya pasado el desastre, querrá hacer una copia de seguridad de sus máquinas. CloudEndure lo prepara para la recuperación mediante recuperación al invertir la dirección de replicación de los datos desde el equipo de destino hasta el equipo de origen. La consola CloudEndure de usuario trata las máquinas de destino actualmente lanzadas como máquinas de origen. La replicación se invierte desde las máquinas de destino seleccionadas hasta la infraestructura de origen original.

> Importante: En noviembre de 2021, AWS lanzó AWS Elastic Disaster Recovery, que ahora es el servicio recomendado para la recuperación ante desastres en AWS.
>
> Tras el exitoso lanzamiento de Elastic Disaster Recovery, AWS empezará a limitar la disponibi lidad de CloudEndure Disaster Recovery en todas las regiones de AWS, incluidas las regiones de

AWS GovCloud (EE. UU.) (se seguirá admitiendo las regiones de AWS en China). Esto se llevará a cabo de acuerdo con el siguiente calendario:

1. 1 de septiembre de 2023: los clientes ya no podrán registrarse para obtener nuevas cuentas de CloudEndure recuperación ante desastres en ninguna región de AWS (excepto en las regiones de AWS en China).
2. 1 de diciembre de 2023: las nuevas instalaciones de agentes de CloudEndure recuperación ante desastres ya no se admitirán en ninguna región de AWS (excepto en las regiones de AWS en China). Tenga en cuenta que se admitirán las actualizaciones de los agentes existentes.
3. 31 de marzo de 2024: Se suspenderá la recuperación ante CloudEndure desastres en todas las regiones de AWS (excepto en las regiones de AWS en China).
4. Para ver los plazos actualizados de la EOL de recuperación CloudEndure ante desastres, consulte la CloudEndure documentación.

Esta publicación se retirará el 31 de marzo de 2024. Si lo necesita para un proyecto de migración en curso, descargue y guarde el archivo PDF mediante el enlace PDF que se encuentra debajo del título de esta página.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Base de datos en las instalaciones

Arquitectura

Pila de tecnología de origen

- Una base de datos en un centro de datos en las instalaciones

Pila de tecnología de destino

- Una base de datos en una instancia EC2 (para obtener una lista completa de las versiones de sistemas operativos compatibles, consulte Preguntas frecuentes de Amazon EC2)

Arquitectura de red de origen y destino

Herramientas

- CloudEndure Recuperación ante CloudEndure desastres: la recuperación ante desastres reduce el tiempo de inactividad y la pérdida de datos al proporcionar una recuperación rápida y confiable de servidores físicos, virtuales y basados en la nube en AWS. CloudEndure Disaster Recovery replica continuamente sus máquinas (incluido el sistema operativo, la configuración del estado del sistema, las bases de datos, las aplicaciones y los archivos) en un área de almacenamiento de bajo costo en su cuenta de AWS de destino y en la región preferida. Si se produce un desastre, puede indicarle a CloudEndure Disaster Recovery que inicie automáticamente miles de máquinas en el estado totalmente aprovisionado en cuestión de minutos.

Epics

Suscríbase a Disaster Recovery CloudEndure

Tarea	Descripción	Habilidades requeridas
Suscríbase a CloudEndure Disaster Recovery.	CloudEndure La recuperación ante desastres está disponible en AWS Marketplace.	AWS general
Cree una CloudEndure cuenta.	Regístrese CloudEndure y cree una cuenta. Posterior mente, en el correo electróni co, confirme la suscripción.	AWS general
Establezca la contraseña de la cuenta y acepte los términos y condiciones.	La contraseña debe tener al menos 8 caracteres de longitud, y debe contener como mínimo, una letra mayúscula, una minúscula s, un número y un carácter especial.	AWS general

Crea un CloudEndure proyecto

Tarea	Descripción	Habilidades requeridas
Inicie sesión en la consola CloudEndure de usuario.	En la consola CloudEndure de usuario, inicie sesión con las credenciales que creó en el paso anterior.	CloudEndure administrador
Cree un proyecto de nuevo.	En la esquina superior izquierda de la consola, elija el botón más (+) para crear un proyecto. Seleccione Recuperación de desastres como tipo de proyecto. Puede adquirir una licencia a través de AWS Marketplace.	CloudEndure administrador

Generar y usar credenciales de AWS

Tarea	Descripción	Habilidades requeridas
Cree una política de IAM para la CloudEndure solución.	La política de AWS Identity and Access Management (IAM) que debe crear para ejecutar la CloudEndure solución se basa en una CloudEndure política predefini da. Esta CloudEndure política contiene los permisos necesarios para usar AWS como infraestructura de destino.	Administrador de sistemas de AWS
Cree un nuevo usuario de IAM y genere credenciales de AWS.	Para generar las credencia les de AWS necesarias para la consola de CloudEndure	Administrador de sistemas de AWS

Tarea	Descripción	Habilidades requeridas
	usuario, cree al menos un usuario de IAM y asígnele la política de CloudEndure permisos. La consola necesita una ID de clave de acceso y una clave de acceso secreta. Para seguir las prácticas recomendadas de administración de las claves de acceso de AWS, debe rotar las claves de IAM periódicamente. Si se cambian las claves de IAM, los servidores de replicación se reiniciarán, lo que provocará un retraso temporal.	
Configure las credenciales de la cuenta del área de ensayo.	Inicie sesión en la consola CloudEndure de usuario y seleccione su proyecto de migración. En la pestaña Configuración e información, vaya a credenciales de AWS y proporcione sus Identificadores de clave de acceso y clave de acceso secreta.	Administrador de sistemas de AWS

Configuración de los ajustes de replicación

Tarea	Descripción	Habilidades requeridas
Defina los servidores de replicación.	Para obtener más informaci ón, consulte la CloudEndure documentación.	CloudEndure administrador

Instalación de CloudEndure agentes en el equipo de origen

Tarea	Descripción	Habilidades requeridas
Localice el token de instalaci ón del agente.	En la consola CloudEndure de usuario, vaya a Máquinas, Acciones de la máquina y Añadir máquinas. Al ejecutar el archivo de instalación en una máquina de origen, primero se le pide que introduzca su token de instalación. El token es una cadena única de caractere s que se genera automátic amente cuando se activa la CloudEndure cuenta. Puede usar un token de instalaci ón para instalar el agente en tantos equipos de origen como lo permita su proyecto.	CloudEndure administrador
En máquinas Linux, ejecute el instalador.	En máquinas Linux, copie el comando del instalador, inicie sesión en las máquinas de origen y ejecute el instalador.	CloudEndure administrador

Tarea	Descripción	Habilidades requeridas
	Para obtener instrucciones detalladas, consulte la CloudEndure documentación.	
En máquinas con Windows, ejecute el instalador.	Para máquinas Windows, descargue el archivo de instalación en cada máquina y, a continuación, ejecute el comando installer. Para obtener instrucciones detalladas, consulte la CloudEndure documentación.	CloudEndure administrador
Replique los datos.	Una vez instalado el agente, CloudEndure comienza a replicar la máquina de origen y comienza en el área de ensayo. Cuando se completa la sincronización inicial, la máquina aparece en la pestaña Máquinas de la consola CloudEndure de usuario.	CloudEndure administrador

Configure el esquema de la máquina de destino

Tarea	Descripción	Habilidades requeridas
Elija la máquina de origen para el esquema.	En la consola CloudEndu re de usuario, en la pestaña Máquinas, elija la máquina de origen para acceder al panel de detalles de la máquina.	CloudEndure administrador

Tarea	Descripción	Habilidades requeridas
Configure el esquema para la máquina de destino.	En la pestaña Esquema, configure los ajustes de la máquina de destino en función de sus requisito s. Para obtener instrucci ones detalladas, consulte la CloudEndure documentación.	CloudEndure administrador

Pruebe su solución de DR

Tarea	Descripción	Habilidades requeridas
Utilice el modo de prueba para probar la solución.	Para obtener instrucciones detalladas sobre el modo de prueba y la verificación de la transición de la prueba, consulte la CloudEndure documentación.	CloudEndure administrador
Pruebe la instancia de destino lanzada en el servidor Amazon EC2.	Para probar cada una de las máquinas de destino, elija el nombre de la máquina. A continuación, abra la pestaña Destino, copie la nueva dirección IP e inicie sesión en el servidor recién lanzado en la instancia de Amazon EC2.	CloudEndure administrador

Realice una conmutación por error con CloudEndure

Tarea	Descripción	Habilidades requeridas
Compruebe el estado de la máquina fuente.	En la página Máquinas de la consola de CloudEndure	CloudEndure administrador

Tarea	Descripción	Habilidades requeridas
	usuario, compruebe que la máquina de origen a la que desea realizar la conmutación por error tiene las siguientes indicaciones de estado: • Progreso de la replicación de datos: Protección continua de los datos • Estado: icono de cohete, que indica que se puede lanzar la máquina objetivo • Ciclo de vida de la recuperación de desastres: Probado recientemente	

Tarea	Descripción	Habilidades requeridas
Comience la transición.	1. En la página Máquinas, elija la máquina de origen. 2. En la pestaña Iniciar máquinas de destino, elija Modo de recuperación. 3. Elija el punto de recuperación para la máquina de destino. El sistema utilizará el punto de recuperación al lanzar las nuevas máquinas de destino para la conmutación por error. Puede utilizar el punto de recuperación más reciente o elegir un punto de recuperación anterior de la lista. 4. Seleccione Continuar con el inicio.	CloudEndure administrador
Compruebe el progreso y el estado de finalización del trabajo.	La ventana Job Progress muestra los detalles del proceso de lanzamiento de la máquina de destino. Una vez finalizada la conmutación por error, el estado del ciclo de vida de la recuperación ante desastres en la consola de CloudEndure usuario cambia a Conmutación fallida para indicar que se ha completado correctamente.	CloudEndure administrador

Realice una conmutación por recuperación con el cliente de CloudEndure recuperación

Tarea	Descripción	Habilidades requeridas
Revise los requisitos del cliente de CloudEndure conmutación por recuperación.	Utilice el cliente CloudEndure Failback para replicar a AWS desde una infraestructura local u otra infraestructura en la nube. El cliente CloudEndure Failback tiene los siguientes requisitos: • Las máquinas deben estar configuradas para arrancar en modo BIOS y ser compatibles con el arranque MBR. No se admiten las máquinas configuradas para arrancar en modo UEFI, que solo admiten el arranque mediante GPT. • El cliente CloudEndure Failback requiere al menos 4 GB de RAM dedicada.	CloudEndure administrador
Prepararse para la conmutación por recuperación.	Antes de poder iniciar la acción de preparación para la conmutación por recuperación, todas las máquinas de origen deben haber lanzado las máquinas de destino en modo de prueba o en modo de recuperación. En el menú Acciones del proyecto, seleccione Preparar para la conmutación por	CloudEndure administrador

Tarea	Descripción	Habilidades requeridas
	recuperación y, a continuación, elija Continuar. Cuando se muestra Emparejar el CloudEndure agente con el cliente de conmutación por recuperación, las máquinas están listas para la conmutación por recuperación.	
Descargue el cliente CloudEndure Failback en su entorno local.	Para descargar el cliente de CloudEndure recuperación en su entorno de origen, haga lo siguiente: 1. En su proyecto de recuperación de desastres, seleccione Configuración e información. 2. En la página de Configuración de la replicación, seleccione el enlace Más información sobre Conmutación por recuperación a “Otras infraestructuras”. 3. En el cuadro de diálogo Conmutación por recuperación a una nube/otra infraestructura sin identificar, seleccione Descargar desde aquí. El archivo se descargará automáticamente.	CloudEndure administrador

Tarea	Descripción	Habilidades requeridas
Inicie la replicación de la máquina en las instalaciones.	Para iniciar la replicación de la máquina de origen, la máquina de destino debe arrancarse en la imagen de cliente de CloudEndu re conmutación por error ()`failback_client.is o` . Si el cliente no puede obtener la configuración de red mediante el protocolo de configuración dinámica de host (DHCP), introduzca la configuración manualmente. El cliente CloudEndure Failback se conecta a console.clouendure.com a través del puerto TCP 443 y se autentica con las credenciales que se le piden que introduzca. CloudEndure	CloudEndure administrador

Tarea	Descripción	Habilidades requeridas
Siga las instrucciones para proporcionar los detalles necesarios.	Proporcione los siguientes detalles: • Token de instalación • Identificador de máquina de la máquina de origen • Mapeo de discos entre el origen y el destino Asegúrese de que el cliente de CloudEndure conmutaci ón por error esté conectado a la consola de CloudEndure usuario y al equipo de destino a través de direcciones IP públicas o privadas.	CloudEndure administrador
Localice el Identificador de la máquina de origen.	Para localizar el Identificador de la máquina de origen, elija el nombre de la máquina en la pestaña Máquinas y copie el Identificador de la pestaña Origen.	CloudEndure administrador

Tarea	Descripción	Habilidades requeridas
Conecte la máquina de origen a la máquina de destino.	Proporcione el Identificador de la máquina de origen (el servidor de AWS es ahora la fuente de la conmutación por recuperación) en el servidor en las instalaciones (máquina de destino). La máquina de AWS (origen) se conecta al servidor en las instalaciones (destino) en el puerto TCP 1500 para iniciar la replicación. Una vez completada la replicación inicial, la consola CloudEndure de usuario indica que la replicación está en modo de protección continua de datos.	CloudEndure administrador
Edite la configuración de conmutación por recuperación, si es necesario.	Para editar la configuración de conmutación por recuperación, elija el nombre de la máquina y, a continuación, elija la pestaña Configuración de conmutación por recuperación.	CloudEndure administrador

Tarea	Descripción	Habilidades requeridas
Inicie la máquina de destino.	Para lanzar la máquina de destino, haga lo siguiente: Seleccione la casilla de verificación situada a la izquierda del nombre de cada máquina, elija Launch x Target Machine y, a continuación, elija el Modo de recuperación. En el cuadro de diálogo, seleccione Siguiente. Elija el punto de recuperación Más reciente y, a continuac ión, elija Continuar con el inicio. Una vez finalizado el proceso de inicio, la consola de CloudEndure usuario muestra el estado Empareje el CloudEndure agente con el servidor de replicación en Progreso de la replicación de datos.	CloudEndure administrador

Tarea	Descripción	Habilidades requeridas
Vuelva a poner las máquinas en funcionamiento normal.	Ahora cambie la dirección de la replicación de datos para que la máquina en las instalaciones sea la fuente y la máquina de AWS sea el destino. Elija Acciones del proyecto y, a continuación, elija Volver a la normalidad y Continuar. La dirección de la replicación de los datos se invierte y las máquinas se someten al proceso de sincronización inicial. El proceso de conmutación por recuperación finaliza cuando la columna Progreso de la replicación de datos muestra el estado de Protección continua de datos de todas las máquinas.	CloudEndure administrador

Recursos relacionados

AWS Marketplace

- CloudEndure Recuperación ante desastres

CloudEndure documentación

- Inicie sesión en la consola
- Creación de un proyecto
- Generación y uso de credenciales
- Configuración de los ajustes de replicación

- Instalación de CloudEndure agentes
- Realizar una conmutación por error de recuperación de desastres

Tutoriales y vídeos

- CloudEndure manual de solución de problemas
- CloudEndure vídeos
- Demostración de recuperación de desastres en AWS

Más patrones

- Automatice las copias de seguridad basadas en eventos desde CodeCommit Amazon S3 mediante CodeBuild and Events CloudWatch
- Archivar automáticamente los elementos en Amazon S3 con DynamoDB TTL
- Realice copias de seguridad automáticas de las bases de datos de SAP HANA mediante Systems Manager y EventBridge
- Realice copias de seguridad y archive los datos del mainframe en Amazon S3 mediante AMI Cloud Data de BMC
- Cree una canalización de servicios de ETL para cargar datos de forma incremental desde Amazon S3 a Amazon Redshift mediante AWS Glue
- Convierta y desempaquete datos EBCDIC a ASCII en AWS mediante Python
- Convierta el tipo de datos VARCHAR2 (1) para Oracle en un tipo de datos booleano para Amazon Aurora PostgreSQL
- Crear una definición de tareas de Amazon ECS y montar un sistema de archivos en instancias EC2 mediante Amazon EFS
- ???
- Costos de almacenamiento estimados para una tabla de Amazon DynamoDB
- Identifique los buckets públicos de S3 en AWS Organizations mediante Security Hub
- Migrar las instancias de base de datos de Amazon RDS para Oracle a otras cuentas que usen AMS
- Migración de un servidor SFTP en las instalaciones a AWS mediante AWS Transfer para SFTP
- Migre una tabla particionada de Oracle a PostgreSQL mediante AWS DMS
- Migre datos de Microsoft Azure Blob a Amazon S3 mediante Rclone
- Migre valores CLOB de Oracle a filas individuales en PostgreSQL en AWS
- Migración de sistemas de archivos compartidos en una gran migración de AWS
- Migración de pequeños conjuntos de datos de las instalaciones a Amazon S3 mediante AWS SFTP
- Supervisar Amazon Aurora en busca de instancias sin cifrado
- ???
- Ejecutar cargas de trabajo con estado y almacenamiento de datos persistente mediante Amazon EFS en Amazon EKS con AWS Fargate

- Importación correcta de un bucket de S3 como CloudFormation pila de AWS
- Sincronice los datos entre los sistemas de archivos de Amazon EFS en distintas regiones de AWS mediante AWS DataSync
- Vea los detalles de la instantánea de EBS de su cuenta u organización de AWS

Aplicaciones web y móviles

Temas

- Implemente de forma continua una aplicación web AWS Amplify moderna desde un repositorio de AWS CodeCommit
- Crear una aplicación React con AWS Amplify y añadir autenticación con Amazon Cognito
- Implemente una aplicación de una sola página basada en React en Amazon S3 y CloudFront
- Implemente una API de Amazon API Gateway en un sitio web interno mediante puntos de conexión privados y un Equilibrador de carga de aplicación
- Inserta un QuickSight panel de Amazon en una aplicación Angular local
- Más patrones

Implemente de forma continua una aplicación web AWS Amplify moderna desde un repositorio de AWS CodeCommit

Creado por Deekshitulu Pentakota (AWS) y Sai Katakam (AWS)

Entorno: PoC o piloto	Tecnologías: aplicaciones web y móviles; Modernización DevOps	Servicios de AWS: AWS Amplify; AWS CodeCommit

Resumen

Las aplicaciones web modernas se construyen como una sola página de aplicaciones (SPA) que engloban todos los componentes de la aplicación en archivos estáticos. Con AWS Amplify Hosting, puede diseñar un proceso de integración e implementación continuas (CI/CD) que cree, implemente y aloje una aplicación web moderna administrada en un repositorio basado en Git. Al conectar Amplify Hosting al repositorio de código, cada confirmación inicia un único flujo de trabajo para implementar el frontend y el backend de la aplicación. El beneficio de este enfoque es que la aplicación web se actualiza solo después de haber realizado correctamente la implementación, lo que elimina inconsistencias entre el front-end y el backend.

En este patrón, utiliza un CodeCommit repositorio de AWS para administrar su aplicación web moderna. La aplicación web de ejemplo que se incluye en estas instrucciones emplea el marco React SPA. Sin embargo, Amplify Hosting es compatible con muchos otros marcos SPA, como Angular, Vue o Next.js, y también con generadores de sitio único, como Gatsby, Hugo y Jekyll.

Este patrón está destinado a creadores de AWS que tienen experiencia con los siguientes servicios y conceptos:

- AWS CodeCommit
- AWS Amplify Hosting
- React
- JavaScript
- Node.js
- npm
- Git

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Permisos para crear recursos en Amplify y. CodeCommit Para obtener más información, consulte Identity and Access Management for Amplify e Identity and Access Management for AWS. CodeCommit
- Interfaz de la línea de comandos de AWS (AWS CLI) instalada y configurada.
- Un editor de texto o de código.
- CodeCommit, configurado para los usuarios de HTTPS que utilizan credenciales de Git.
- Un rol de servicio de IAM para Amplify.
- npm y Node.js instalados (documentación de npm).

Limitaciones

- Este patrón no aborda el desarrollo y la integración de un backend para la aplicación de Amplify, como API, autenticación o base de datos. Para obtener más información, consulte Crear un backend en la documentación de Amplify.

Versiones de producto

- CLI de AWS versión 2.0
- Node.js versión 16.x o posterior

Arquitectura

Pila de tecnología de destino

- CodeCommitRepositorio de AWS que contiene un SPA de React
- Flujo de trabajo de AWS Amplify Hosting

Arquitectura de destino

Herramientas

Servicios de AWS

- AWS Amplify Hosting proporciona un flujo de trabajo basado en Git para alojar aplicaciones web sin servidor de pila completa con implementación continua.
- AWS CodeCommit es un servicio de control de versiones que le ayuda a almacenar y gestionar repositorios de Git de forma privada, sin necesidad de gestionar su propio sistema de control de código fuente.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.

Otras herramientas

- Node.js es un entorno de JavaScript ejecución basado en eventos diseñado para crear aplicaciones de red escalables.
- npm es un registro de software que se ejecuta en un entorno Node.js y se utiliza para compartir o tomar prestados paquetes y administrar la implementación de paquetes privados.

Epics

Cree un repositorio CodeCommit

Tarea	Descripción	Habilidades requeridas
Creación de un repositorio.	Para obtener instrucciones, consulte Crear un CodeCommit repositorio de AWS en la CodeCommit documentación.	AWS DevOps
Clonar el repositorio.	Para obtener instrucciones, consulte Conectarse al CodeCommit repositorio mediante la clonación del repositorio en la CodeCommit documentación. Si se	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	le solicita iniciar sesión, proporcione sus credenciales de Git.	

Crear una aplicación React

Tarea	Descripción	Habilidades requeridas
Para crear una nueva aplicación React.	1. Ingrese el comando siguiente para navegar en el repositorio clonado. `<repo name>`Sustitúya lo por el nombre de tu CodeCommit repositorio. `$ cd <repo name>` 2. Ejecute el siguiente comando para crear una nueva aplicación de React en el repositorio clonado. `$ npx create-react-app .` 3. Codifique la aplicación y, a continuación, ejecute el siguiente comando para iniciarla. `$ npm start` Para obtener más informaci ón sobre cómo crear una aplicación React personali	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	zada, consulte las instrucciones Crear una aplicación React en la documentación de Crear una aplicación React. También puede implementar una aplicación React de muestra en su cuenta de Amplify siguiendo las instrucciones de Implementar un frontend en la documentación de Amplify.	
Cree una ramificación e introduzca el código.	1. Ejecute el siguiente comando para crear una nueva ramificación local. `<branch>` es el nombre que desea asignar a la nueva ramificación. `$ git checkout -b <branch>` 2. Ingresa el siguiente comando para enviar la rama al CodeCommit repositorio, donde `<branch>` está el nombre que asignaste en el paso anterior. Para obtener más información, consulte Trabajar con confirmaciones. `$ git push --set-upstream origin <branch>`	Desarrollador de aplicaciones

Implemente la aplicación en AWS Amplify Hosting

Tarea	Descripción	Habilidades requeridas
Conecte Amplify al repositorio.	Para obtener más instrucciones, consulte Conectar un repositorio en la documentación de Amplify Hosting. Seleccione AWS CodeCommit y el repositorio y la rama que creó anteriormente.	Desarrollador de aplicaciones
Defina la configuración de compilación del frontend.	Para obtener más instrucciones, consulte Confirmar la configuración de compilación de frontend en la documentación de Amplify Hosting. Acepte los valores predeterminados o introduzca los siguientes. `Build settings:` `version: 0.1` `frontend:` `  phases:` `  preBuild:` `  commands:` `  - npm ci` `  build:` `  commands:` `  - npm run build` `  artifacts:` `  baseDirectory:` `  build` `  files:` `  - '**/*'` `  cache:` `  paths:`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`- node_modules/**/*`	
Revise e implemente.	Para obtener más instrucciones, consulte Guardar e implementar en la documentación de Amplify Hosting. Espere hasta que se complete el proceso de implementación.	Desarrollador de aplicaciones

Valide la implementación continua

Tarea	Descripción	Habilidades requeridas
Verifique la implementación inicial.	Cuando se complete el proceso de implementación, seleccione el enlace en Dominio. Compruebe que la aplicación funciona según lo previsto.	Desarrollador de aplicaciones
Envíe los cambios al repositorio de código.	Edite el código en su estación de trabajo local e inserte los cambios en el CodeCommit repositorio. Amplify Hosting detectará el cambio en el repositorio e iniciará automáticamente el proceso de creación e implementación. Confirme que las actualizaciones de la aplicación sean visibles en el dominio.	Desarrollador de aplicaciones

Recursos relacionados

CodeCommit Documentación de AWS

- Configuración para AWS CodeCommit
  - Configuración de usuarios HTTPS mediante credenciales de Git
  - Pasos de configuración para las conexiones HTTPS a CodeCommit los repositorios de AWS en Linux, macOS o Unix con el asistente de credenciales de la CLI de AWS
- Cómo empezar a usar AWS CodeCommit

Documentación de AWS Amplify Hosting

- Introducción al código existente
- Configuración de dominios personalizados

Recursos de React

- Sitio web de Crear aplicación React
- Documentación de Crear aplicación React
- Crear un repositorio de aplicaciones React (GitHub)

Crear una aplicación React con AWS Amplify y añadir autenticación con Amazon Cognito

Creado por Rishi Singla (AWS)

Entorno: PoC o piloto	Tecnologías: aplicaciones web y móviles; seguridad, identidad y cumplimiento	Carga de trabajo: todas las demás cargas de trabajo
Servicios de AWS: AWS Amplify; Amazon Cognito		

Resumen

Este patrón muestra cómo usar AWS Amplify para crear una aplicación basada en React y cómo añadir autenticación a frontend mediante Amazon Cognito. AWS Amplify consta de un conjunto de herramientas (marco de código abierto, entorno de desarrollo visual, consola) y servicios (alojamiento de aplicaciones web y sitios web estáticos) para acelerar el desarrollo de aplicaciones móviles y web en AWS.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Node.js y npm instalados en su equipo

Versiones de producto

- Node.js versión 10.x o posterior (para verificar su versión, ejecute `node -v` en una ventana de terminal)
- npm versión 6.x o posterior (para verificar su versión, ejecute `npm -v` en una ventana de terminal)

Arquitectura

Pila de tecnología de destino

- AWS Amplify
- Amazon Cognito

Herramientas

- Amplificar la interfaz de la línea de comandos (CLI)
- Bibliotecas Amplify (bibliotecas cliente de código abierto)
- Amplify Studio (interfaz visual)

Epics

Instalar la CLI de AWS Amplify

Tarea	Descripción	Habilidades requeridas
Instalar la CLI de Amplify	La CLI de Amplify es una cadena de herramientas unificada para crear servicios en la nube de AWS para su aplicación React. Para instalar la CLI de Amplify, ejecute: `npm install -g @aws-amplify/cli` npm le notificará si hay una nueva versión principal disponible. Si es así, utilice el siguiente comando para actualizar su versión de npm:	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`npm install -g npm@9.8.0` donde 9.8.0 se refiere a la versión que desea instalar.	

Crear una aplicación React

Tarea	Descripción	Habilidades requeridas
Crear una React App.	Para crear una nueva aplicación React, utilice el comando: `npx create-react-app amplify-react-application` donde `ampify-react-application` es el nombre de la aplicación. Cuando haya creado correctamente la aplicación, verá el siguiente mensaje: `Success! Created amplify-react-application` Se creará un directorio con varias subcarpetas para la aplicación React.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Inicie la aplicación en el equipo local.	Vaya al directorio `amplify-react-application` que se creó en el paso anterior y ejecute el comando: `amplify-react-appl ication% npm start` Esto inicia la aplicación React en la máquina local.	Desarrollador de aplicaciones

Configurar la CLI de Amplify

Tarea	Descripción	Habilidades requeridas
Configure Amplify para que se conecte a su cuenta de AWS.	Configure Amplify ejecutando el comando: `amplify-react-appl ication % amplify configure` La CLI de Amplify le pide que siga estos pasos para configurar el acceso a su cuenta de AWS: 1. Inicie sesión en su cuenta de administrador de AWS. 2. Especifique la región de AWS que quiere utilizar. 3. Cree un usuario de AWS Identity and Access Management (IAM) con	AWS general, desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	acceso programático y adjunte la política de permisos `AdministratorAccess-Amplify` al usuario. 4. Cree y luego copie el ID de la clave de acceso y la clave de acceso secreta. 5. Introduzca estos detalles en la terminal. 6. Cree un nombre de perfil o utilice el perfil por defecto. Advertencia: este escenario requiere que los usuarios de IAM tengan acceso programático y credenciales de larga duración, lo que supone un riesgo para la seguridad. Para ayudar a mitigar este riesgo, le recomendamos que brinde a estos usuarios únicamente los permisos que necesitan para realizar la tarea y que los elimine cuando ya no los necesiten. Las claves de acceso se pueden actualizar si es necesario. Para obtener más información, consulte Actualización de claves de acceso en la Guía de usuario de IAM.	

Tarea	Descripción	Habilidades requeridas
	Estos pasos se muestran en la terminal de la siguiente manera. `Follow these steps to set up access to your AWS account:` `Sign in to your AWS administrator account: https://console.aws.amazon.com/` `Press Enter to continue` `Specify the AWS Region` `? region:  us-east-1` `Follow the instructions at https://docs.amplify.aws/cli/start/install/#configure-the-amplify-cli` `to complete the user creation in the AWS console` `https://console.aws.amazon.com/iamv2/home#/users/create` `Press Enter to continue` `Enter the access key of the newly created user:` `? accessKeyId: ********************` `? secretAccessKey: ********************` `This would update/create the AWS Profile in your local machine` `? Profile Name:  new`	

Tarea	Descripción	Habilidades requeridas
	`Successfully set up the new user.` Para obtener más información sobre estos pasos, consulte la documentación del Amplify Dev Center.	

Inicializar Amplify

Tarea	Descripción	Habilidades requeridas
Inicialice Amplify.	1. Para inicializar Amplify en el nuevo directorio, ejecute: `amplify init` Amplify le solicita el nombre del proyecto y los parámetros de configuración 2. Especifique todos los parámetros y, a continuación, pulse Y para inicializar el proyecto con la configuración especificada. `Project information` `| Name: amplifyreactproject` `| Environment: dev` `| Default editor: Visual Studio Code`	Desarrollador de aplicaciones, AWS general

Tarea	Descripción	Habilidades requeridas
	<pre>| App type: javascrip t | Javascript framework: react | Source Directory Path: src | Distribution Directory Path: build | Build Command: npm run-script build | Start Command: npm run-script start</pre>	
	3. Seleccione el perfil que creó en el paso anterior. Los recursos se desplegar án en el entorno `dev` del proyecto Amplify que creó. 4. Para confirmar que se han creado los recursos, puede abrir la consola de AWS Amplify y ver la CloudForm ation plantilla de AWS que se utilizó para crear los recursos y los detalles.	
	<pre>Deploying root stack amplifyreactproject [================== ==---------------- ----] 2/4 amplify-amplif yreactproject-d… AWS::CloudFormatio</pre>	

Tarea	Descripción	Habilidades requeridas
	`n::Stack CREATE_IN_PROGRESS` `UnauthRole AWS::IAM::Role CREATE_COMPLETE` `DeploymentBucket AWS::S3::Bucket CREATE_IN_PROGRESS` `AuthRole AWS::IAM::Role CREATE_COMPLETE`	

Agregar la autenticación a frontend

Tarea	Descripción	Habilidades requeridas
Añada la autenticación.	Puede usar el comando `amplify add <category>` para agregar caracterí stica como el inicio de sesión de un usuario o una API de backend. En este paso, utilizará el comando para añadir la autenticación. Amplify proporciona un servicio de autenticación de backend con Amazon Cognito,	Desarrollador de aplicaciones, AWS general

Tarea	Descripción	Habilidades requeridas
	bibliotecas de frontend y un componente de Authenticator UI integrado. Las caracterí sticas incluyen el registro de usuarios, el inicio de sesión de los usuarios, la autentica ción multifactorial, el cierre de sesión de los usuarios y el inicio de sesión sin contraseñ a. También puede autentica r a los usuarios mediante la integración con proveedores de identidad federados, como Amazon, Google y Facebook. La categoría de autentica ción de Amplify se integra perfectamente con otras categorías de Amplify, como API, análisis y almacenam iento, para que pueda definir reglas de autorización para usuarios autenticados y no autenticados. 1. Para configurar la autentica ción de su aplicación React, ejecute el comando: `amplify-react-appl ication1 % amplify add auth` Esto muestra la siguiente información y solicitudes. Puede elegir la configura	

Tarea	Descripción	Habilidades requeridas
	ción adecuada en función de sus requisitos empresariales y de seguridad. `Using service:` ` Cognito, provided by:` ` awscloudformation` ` The current configured provider is Amazon` ` Cognito.` `Do you want to use the` ` default authentication and security` ` configuration? (Use` ` arrow keys)` `# Default configuration` `  Default configuration with Social` ` Provider (Federation)` `  Manual configuration` `  I want to learn` ` more.` 2. Para ver un ejemplo sencillo, seleccione la configuración predeterminada y, a continuación, seleccione el mecanismo de inicio de sesión para los usuarios (en este caso, el correo electrónico):	

Tarea	Descripción	Habilidades requeridas
	`` How do you want users to be able to sign in? Username # Email Phone Number Email or Phone Number I want to learn more. ```	
	3. Omita la configuración avanzada para completar la adición de los recursos de autenticación: ``` Do you want to configure advanced settings? (Use arrow keys) # No, I am done. Yes, I want to make some additional changes. ```	
	4. Cree sus recursos de backend locales y aprovisió nelos en la nube: ``` amplify-react-appl ication1 % amplify push ```	

Tarea	Descripción	Habilidades requeridas
	Este comando realiza los cambios adecuados en los grupos de usuarios de Congito de su cuenta. 5. Pulse Y para configurar el `auth` recurso mediante CloudFormation. Esto configura los siguiente s recursos: `UserPool AWS::Cognito::UserPool CREATE_COMPLETE` `UserPoolClientWeb AWS::Cognito::UserPoolClient CREATE_COMPLETE` `UserPoolClientWeb AWS::Cognito::UserPoolClient CREATE_COMPLETE` `UserPoolClientRole AWS::IAM::Role CREATE_COMPLETE` `UserPoolClientLambda AWS::Lambda::Function CREATE_COMPLETE` `UserPoolClientLambdaPolicy AWS::IAM::Policy CREATE_CO`	

Tarea	Descripción	Habilidades requeridas
	<pre>MPLETE UserPoolClientLog Policy AWS::IAM::Policy CREATE_IN _PROGRESS</pre> También puede usar la Consola de AWS Cognito para ver estos recursos (busque grupos de usuarios y grupos de identidades de Cognito). Este paso actualiza el archivo `aws-exports.js` de la carpeta `src` de la aplicación React con las configuraciones del grupo de usuarios y del grupo de identidades de Cognito.	

Cómo cambiar el archivo App.js

Tarea	Descripción	Habilidades requeridas
Cambie el archivo App.js.	En la carpeta `src`, abra y revise el archivo `App.js`. El archivo modificado debe tener el siguiente aspecto: <pre>{ App.Js File after modifications:</pre>	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`import React from 'react';` `import logo from './logo.svg';` `import './App.css';` `import { Amplify } from 'aws-amplify';` `import { withAuthenticator, Button, Heading } from '@aws-amplify/ui-react';` `import awsconfig from './aws-exports';` `Amplify.configure(awsconfig);` `function App({ signOut }) {` `return (` `<div>` `<h1>Thankyou for doing verification</h1>` `<h2>My Content</h2>` `<button onClick={signOut}>Sign out</button>` `</div>` `);` `}` `export default withAuthenticator(App);`	

Tarea	Descripción	Habilidades requeridas
Importe paquetes de React.	El archivo `App.js` importa dos paquetes de React. Instale estos paquete mediante el comando: `amplify-react-application1 % npm install --save aws-amplify @aws-amplify/ui-react`	Desarrollador de aplicaciones

Inicie la aplicación React y compruebe la autenticación

Tarea	Descripción	Habilidades requeridas
Inicie la aplicación.	Inicie la aplicación React en su máquina local: `amplify-react-application1 % npm start`	Desarrollador de aplicaciones, AWS general
Compruebe la autenticación.	Compruebe si la aplicación solicita los parámetros de autenticación. (En nuestro ejemplo, configuramos el correo electrónico como método de inicio de sesión). La frontend UI debería pedirle las credenciales de inicio de sesión y ofrecerle la opción de crear una cuenta. También puede configurar el proceso de compilación de Amplify para añadir el	Desarrollador de aplicaciones, AWS general

Tarea	Descripción	Habilidades requeridas
	backend como parte de un flujo de trabajo de implement ación continua. Sin embargo, este patrón no aborda esa opción.	

Recursos relacionados

- Introducción (documentación de npm)
- Crear una cuenta de AWS independiente (documentación de administración de cuentas de AWS)
- Documentación de AWS Amplify
- Documentación de Amazon Cognito

Implemente una aplicación de una sola página basada en React en Amazon S3 y CloudFront

Creado por Jean-Baptiste Guillois (AWS)

Repositorio de código: aplicación CORS de una sola página basada en React	Entorno: producción	Tecnologías: aplicaciones web y móviles; nativas de la nube; sin servidor
Carga de trabajo: todas las demás cargas de trabajo	Servicios de AWS: Amazon CloudFront; Amazon S3; Amazon API Gateway	

Resumen

Una aplicación de una sola página (SPA) es un sitio web o una aplicación web que actualiza dinámicamente el contenido de una página web mostrada mediante JavaScript API. Este enfoque mejora la experiencia del usuario y el rendimiento de un sitio web porque solo actualiza los datos nuevos en lugar de volver a cargar toda la página web desde el servidor.

Este patrón proporciona un step-by-step enfoque para codificar y alojar un SPA escrito en React en Amazon Simple Storage Service (Amazon S3) y Amazon. CloudFront La SPA de este patrón usa una API de REST expuesta por Amazon API Gateway y también muestra las prácticas recomendadas para el intercambio de recursos entre orígenes (CORS).

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa.
- Un entorno de desarrollo integrado (IDE) existente, como AWS Cloud9.
- Node.js y `npm`, instalados y configurados. Para obtener más información, consulte la sección Descargas de la documentación de Node.js.
- Yarm, instalado y configurado. Para obtener más información, consulte la documentación de Yarn.
- Git, instalado y configurado. Para obtener más información, consulte la documentation de Git.

Arquitectura

Esta arquitectura se implementa automáticamente mediante AWS CloudFormation (infraestructura como código). Utiliza servicios regionales como Amazon S3 para almacenar los activos estáticos y Amazon API Gateway para exponer los puntos de conexión de las API regionales (REST). Los registros de la aplicación se recopilan a través de Amazon CloudWatch. Todas las llamadas a las API de AWS se auditan en AWS CloudTrail. Toda la configuración de seguridad (por ejemplo, identidades y permisos) se gestiona en Amazon Identity and Access Management (IAM). El contenido estático se entrega a través de la red de entrega de CloudFront contenido (CDN) de Amazon y Amazon Route 53 gestiona las consultas de DNS.

Pila de tecnología

- Amazon API Gateway
- Amazon CloudFront
- Amazon Route 53
- Amazon S3
- IAM
- Amazon CloudWatch
- AWS CloudTrail
- AWS CloudFormation

Herramientas

Servicios de AWS

- Amazon API Gateway le ayuda a crear, publicar, mantener, supervisar y proteger REST, HTTP y WebSocket API a cualquier escala.
- AWS Cloud9 es un IDE que ayuda a codificar, crear, ejecutar, probar y depurar software. También ayuda a lanzar software a la nube de AWS.
- AWS le CloudFormation ayuda a configurar los recursos de AWS, aprovisionarlos de forma rápida y coherente y gestionarlos durante todo su ciclo de vida en todas las cuentas y regiones de AWS.
- Amazon CloudFront acelera la distribución de tu contenido web al distribuirlo a través de una red mundial de centros de datos, lo que reduce la latencia y mejora el rendimiento.

- AWS le CloudTrail ayuda a auditar la gobernanza, el cumplimiento y el riesgo operativo de su cuenta de AWS.
- Amazon le CloudWatch ayuda a monitorizar las métricas de sus recursos de AWS y las aplicaciones que ejecuta en AWS en tiempo real.
- AWS Identity and Access Management (IAM) le permite administrar de forma segura el acceso a los recursos de AWS mediante el control de quién está autenticado y autorizado a utilizarlos.
- Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad.
- Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que le ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Código

El código de aplicación de muestra de este patrón está disponible en el repositorio de aplicaciones de una sola página CORS GitHub basado en React.

Epics

Cree e implemente la aplicación de forma local

Tarea	Descripción	Habilidades requeridas
Clonar el repositorio.	Recomendamos usar AWS Cloud9 como el IDE para este patrón, pero también puede usar otro IDE, (por ejemplo, Visual Studio Code o IntelliJ IDEA). Ejecute el siguiente comando para clonar el repositorio de la aplicación de ejemplo en su IDE: `git clone https://github.com/aws-samples/react-cors-spa`	Desarrollador de aplicaciones, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	`react-cors-spa && cd react-cors-spa`	
Implemente la aplicación de forma local.	1. En el directorio del proyecto, ejecute el comando `npm install` para iniciar las dependencias de la aplicación. 2. Ejecute el comando `yarn start` para iniciar la aplicación localmente.	Desarrollador de aplicaciones, AWS DevOps
Acceda a la aplicación de forma local.	Abra una ventana del navegador e introduzca la URL `http://localhost:3000` para acceder a la aplicación.	Desarrollador de aplicaciones, AWS DevOps

Implemente de la aplicación

Tarea	Descripción	Habilidades requeridas
Implemente la CloudFormation plantilla de AWS.	1. Inicie sesión en la consola de administración de AWS y, a continuación, abra la CloudFormation consola de AWS. 2. Elija Create stack (Crear pila), y, a continuación, elija With new resources (standard) (Con nuevos recursos [estándar]).	Desarrollador de aplicaciones, AWS DevOps

Tarea	Descripción	Habilidades requeridas
	3. Elija Upload a template file (Cargar un archivo de plantilla). 4. Elija Choose file (Elegir archivo), elija el archivo `react-cors-spa-stack.yaml` del repositorio clonado y, a continuación, elija Next (Siguiente). 5. Escriba un nombre para la pila y después elija Next (Siguiente). 6. Conserve todas las opciones predeterminadas, y luego elija Next (Siguiente). 7. Revise la configuración final de su pila, y luego seleccione Create stack (Crear pila).	

Tarea	Descripción	Habilidades requeridas
Personalice los archivos de origen de su aplicación.	1. Una vez implementada la pila, abra la pestaña Output (Salida) e identifique la URL `APIEndpoint` , el nombre `Bucket` y `CFDistributionURL` . 2. Copie la URL del punto de conexión de la API. 3. Navegue hasta la URL `<project_root>/src/App.js` y péguela en el valor de la variable `APIEndPoint` en la línea 26 del archivo `App.js`.	Desarrollador de aplicaciones
Cree el paquete de aplicación.	En el directorio del proyecto, ejecute el comando `yarn build` para crear el paquete de aplicación.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Implemente el paquete de aplicación.	1. Abra la consola de Amazon S3. 2. Identifique y seleccione el bucket de S3 que creó con anterioridad. 3. Elija Upload (Cargar) y, a continuación, Add files (Añadir archivos). 4. Elija el contenido de su carpeta de compilación. 5. Elija Add folder (Añadir carpeta) y, a continuación, elija el directorio estático. Importante: no elija el contenido, elija el directorio. 6. Elija Upload (Cargar) para cargar los archivos y el directorio a su bucket de S3.	Desarrollador de aplicaciones, AWS DevOps

Pruebe la aplicación

Tarea	Descripción	Habilidades requeridas
Acceda y pruebe la aplicación.	Abra una ventana del navegador y, a continuación, pegue la URL (el `CFDistributionURL` resultado de la CloudFormation pila que implementó anteriormente) para acceder a la aplicación.	Desarrollador de aplicaciones, AWS DevOps

Limpie los recursos

Tarea	Descripción	Habilidades requeridas
Elimine el contenido del bucket de S3.	1. Abra la consola de Amazon S3 y elija el bucket que creó anteriormente con la pila (el primer bucket cuyo nombre comience por `react-cors-spa-`). 2. Seleccione Empty (Vaciar) para eliminar el contenido del bucket. 3. Abra el segundo bucket que creó anteriormente con la pila (el segundo bucket cuyo nombre comience por `react-cors-spa-` y termine por `-logs`). 4. Seleccione Empty (Vaciar) para eliminar el contenido del bucket.	AWS DevOps, desarrollador de aplicaciones
Elimine la CloudFormation pila de AWS.	1. Abra la CloudFormation consola de AWS y elija la pila que creó anteriormente. 2. Elija Delete (Eliminar) para eliminar la pila y todos los recursos relacionados.	AWS DevOps, desarrollador de aplicaciones

Información adicional

Para implementar y alojar su aplicación web, también puede utilizar AWS Amplify Hosting, que proporciona un flujo de trabajo basado en Git para alojar aplicaciones web sin servidor de pila completa con implementación continua. Amplify Hosting es parte de AWS Amplify, que proporciona un conjunto de herramientas y funciones diseñadas específicamente que permiten a los

desarrolladores web y móviles front-end crear, rápida y fácilmente, aplicaciones de pila completa en AWS.

Implemente una API de Amazon API Gateway en un sitio web interno mediante puntos de conexión privados y un Equilibrador de carga de aplicación

Creado por Saurabh Kothari (AWS)

Entorno: producción	Tecnologías: aplicaciones web y móviles; redes; sin servidor; infraestructura	Servicios de AWS: Amazon API Gateway; Amazon Route 53; AWS Certificate Manager (ACM)

Resumen

Este patrón muestra cómo implementar una API de Amazon API Gateway en un sitio web interno al que se puede acceder desde una red en las instalaciones. Aprenderá a crear un nombre de dominio personalizado para una API privada mediante una arquitectura diseñada con puntos de enlace privados, un Application Load Balancer, PrivateLink AWS y Amazon Route 53. Esta arquitectura evita las consecuencias imprevistas del uso de un nombre de dominio y un servidor proxy personalizados para facilitar el enrutamiento basado en el dominio en una API. Por ejemplo, si despliega un punto de conexión de nube privada virtual (VPC) en una subred no enrutable, su red no podrá acceder a API Gateway. Una solución habitual consiste en utilizar un nombre de dominio personalizado y, a continuación, implementar la API en una subred enrutable, pero esto puede dañar otros sitios internos cuando la configuración del proxy transfiere el tráfico (`execute-api.{region}.vpce.amazonaws.com`) a AWS Direct Connect. Por último, este patrón puede ayudarle a cumplir los requisitos organizativos relacionados con el uso de una API privada a la que no se pueda acceder desde Internet y un nombre de dominio personalizado.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de AWS activa
- Un certificado de indicación de nombre de servidor (SNI) para su sitio web y API
- Una conexión desde un entorno en las instalaciones a una cuenta de AWS configurada mediante AWS Direct Connect o AWS Site-to-Site VPN

- Una zona alojada privada con el dominio correspondiente (por ejemplo, domain.com) que se resuelve desde una red en las instalaciones y reenvía las consultas de DNS a Route 53
- Una subred privada enrutable a la que se puede acceder desde una red en las instalaciones

Limitaciones

Para obtener más información sobre las cuotas (antes denominadas límites) para los equilibradores de carga, las reglas y otros recursos, consulte Cuotas para los Equilibrador de carga de aplicación en la documentación de Elastic Load Balancing.

Arquitectura

Pila de tecnología

- Amazon API Gateway
- Amazon Route 53
- Equilibrador de carga de aplicación
- AWS Certificate Manager
- AWS PrivateLink

Arquitectura de destino

En el siguiente diagrama, se muestra cómo se implementa un Equilibrador de carga de aplicación en una VPC que dirige el tráfico web a un grupo objetivo de un sitio web o a un grupo objetivo de la API Gateway en función de las reglas de oyenete de Equilibrador de carga de aplicación. El grupo objetivo de API Gateway es una lista de direcciones IP para el punto de conexión de VPC en la API Gateway. Puerta de enlace de API está configurado para hacer que la API sea privada con su política de recursos. La política deniega todas las llamadas que no procedan de un punto de conexión de VPC específico. Los nombres de dominio personalizados de la API Gateway se actualizan para usar api.domain.com para la API y su fase. Las reglas de Equilibrador de carga de aplicación se agregan para enrutar el tráfico en función del nombre del host.

En el diagrama, se muestra el siguiente flujo de trabajo:

1. Un usuario de una red en las instalaciones intenta acceder a un sitio web interno. La solicitud se envía a ui.domain.com y api.domain.com. A continuación, la solicitud se resuelve en el

Equilibrador de carga de aplicación interno de la subred privada enrutable. El SSL finaliza en el Equilibrador de carga de aplicación de ui.domain.com y api.domain.com.

2. Las reglas de oyente, configuradas en Equilibrador de carga de aplicación, comprueban el encabezado del host.

   a. Si el encabezado del host es api.domain.com, la solicitud se reenvía al grupo objetivo de la API Gateway. El Equilibrador de carga de aplicación inicia una nueva conexión a la API Gateway a través del puerto 443.

   b. Si el encabezado del host es ui.domain.com, la solicitud se reenvía al grupo objetivo del sitio web.

3. Cuando la solicitud llega a la API Gateway, la asignación de dominios personalizada configurada en la API Gateway determina el nombre de host y la API que se debe ejecutar.

Automatizar y escalar

Los pasos de este patrón se pueden automatizar mediante AWS CloudFormation o el AWS Cloud Development Kit (AWS CDK). Para configurar el grupo objetivo de las llamadas a la API Gateway, debe usar un recurso personalizado para recuperar la dirección IP del punto de conexión de VPC. Las llamadas a la API describe-network-interfacesenvían describe-vpc-endpointsy devuelven las direcciones IP y el grupo de seguridad, que se pueden utilizar para crear el grupo de direcciones IP objetivo de la API.

Herramientas

- Amazon API Gateway le ayuda a crear, publicar, mantener, supervisar y proteger REST, HTTP y WebSocket API a cualquier escala.
- Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad.
- AWS Certificate Manager (ACM) le ayuda a crear, almacenar y renovar certificados y claves SSL/TLS X.509 públicos y privados que protegen sus sitios web y aplicaciones de AWS.
- AWS Cloud Development Kit (AWS CDK) es un marco de desarrollo de software que le ayuda a definir y aprovisionar la infraestructura de la nube de AWS en código.
- AWS le PrivateLink ayuda a crear conexiones unidireccionales y privadas desde sus VPC a servicios externos a la VPC.

Epics

Crear un certificado SNI

Tarea	Descripción	Habilidades requeridas
Cree un certificado SNI e impórtelo a ACM.	1. Cree un certificado SNI para ui.domain.com y api.domain.com. Para obtener más información, consulta Cómo CloudFront atender las solicitudes HTTPS en la CloudFront documentación de Amazon. 2. Importe los certificados SNI a AWS Certificate Manager (ACM). Para obtener más información sobre estas dos opciones, consulte Importar certificados a AWS Certificate Manager en la documentación de ACM.	Administrador de red

Implemente un punto de conexión de VPC en una subred privada no enrutable

Tarea	Descripción	Habilidades requeridas
Creación de un punto de conexión de VPC de la interfaz para API Gateway.	Para crear un punto de conexión de VPC de interfaz, siga las instrucciones de Acceder a un servicio de AWS mediante un punto de conexión de VPC de interfaz en la documentación de Amazon Virtual Private Cloud (Amazon VPC).	Administrador de la nube

Configure el Equilibrador de carga de aplicación

Tarea	Descripción	Habilidades requeridas
Creación de un grupo de destino para la aplicación.	Creación de un grupo de destino para los recursos de interfaz de usuario de su aplicación.	Administrador de la nube
Cree un grupo objetivo para el punto de conexión de la API Gateway.	1. Cree un grupo de destino con un tipo de dirección IP y, a continuación, añada la dirección IP del punto de conexión de VPC del punto de conexión de la API Gateway al grupo de destino. 2. Configure las comprobaciones de estado para sus grupos objetivo con los códigos de éxito 200 y 403. El 403 es obligatorio porque la API puede utilizar la autenticación y devolver una respuesta 403.	Administrador de la nube
Cree un Equilibrador de carga de aplicación.	1. Cree un Equilibrador de carga de aplicación (interno) en una subred privada enrutable. 2. Añada el oyente 443 al Equilibrador de carga de aplicación y, a continuación, elija el certificado de ACM.	Administrador de la nube
Cree reglas de oyentes.	Cree reglas de oyente para hacer lo siguiente:	Administrador de la nube

Tarea	Descripción	Habilidades requeridas
	1. Reenviar el host api.domain.com al grupo objetivo de la API Gateway 2. Reenvíe el host ui.domain.com al grupo de destino de los recursos de la interfaz de usuario	

Configure Route 53

Tarea	Descripción	Habilidades requeridas
Crear una zona alojada privada.	Cree una zona alojada privada para domain.com.	Administrador de la nube
Cree registros de dominio.	Cree registros CNAME para lo siguiente: • Una API con el valor establecido en el nombre DNS del Equilibrador de carga de aplicación • Una interfaz de usuario con el valor establecido en el nombre DNS del Equilibrador de carga de aplicación	Administrador de la nube

Cree un punto de conexión de API privado en la API Gateway

Tarea	Descripción	Habilidades requeridas
Cree y configure un punto de conexión de API privado.	1. Para crear un punto de conexión de API privado, siga las instrucciones	Desarrollador de aplicaciones, administrador de la nube

Tarea	Descripción	Habilidades requeridas
	de Cómo crear una API privada en Amazon API Gateway en la documentación de API Gateway. 2. Configure la política de recursos para permitir las llamadas únicamente a la API desde el punto de conexión de VPC. Para obtener más información, consulte Controlar el acceso a una API con las políticas de recursos de API Gateway en la documentación de API Gateway.	
Cree un nombre de dominio personalizado.	1. Crea un nombre de dominio personalizado para api.domain.com. Para obtener más información, consulte Configuración de nombres de dominio personalizados para API de REST en la documentación de API Gateway. 2. Seleccione la API y la etapa creadas. Para obtener más información, consulte Trabajar con asignaciones de API para API de REST en la documentación de API Gateway.	Administrador de la nube

Recursos relacionados

- Amazon API Gateway
- Amazon Route 53
- Equilibrador de carga de aplicación
- AWS PrivateLink
- AWS Certificate Manager

Inserta un QuickSight panel de Amazon en una aplicación Angular local

Creado por Sean Griffin (AWS) y Milena Godau (AWS)

Entorno: PoC o piloto	Tecnologías: aplicaciones web y móviles; análisis	Servicios de AWS: AWS Lambda; Amazon QuickSight; Amazon API Gateway

Resumen

Este patrón proporciona orientación para incrustar un QuickSight panel de Amazon en una aplicación Angular alojada localmente para su desarrollo o prueba. La función de análisis integrada QuickSight no admite esta funcionalidad de forma nativa. Requiere una QuickSight cuenta con un panel de control existente y conocimientos de Angular.

Cuando trabajas con QuickSight paneles integrados, normalmente tendrás que alojar tu aplicación en un servidor web para ver el panel. Esto dificulta el desarrollo, ya que hay que enviar continuamente los cambios al servidor web para asegurarse de que todo funciona correctamente. Este patrón muestra cómo ejecutar un servidor alojado localmente y cómo utilizar el análisis QuickSight integrado para facilitar y agilizar el proceso de desarrollo.

Requisitos previos y limitaciones

Requisitos previos

- Una cuenta de Amazon Web Services (AWS) activa
- Una QuickSight cuenta activa con precios por capacidad de sesión
- QuickSight SDK de incrustación instalado
- CLI de Angular instalada
- Familiaridad con Angular
- mkcert instalado

Limitaciones

- Este patrón proporciona orientación sobre cómo incrustar un QuickSight panel mediante el tipo de autenticación `ANONYMOUS` (de acceso público). Si utiliza AWS Identity and Access Management (IAM) o la QuickSight autenticación con sus paneles integrados, el código proporcionado no se aplicará. Sin embargo, los pasos para alojar la aplicación Angular en la sección Epics siguen siendo válidos.
- El uso de la GetDashboardEmbedUrlAPI con el tipo de `ANONYMOUS` identidad requiere un plan de precios por QuickSight capacidad.

Versiones

- CLI de Angular versión 13.3.4
- QuickSight Incorporar la versión 2.3.1 del SDK

Arquitectura

Pila de tecnología

- Interfaz de Angular
- Backend de AWS Lambda y Amazon API Gateway

Arquitectura

En esta arquitectura, las API HTTP de API Gateway permiten que la aplicación Angular local llame a la función de Lambda. La función Lambda devuelve la URL para incrustar el panel. QuickSight

Automatizar y escalar

Puede automatizar la implementación de back-end mediante AWS CloudFormation o AWS Serverless Application Model (AWS Serverless Application Model).

Herramientas

Herramientas

- CLI de Angular es una herramienta de interfaz de la línea de comandos que se utiliza para inicializar, desarrollar, estructurar y mantener aplicaciones de Angular directamente desde un intérprete de comandos.
- QuickSight El SDK de incrustación se utiliza para incrustar QuickSight paneles en el código HTML.
- mkcert es una herramienta sencilla para crear certificados de desarrollo fiables a nivel local. No requiere configuración. Se requiere mkcert porque solo QuickSight permite solicitudes HTTPS para incrustar paneles.

Servicios de AWS

- Amazon API Gateway es un servicio de AWS para crear, publicar, mantener, supervisar y proteger REST, HTTP y WebSocket API a cualquier escala.
- AWS Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. Lambda ejecuta su código solo cuando es necesario y escala de manera automática, desde unas pocas solicitudes por día hasta miles por segundo. Solo pagará por el tiempo de computación que consuma, no se aplican cargos cuando el código no se está ejecutando.
- Amazon QuickSight es un servicio de análisis empresarial para crear visualizaciones, realizar análisis ad hoc y obtener información empresarial a partir de sus datos.

Epics

Generar EmbedURL

Tarea	Descripción	Habilidades requeridas
Cree una EmbedUrl política.	Cree una política de IAM con un nombre Quicksigh tGetDashboardEmbedUrlque tenga las siguientes propiedad es. `{ "Version": "2012-10-17", "Statement": [`	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
	<pre>{ "Effect": "Allow", "Action": ["quicksight:GetDashboardEmbedUrl", "quickSight:GetAnonymousUserEmbedUrl"], "Resource": "*" }] }</pre>	

Tarea	Descripción	Habilidades requeridas
Crear la función de Lambda.	1. Abra la página Funciones en la consola de Lambda. 2. Elija Crear función. 3. Elija Crear desde cero. 4. En Nombre de la función, introduzca `get-qs-embed-url`. 5. En Runtime (Tiempo de ejecución), elija Python 3.9. 6. Elija Crear función. 7. En la pestaña Código, copie el siguiente código en la función de Lambda. `import json` `import boto3` `from botocore.` `exceptions import` ` ClientError` `import time` `from os import environ` `qs = boto3.client('quic` `ksight',region_nam` `e='us-east-1')` `sts = boto3.cli` `ent('sts')` `ACCOUNT_ID = boto3.cli` `ent('sts').get_cal` `ler_identity().get` `('Account')`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	DASHBOARD_ID = environ['DASHBOARD _ID'] def getDashboardURL(ac countId, dashboardId, quicksightNamespac e, resetDisabled, undoRedoDisabled): try: response = qs.get_da shboard_embed_url(AwsAccountId = accountId, DashboardId = dashboardId, Namespace = quicksightNamespace, IdentityType = 'ANONYMOUS', SessionLi fetimeInMinutes = 600, UndoRedoDisabled = undoRedoDisabled, ResetDisabled = resetDisabled) return response except ClientError as e: print(e) return "Error generating embeddedU RL: " + str(e) def lambda_handler(eve nt, context): url = getDashbo ardURL(ACCOUNT_ID, DASHBOARD_ID,	

Tarea	Descripción	Habilidades requeridas
	"default", True, True) ['EmbedUrl'] return { 'statusCode': 200, 'url': url } 8. Seleccione Implementar.	

Tarea	Descripción	Habilidades requeridas
Añada el ID del panel de control como variable de entorno.	Añada `DASHBOARD_ID` como variable de entorno a su función de Lambda: 1. En la pestaña Configuración, seleccione Variables de entorno, Editar y Añadir variable de entorno. 2. Añada una variable de entorno con la clave `DASHBOARD_ID` . 3. Para obtener el valor de`DASHBOARD_ID` , vaya al panel de control QuickSight y copie el UUID al final de la URL en el navegador. Por ejemplo, si la URL es `https://us-east-1.quicksight.aws.amazon.com/sn/dashboards/<dashboard-id>` , especifique la parte `<dashboard-id>` de la URL como valor clave. 4. Seleccione Guardar.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Añada permisos para la función de Lambda.	Modifique la función de ejecución de la función Lambda y agréguele la QuicksightGetDashboardEmbedUrlpolítica. 1. En la pestaña Configuración, elija Permisos y, a continuación, elija el nombre del rol. 2. Elija Adjuntar políticas, busque `QuicksightGetDashboardEmbedUrl`, marque su casilla de verificación y, a continuación, elija Adjuntar política.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Probar la función de Lambda.	Cree y ejecute un evento de prueba. Puede usar la plantilla "Hello World", ya que la función no utilizará ninguno de los datos del evento de prueba. 1. Elija la pestaña Prueba. 2. Asigne un nombre al evento de prueba y, a continuac ión, seleccione Guardar. 3. Para probar su función de Lambda, elija Probar. La respuesta debería ser similar a la siguiente. `{ "statusCode": 200, "url": "\"https://us-east-1.quicksight.aws.amazon.com/embed/f1acc0786687783b9a4543a05ba929b3a/dashboards/... }` Nota: Como se menciona en la sección Requisitos previos y limitaciones, su QuickSight cuenta debe estar sujeta a un plan de precios por capacidad de sesión. De lo contrario, en este se paso mostrará un mensaje de error.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Crear una API en API Gateway.	1. En la consola de API Gateway, elija Crear API y, a continuación, elija REST API, Crear. • Para el nombre de la API, escriba `qs-embed-api` . • Seleccione Crear API. 2. En Acciones, elija Crear método. • Seleccione GET y confirme pulsando la marca de verificación. • Elija Función de Lambda como tipo de integración. • En Función de Lambda, introduzca `get-qs-embed-url` . • Seleccione Guardar. • En el cuadro Agregar permiso a la función de Lambda, elija Aceptar. 3. Habilite CORS. • En Acciones, elija Habilitar CORS. • Para Access-Control-Allow-Origin, introduca `'https://my-qs-app.net:4200'` . • Elija Habiltar CORS y reemplazar los	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	encabezados CORS existentes, y confirme. 4. Implementar la API. • Para Acciones, seleccione Implementar API. • En Deployment stage (Etapa de implementación), elija [new stage] ([nueva etapa]). • En Stage name (Nombre de etapa), escriba `dev`. • Elija Deploy (Implementar). • Copie la URL de invocación. Nota: `my-qs-app.net` puede ser cualquier dominio. Si quiere usar un nombre de dominio diferente, asegúrese de actualizar la información de Access-Control-Allow-Origin en el paso 3 y cambiar `my-qs-app.net` en los pasos siguientes.	

Crear la aplicación Angular

Tarea	Descripción	Habilidades requeridas
Cree la aplicación con la CLI de Angular.	1. Cree la aplicación.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`` ng new quicksight-app --defaults cd quicksight-app/src /app ``` 2. Cree el componente del panel de control. ``` ng g c dashboard ``` 3. Vaya a su archivo `src/environments/environment.ts` y agregue `apiUrl: '<Invoke URL from previous steps>'` al objeto del entorno. ``` export const environme nt = { production: false, apiUrl: '<Invoke URL from previous steps>', }; ```	

Tarea	Descripción	Habilidades requeridas
Agrega el SDK de QuickSight incrustación.	1. Instala el SDK QuickSight de incrustación ejecutando el siguiente comando en la carpeta raíz del proyecto. `npm i amazon-quicksight-embedding-sdk` 2. Cree un nuevo archivo `decl.d.ts` en la carpeta `src` con el siguiente contenido. `declare module 'amazon-quicksight-embedding-sdk';`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Añada código a su archivo dashboard.component.ts.	`import { Component, OnInit } from '@angular/core';` `import { HttpClient } from '@angular/common/http';` `import * as QuicksightEmbedding from 'amazon-quicksight-embedding-sdk';` `import { environment } from "../../environments/environment";` `import { take } from 'rxjs';` `import { EmbeddingContext } from 'amazon-quicksight-embedding-sdk/dist/types';` `import { createEmbeddingContext } from 'amazon-quicksight-embedding-sdk';` `@Component({` `  selector: 'app-dashboard',` `  templateUrl: './dashboard.component.html',` `  styleUrls: ['./dashboard.component.scss']` `})` `export class DashboardComponent implements OnInit {` `  constructor(private http: HttpClient) { }`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`  loadingError = false;` `  dashboard: any;` `  ngOnInit() {` `  this.GetDashboardU` `RL();` `  }` `  public GetDashbo` `ardURL() {` `  this.http.get(envi` `ronment.apiUrl)` `  .pipe(` `  take(1),` `  )` `  .subscribe((data:` ` any) => this.Dash` `board(data.url));` `  }` `  public async Dashboard` `(embeddedURL: any) {` `  var containerDiv` ` = document.getElemen` `tById("dashboardCo` `ntainer") || '';` `  const frameOptions` ` = {` `  url: embeddedURL,` `  container:` ` containerDiv,` `  height: "850px",` `  width: "100%",` `  resizeHei` `ghtOnSizeChangedEv` `ent: true,` `  }` `  const embedding` `Context: Embedding` `Context = await` ` createEmbeddingCon` `text();`	

Tarea	Descripción	Habilidades requeridas
	`this.dashboard = embeddingContext.embedDashboard(frameOptions); } }`	
Añada código a su archivo dashboard.component.html.	Agregue el siguiente código al archivo `src/app/dashboard/dashboard.component.html` . `<div id="dashboardContainer"></div>`	Desarrollador de aplicaciones
Modifique el archivo app.component.html para cargar el componente del panel de control.	1. Elimine el contenido del archivo `src/app/app.component.html` . 2. Añada lo siguiente. `<app-dashboard></app-dashboard>`	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
Importa HttpClientModule a tu archivo app.module.ts.	1. En la parte superior del archivo `src/app/app.module.ts` , añada lo siguiente: `import { HttpClientModule } from '@angular/common/http';` 2. Agregue `HttpClientModule` a la matriz `imports` para su `AppModule` .	Desarrollador de aplicaciones

Alojar la aplicación Angular

Tarea	Descripción	Habilidades requeridas
Configure mkcert.	Nota: Los siguientes comandos son para máquinas Unix o macOS. Si utiliza Windows, consulte la sección Información adicional para ver el comando echo equivalente. 1. Cree una entidad de certificación (CA) local en el equipo. `mkcert -install` 2. Configure `my-qs-app.net` para que siempre se redirija a su PC local.	Desarrollador de aplicaciones

Tarea	Descripción	Habilidades requeridas
	`echo "127.0.0.1 my-qs-app.net" | sudo tee -a /private/etc/hosts` 3. Asegúrese de que está en el directorio `src` del proyecto de Angular. `mkcert my-qs-app.net 127.0.0.1`	
Configúralo para permitir tu dominio QuickSight .	1. En QuickSight, elige tu nombre en la esquina superior derecha y, a continuación, selecciona Administrar Quicksight. 2. Vaya a Dominios e integración. 3. Añada `https://my-qs-app.net:4200` como dominio permitido.	Administrador de AWS

Tarea	Descripción	Habilidades requeridas
Probar la solución.	Para iniciar un servidor de desarrollo local de Angular, ejecute el siguiente comando. `ng serve --host my-qs-app.net --port 4200 --ssl --ssl-key "./src/my-qs-app.net-key.pem" --ssl-cert "./src/my-qs-app.net.pem" -o` Esto habilita la capa de conexión segura (SSL) con el certificado personalizado que ha creado anteriormente. Cuando se complete la compilación, se abrirá una ventana del navegador y podrás ver tu QuickSight panel integrado alojado localmente en Angular.	Desarrollador de aplicaciones

Recursos relacionados

- Sitio web de Angular
- Incrustar paneles de QuickSight datos para usuarios anónimos (no registrados) (documentación) QuickSight
- QuickSight Incrustar el SDK
- herramienta mkcert

Información adicional

Si utiliza Windows, ejecute la ventana de línea de comandos como administrador y configure `my-qs-app.net` para que siempre se redirija a su PC local mediante el siguiente comando.

```
echo 127.0.0.1 my-qs-app.net >> %WINDIR%\System32\Drivers\Etc\Hosts
```

Más patrones

- Acceder a los servicios de AWS desde una aplicación ASP.NET Core mediante los grupos de identidades de Amazon Cognito
- Acceda a las aplicaciones de contenedores de forma privada en Amazon ECS mediante AWS Fargate PrivateLink, AWS y un Network Load Balancer
- Acceda a las aplicaciones de contenedores de forma privada en Amazon ECS mediante AWS PrivateLink y un Network Load Balancer
- Automatice la identificación y planificación de la estrategia de migración mediante AppScore
- Cree una arquitectura de acoplamiento flexible con microservicios mediante DevOps prácticas y AWS Cloud9
- Cree una aplicación móvil React Native sin servidor con AWS Amplify
- Cree y pruebe aplicaciones iOS con AWS CodeCommit CodePipeline, AWS y AWS Device Farm
- Configure el registro para aplicaciones.NET en Amazon CloudWatch Logs mediante nLog
- ???
- Cree una canalización e implemente actualizaciones de artefactos en instancias EC2 locales mediante CodePipeline
- Crear una definición de tareas de Amazon ECS y montar un sistema de archivos en instancias EC2 mediante Amazon EFS
- Implemente una aplicación basada en gRPC en un clúster de Amazon EKS y acceda a ella con un Equilibrador de carga de aplicación
- Despliega canarios de CloudWatch Synthetics con Terraform
- Implemente microservicios Java en Amazon ECS mediante Amazon ECR y AWS Fargate
- Implementar microservicios de Java en Amazon ECS mediante Amazon ECR y el equilibrio de carga
- Implementar microservicios de Java en Amazon ECS con AWS Fargate
- Explore el desarrollo completo de aplicaciones web nativas en la nube con Green Boost
- Migración de una cola de mensajes de Microsoft Azure Service Bus a Amazon SQS
- Migración de una aplicación .NET de Microsoft Azure App Service a AWS Elastic Beanstalk
- Migración de una aplicación web Go en las instalaciones a AWS Elastic Beanstalk mediante el método binario
- Migración de un servidor SFTP en las instalaciones a AWS mediante AWS Transfer para SFTP

- Migre de IBM WebSphere Application Server a Apache Tomcat en Amazon EC2
- Migre de IBM WebSphere Application Server a Apache Tomcat en Amazon EC2 con Auto Scaling
- Migre de Oracle GlassFish a AWS Elastic Beanstalk
- Migración de aplicaciones Java locales en las instalaciones a AWS mediante AWS App2Container
- Migre OpenText TeamSite las cargas de trabajo a la nube de AWS
- Migración de los certificados SSL de Windows a un equilibrador de carga de aplicación mediante ACM
- Modernizar las aplicaciones de ASP.NET Web Forms en AWS
- Ejecute un contenedor de Docker de la API web de ASP.NET Core en una instancia Linux de Amazon EC2
- Sirva contenido estático en un bucket de Amazon S3 a través de una VPC mediante Amazon CloudFront
- Configure una PeopleSoft arquitectura de alta disponibilidad en AWS
- Utilice Network Firewall para capturar los nombres de dominio DNS de la indicación del nombre del servidor (SNI) para el tráfico saliente
- ???

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.